

## **Lawyers, Data, Money -- Start now examining the products, partners, and processes you need to accommodate the feds' new rules of evidence**

Information Week Via Thomson Dialog NewsEdge  
More detail on implications of e-discovery

It's a perfect storm: the rapid-fire growth of digitized enterprise data, new regulatory requirements, and tough e-discovery readiness levels demanded by the revised Federal Rules of Civil Procedure. No wonder Gartner estimates that by 2010, three of four large enterprise IT departments will employ dedicated legal or e-discovery specialists-few IT groups have experienced the level of interdisciplinary cooperation they'll need to stay afloat.

A proactive strategy involving your legal counsel and one or more e-discovery vendors is necessary to stay agile in the face of litigation. The good news is that there are a variety of products to help with this task. Many major data management players have built or acquired e-discovery functionality. Specialized vendors' products range from document management tools to full-service systems.

Although not a surprise to industry watchers-the e-discovery amendments to the FRCP, the legal code governing the critical discovery phase of civil litigation in federal court, slogged through a five-year administrative process-IT pros and even some corporate counsel are scrambling to adjust. Vendors have been grooming their offerings, and we expect a flurry of merger and acquisition activity that began a few years ago to intensify as the market continues to double in size annually for at least the next two years.

E-discovery raises some of the same questions that we've seen with records management, regulatory compliance, e-mail archiving, and other data management issues. You need to evaluate relevant policies and procedures, including data retention, backup and restoration, and litigation-hold compliance. Finally, start e-discovery vendor and product evaluations now so you're ready for the day when you need those systems.

### **AN EXPENSIVE AWAKENING**

In 2003, Morgan Stanley was embroiled in its fifth year of litigation over an accounting fraud case stemming from its role as adviser to Sunbeam. During the discovery process, the opposing party requested e-mail that Morgan Stanley couldn't produce. Finally, backup tapes were located, but some may have been overwritten. Then, in its attempt to begin archiving e-mail according to the discovery order, Morgan Stanley flubbed the filter, causing as many as 7,000 messages to be left out of its response.

But wait, it gets better: Morgan Stanley refused the opposing party's offer to hire a neutral third party to handle e-mail discovery, even rebuffing its offer to foot half the bill. The judge came down hard, presaging the jury's \$1.5 billion decision against the company. The Securities and Exchange Commission imposed a \$15 million fine and ordered the financial firm to overhaul its e-mail retention policies.

Then, early last December, the Federal Rules of Civil Procedure were officially revised and updated for the electronic age. While specifics of the new FRCP may not become part of your average IT manager's lexicon, we guarantee that the requirements they spawn will affect how your systems are deployed and operated. Essentially, they create critical new obligations for any party to a lawsuit in federal court. For example, following the filing of a case, parties are required to discuss as soon as possible e-discovery issues, including preserving discoverable data, a plan for producing the data, and the format in which it will be provided. And be prepared to equip your counsel to discuss these plans with a judge.

In the past, e-discovery was often the elephant in the room. Now, the revised FRCP forces IT groups and their attorneys to face these issues from the very start of a lawsuit. Because the vast majority of cases settle before going to trial, the discovery phase is often the most critical part of litigation.

Prepare now to handle e-discovery by undertaking a broad survey of IT systems that could be implicated in a typical litigation context. That includes e-mail and file servers, individual users' workstations and laptops, mobile devices, network access control systems, and in-house or custom applications.

Define data retention policies for each IT system. If you don't have these policies, the best time to implement them is during a lull, when you're free from active litigation that relates to the system in question. Retention policies adopted during a litigation hold, or even when litigation is reasonably anticipated, could draw sanctions for spoliation-alteration-of evidence, not to mention a risk of malpractice for attorneys recommending such policies. While the new FRCP includes a safe-harbor provision for inadvertent loss of documents from "routine, good-faith operation" of an IT system, courts haven't yet defined how this provision will apply. It certainly won't excuse sloppy handling of e-discovery requests.

From an IT service delivery standpoint, these issues loom large and will spur, shall we say, an interesting evolution in the relationship between IT and the rest of the enterprise. The trend over the past 20 years has been to cede autonomy to end users, who now expect to wield significant control over their computing devices and services. A strategic balance must be struck between user productivity and e-discovery readiness-not an easy task.

## **WAKE UP TO E-DISCOVERY**

Your strategic reverie has just been shattered by an e-mail from the legal department saying you'll be teaming on a request for proposals for e-discovery vendors to be sent out next week, with final selection in short order. What should you look for in an e-discovery product? And what should you look for in a vendor?

Search accuracy is important for two reasons. First, it's critical to produce relevant documents; failure here can lead to sanctions. Second, improved search can lower the cost of e-discovery. Search and analysis apps churn out documents that are potentially relevant and, more important, potentially protected by attorney-client or other privileges. Nonrelevant or privileged documents need to be flagged and not disclosed to the opposing party. Review of all documents identified by an e-discovery product must still be performed by an individual, typically an attorney. Therefore, reducing the time required for review through better search capabilities largely determines the total cost of a discovery response.

More advanced methodologies are emerging. For example, "concept searching" promises to discover documents pertaining to the concept sought but containing terms different from those used in typical documents that fit the parameters of the discovery request. While such methods remain more of a curiosity, some industry analysts expect them to gain popularity if and when they're approved by the various organizations overseeing the development and standardization of the e-discovery industry, such as the nonprofit Sedona Conference ([www.thesedonaconference.org](http://www.thesedonaconference.org)).

Detecting all relevant documents is only half the game. Providing context for making sense of a massive data set is also critical. As always, good visualization tools are priceless. You can try such a tool online by digging through 200,000 e-mail messages from Enron senior management in a database released to the public in 2003 by the Federal Energy Regulatory Commission ([enron.trampolinesystems.com](http://enron.trampolinesystems.com)). In this class of tool, some products provide features to "discover" relationships among far-flung parties.

A few niche players inhabit the e-discovery marketplace, including tape-restoration companies offering high-speed services for legacy and modern backup platforms, and imaging-oriented services that convert large volumes of electronic or scanned paper documents into TIFF images, the standard preferred by legal customers. With vendors streaming into the e-discovery field, competition in the imaging market has halved the standard 25-cents-per-page rate for paper-to-TIFF conversion. Watch for specialized companies to merge or be acquired by larger players.

Evaluating a potential partner is just as crucial as ensuring that its product suits your requirements. Long-term health and financial stability are a must, as a lawsuit can easily stretch to three or more years. Consider entering into a code escrow agreement to enable continuity with a product should the vendor fail to withstand the upcoming market shakeout. Look for vendors that understand the technology as well as the law, as one without the other will leave an insurmountable gap. Also, evaluate the product or service delivery method-standalone, hosted, or hybrid-and ensure that it meets the workflow and availability requirements of both the IT and legal departments.

Investigate the professional services offerings of large product vendors, as well as e-discovery service vendors such as law firms that use a third-party product. While

deploying and running products in-house can reduce costs, being able to rely on specialized technical expertise at crunch time provides an invaluable fallback. E-discovery requests can take on lives of their own, even when managed by experienced legal teams. It may be worth the price premium to ramp up using the resources of your vendor rather than swamping your internal staff and risking an insufficient response, not to mention endangering ongoing business operations. Finally, ensure that your vendor has experience in the courtroom, as its testimony may be necessary at a trial.