



E-Discovery: A Lifecycle of Its Own

December 6, 2006

By Rob Garretson

Legal judgments and sanctions can be costly for companies that can't find the information required for court hearings. Morgan Stanley is expected to post more than \$7 billion in profits for 2006. But even this Wall Street behemoth felt a sting last year when a Florida jury slapped it with a \$1.45 billion judgment, now approaching \$1.6 billion with interest and other adjustments.

The jury found in favor of billionaire Ronald Perelman, who accused the global investment bank of helping Sunbeam Corp. inflate its earnings back in 1998. Perelman had sold Sunbeam his controlling interest in camping equipment maker Coleman Co. for \$680 million in stock that became worthless after Sunbeam restated earnings and filed for bankruptcy. The case famously turned on Morgan Stanley's mishandling of e-mail evidence, which led presiding Judge Elizabeth T. Maass to instruct jurors they could assume Morgan Stanley was complicit in the deception because of its failure to turn over all relevant e-mail.

The case was no legal anomaly, just the most costly warning shot fired to date across the bow of corporate America in advance of new federal rules of evidence that went into effect on Dec. 1. Escalating regulatory requirements, along with spiraling costs of managing burgeoning data stores, have already spurred some companies to implement information lifecycle management—the concept of matching data retention policy and [storage systems](#) to the business value of the underlying information. Now, new legal requirements are adding fuel to the fire and creating strange new bedfellows among CIOs, corporate counsel and compliance officers, who are being forced to collaborate on a solution and reverse decades of unfettered data expansion.

These new revisions to the Federal Rules of Civil Procedure—only the sixth modification to the rules governing civil suits in the last 70 years—are intended to bring the courts up to speed with modern communications technology. Up to 80 percent to 90 percent of all business communication is now conducted via e-mail and electronic documents—to say nothing of instant messaging, cellphone text messaging, voice mail and the like. This evolution of business practices has turned the once-routine pretrial fact-finding called "discovery" into a costly quagmire that has the courts struggling to decipher electronic databases, e-mail archives, backup tapes and other data repositories.

Enter the brave new world of e-discovery. The new rules recognize "electronically stored information" as a distinct form of discovery, and require the parties in a federal lawsuit to provide, at the outset, a detailed description of how they manage, retrieve and purge electronic data—including unstructured repositories such as e-mail systems and instant-messaging logs. Though the Dec. 1 rule changes apply to federal courts only, state courts and other jurisdictions typically adopt the federal rules, or similar variations. Among states that have already adopted them are California, Delaware, Illinois, Maryland, Mississippi, New Jersey and Texas. What this means for CIOs is that they have been formally annexed into the legal team at most large corporations, which typically are party to dozens, if not hundreds, of lawsuits at any given time.

Ask the Legal Department:

Do you and outside counsel have a basic understanding of how and where the company's data is stored?

Ask your Storage Manager:

How easily can we find and produce critical business communications and records that have been archived?

Challenge

New federal e-discovery rules require companies to detail their ILM policies and procedures at the outset of litigation. U.S. companies with gross revenues of \$1 billion or more are currently fielding 556 lawsuits on average, according to the latest edition of Fulbright & Jaworski's "Litigation Trends Survey." Almost half of those companies face 50 new lawsuits annually, a number that many large firms expect to increase in the coming year.

And the vast majority of reporting businesses say they are not prepared to handle an e-discovery challenge.

"The new rules really go to the heart of information lifecycle management and expose the wound that we see," says Rick Wolf, former head of global compliance at Cendant Corp., the \$18 billion hotel and travel services conglomerate that dismantled itself earlier this year. He sees a "global information-management crisis," brought on by years of corporations throwing more cheap, multitiered storage and processing speed at the burgeoning glut of information—particularly unstructured data such as e-mail, instant messaging and Web

pages—without regard to the business value of the information or the cost of locating it when needed.

"It's analogous to the Industrial Revolution, when companies manufactured at a rapid pace irrespective of the effects of that activity on the environment, and we're still cleaning it up today," notes Wolf. "In the Information Age, the way to compete is through the Internet and e-mail. And there's been no regard whatsoever to where all the information is going."

Wolf cites statistics that show more than 84 billion e-mails being sent and received each day by businesses worldwide, almost triple the volume only four years ago. "It's like we need an Information Superfund," he adds. His dire assessment was echoed in a survey of senior corporate executives published in September by the nonprofit Business Performance Management Forum, an industry group. Nearly half of the 400 executives surveyed across North America expressed concern that the failure to effectively archive and manage their electronic content was a critical liability for their companies. A third of respondents to the survey, conducted for compliance software maker AXS-One Inc., said they have no corporate policy covering electronic records management, and another 20 percent said they didn't know if they even had a policy.

The cost of processing data that is subject to discovery—by using a litigation-review tool to preserve it and present it for legal review—can range from \$1,200 to \$2,500 per gigabyte, estimates Laura Bandrowsky, the practice support manager in the IT department at Duane Morris LLP, a law firm based in Philadelphia. But that's just the cost of using the software tool to cull potentially relevant data for lawyers to review, which is only the tip of the iceberg. The big expense is having that subset of data reviewed by high-priced lawyers to determine what's relevant to the case at hand. Some e-discovery practitioners peg the cost of sifting e-mail for relevant information at about \$2 per message, which adds up quickly when archives total in the hundreds of thousands, or millions, of messages.

"The volume of data that must be managed or handled for litigation directly affects the cost of discovery," cautions Bandrowsky, who is also chief operating officer of Wescott Technology Services LLC, a Duane Morris unit that provides technology consulting and e-discovery services to clients and other law firms. She estimates that the discovery costs for a recent client that started with roughly 300 gigabytes of raw data, which was then winnowed to about 150 gigabytes produced for litigation, totaled about \$4 million, including lawyer review time.

Ask the Records Manager(s):

Do we have effective systems for archiving business records and other electronic content?

Ask your Storage Manager:

Do we maintain separate e-mail and records archives that are distinct from backups used for disaster recovery?

Implementation

A comprehensive data inventory and better [collaboration](#) are keys to minimizing discovery and litigation risks. Fortigent, a Rockville, Md., provider of wealth-management services to banks, investment advisors and other financial intermediaries, does more than most companies to manage its data. The subsidiary of Lydian Trust Co., with more than \$10 billion in assets under advisement, captures all client-related e-mail, indexes it and transmits it to an off-site third party for archiving, according to Chief Technology Officer Jamie McIntyre. All other client information—such as investment proposals and performance reports, along with the production data on investment accounts managed for its clients—is stored in perpetuity on the company's servers, which are also backed up off-site. Yet the firm has no formal policy for purging data that may be outdated or unnecessary.

"Data storage has been relatively cheap compared to the amount of information that we have, so it hasn't been worthwhile to set up anything like that," McIntyre says. He notes, however, that a large portion of Fortigent's client base are banks that are subject to Sarbanes-Oxley and other regulations, forcing it to look at its records-retention policy.

Fortigent is among countless companies that invested heavily in recent years in storage systems to keep more and more data rapidly accessible—particularly in response to Sarbanes-Oxley, HIPAA and other regulations mandating the storage and safekeeping of financial data and medical records. Yet the new e-discovery rules have created a diametrical force that is now pulling corporations toward pruning data stores that have mushroomed in recent years. "We're talking about corporations that have petabytes of information," cautions Nicholas Croce, president of Lynbrook, N.Y.-based DOAR Litigation Consulting, "and the new rules will require you to deal with [the data store] no matter how large it is."

But while most large companies have tiered storage and systems for managing the expansion of their data repositories, surprisingly few have comprehensive retention plans that limit their growth. Such plans are critical for effective ILM, experts say. And like Fortigent, many corporations fail to purge data stores of "non-records" or information of fleeting business value, notes Julie Gable, a records-management consultant based in Wyndmoor, Pa. Eliminating extraneous data that must be sifted for relevant information in discovery can help keep costs down.

"I'm not saying you should hide anything from discovery, or do anything unethical. And if litigation is pending or imminent, you can't destroy data," adds Gable. "But it works in everyone's best interests—from a storage standpoint, from a records standpoint, and from a litigation standpoint—to be able to identify those things that are lasting records and protect them, and identify those things that are

fleeting and make them go away."

Automated systems for moving data among multiple tiers of storage—from production systems to disk-based backups, then to tape archives, for example—based on the data's age and frequency of access aren't sufficient, records management and legal experts say. Though they are often billed as ILM "solutions," they fall short of matching the business value of specific pieces of data to the retention policy and storage systems, which requires more procedure than product. Records-management and legal experts agree that companies need to gather high-ranking representatives from IT, legal, compliance and human resources (since employee training is also critical), to hammer out records-management and retention policies that wed business need for access to information with legal and regulatory obligations, while keeping the volume of data in check.

"Most companies already own the technology that will solve their problems," asserts Wolf, who recently launched Lexakos LLC, a consultancy specializing in compliance, records management and e-discovery controls, after leading the development of a records-management system at Cendant. "What they don't have is a handle on their business processes and behavior. The solution is often much simpler than throwing technology at the problem," he says.

One way to address the mushrooming volume of e-mail, instant messages and other unstructured data is for companies to wean themselves off their over-reliance on those tools, Wolf argues. Even simple collaboration tools, such as Microsoft Corp.'s Sharepoint, Novell Inc.'s GroupWise, or IBM Corp.'s Lotus Notes, already used in most large companies, can be used for document management and retention, cutting down on the volume of e-mail generated, for example, when documents need to be circulated for review.

"What companies tend to do, in my experience, is to take new technology and configure it to old processes," Wolf contends. "And that makes it far more expensive and oftentimes unsatisfactory, because people never re-evaluate the way that they communicate."

Ask your CTO:

Are we making maximum use of collaboration tools and document-management systems to limit the overuse of e-mail and IM?

Ask your head of HR:

Have employees been adequately trained on document and records-retention policies, and on how to use the tools needed to implement them?

Future

Corporate litigation is on the rise, heightening the need for CIOs to work with legal and compliance officers on e-discovery. The rising cost of e-discovery and the need for better ILM is creating some strange bedfellows, as CIOs are forced to work more closely with legal and compliance officers, along with records-management and human-resources departments, to develop and enforce effective data-retention policies.

"CIOs and chief legal officers have never been the best of friends," notes DOAR Litigation Consulting's Croce, who nonetheless recommends that "CIOs befriend the general counsel" and attempt to understand the challenges faced by the legal team. "If they don't do that in a positive, proactive sense, the bull's-eye will be on their backs when there's a litigation or regulatory investigation," he warns. IT and legal departments should not only collaborate to develop data retention policies, Croce advises, but possibly even jointly budget for new systems, which could save money on discovery and litigation expenses while trimming data storage costs.

"It really is a collaborative process," echoes consultant Gable, who recommends the formation of a steering committee whose members have enough executive clout to mandate policy companywide and represent IT, legal, compliance, records management, finance and HR functions. "What you don't want to do is have one department writing checks that the others can't cash, so you've got legal saying 'we're going to do this,' and IT saying 'how are we going to do that?'"

"It often boils down to who owns records management or content management, and leaders who are willing to take the risk of implementing something that will require the modification of behavior for almost everyone in the company," Wolf insists. "And there needs to be someone at a very high level who will take responsibility for minding this issue, day in and day out."

And although the CIO isn't always the best judge of the business value of specific pieces of company data in his care—other corporate functions should drive that evaluation, experts say—the buck typically stops in the IT department.

"It's going to be a tough world for the CIOs to really deal with this," Croce adds. "It's one of those situations where, if they get it right, unfortunately, they probably won't get the medal, but if they get it wrong, they'll certainly be feeling the heat."

Ask your General Counsel:

How much do you budget for litigation and discovery costs annually?

Ask your CEO:

Will you provide CXO support for the development of a companywide document and data retention policy?

Copyright (c) 2006 Ziff Davis Media Inc. All Rights Reserved.