

# STREAMLINING e-discovery

Consider the following hypothetical situation involving a large multinational corporation:

*Almost three months after it was publicly threatened, the ACME Corporation was served with a product liability lawsuit. In-house and outside counsel felt positive about the defenses to the action, and all efforts were focused on summary judgment. Meanwhile, discovery was underway, and the in-house attorneys were certain they had taken adequate measures to preserve and produce documents. After all, within a few weeks after the suit was served, the in-house attorneys sent a document preservation notice to key employees and the IT department, instructing everyone to preserve all relevant documents. However, during the deposition of the department manager, he claimed that no one had asked him to retain any documents and admitted that he had deleted emails and other documents since the suit was filed. Three days later, the spoliation motion was served. When counsel went to collect the data, only 30 days' worth of email remained—IT had routinely recycled months of email tapes and had continued the automatic deletion of messages that were at least 90 days old. The company's email administrator had read the preservation notice but, failing to understand it, did not interrupt the deletion process and continued rotating email backup tapes. As a result, the company received significant monetary sanctions, and a case that originally appeared frivolous was later settled for more than six figures.*

## COSTS

BY CYNTHIA NICHOLS AND LINDA G. SHARP





Cynthia Nichols is the litigation manager in Taco Bell Corp.'s legal department in Irvine, CA. In addition to her work on significant litigation, Ms. Nichols has researched, developed, and implemented practices relating to electronic discovery, knowledge-based databases, and company-wide email policies and procedures. She can be reached at [cynthia.nichols@yum.com](mailto:cynthia.nichols@yum.com).



Linda G. Sharp, Esq., MBA, is a legal consultant for Kroll Ontrack. She assists attorneys with discovery and investigations surrounding electronically stored data and emails, and educates litigation support staff on data collection, production, and review options. Ms. Sharp is based in Los Angeles, CA, and can be reached at [lsharp@krollontrack.com](mailto:lsharp@krollontrack.com).

## THE SAD SONG OF METROPOLITAN OPERA

In the *Metropolitan Opera* case,<sup>\*</sup> the Union failed in its obligation to search for, preserve, or produce electronic documents. The court sharply reprimanded its attorneys, stating “[C]ounsel (1) never gave adequate instructions to their clients about the clients’ overall discovery obligations, what constitutes a ‘document’...; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who (at least until July 2001) did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had ‘establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests’....” Displeased with counsel’s behavior, the court granted severe sanctions, finding liability on the part of the Union and ordering the Union to pay Metropolitan’s attorney fees. *Metropolitan Opera* demonstrates that failing to plan for discovery with IT ahead of time can lead to costly results.

<sup>\*</sup> *Metropolitan Opera Assoc., Inc. v. Local 100*, 212 F.R.D. 178 (S.D.N.Y. 2003).

Sound unusual? In today’s technology climate, this situation is routinely faced by in-house counsel who are called upon to make important decisions relating to document preservation and electronic discovery.

Organizations, in-house legal departments, and IT personnel can no longer turn a blind eye and pretend electronic discovery is just a passing fad. From Morgan Stanley to Philip Morris to Samsung, today’s newspapers are filled with headlines about companies being hit with adverse inference jury instructions, default judgments, and enormous damage awards because the companies failed to properly locate, preserve, and produce electronic documents. Twenty-first century courts are not only handling electronic data as mainstream discovery, they are also clearly unwilling to tolerate destruction of relevant electronic evidence.

With more than 90 percent of all communication taking place electronically, in-house counsel must implement procedures for effectively managing and controlling the company’s electronic documents—or risk putting its business, stock price, and reputation at stake.

Not surprisingly, general counsel and in-house litigation support professionals are being called to address electronic discovery issues—and the cost concerns they pose—with greater frequency. With discovery typically representing 50 percent of the litigation costs in the average case, and up to 90 percent of the litigation costs in cases in which it is actively pursued, organizations have cause for concern.<sup>1</sup> Corporations and in-house counsel must figure out the best ways to preserve and produce data, while still minimizing the costs associated with digital discovery.

This article provides tips and ideas for in-house legal professionals on how to trim electronic discovery costs by proactively developing solutions to their electronic discovery approach.

### THE ZUBULAKE CASE: COUNSEL’S STANDARD IN FEDERAL COURT

It is not uncommon for a year to pass between the filing of a complaint and the filing of the first discovery motion. During this time, huge amounts of potentially relevant data could be destroyed per a company’s standard records retention policy (RRP). Even if all of the destroyed data is irrelevant to the case, a company

that fails to take appropriate preservation steps exposes itself to possible liability for spoliation.

In-house counsel can prevent potential spoliation problems by taking control of the electronic discovery process. This is a daunting task for many attorneys who are not technically savvy, and who never expected to be concerned with such matters as backup tapes and metadata. However, courts and lawmakers are forcing practitioners to learn about these technologies. No longer can you just send out a standard preservation letter instructing the IT department and other employees to preserve all relevant data, and then leave it up to them to decide what is relevant and how it should be preserved.

**MOST BUSINESSPEOPLE THINK IT IS ENOUGH FOR THEM TO PRESERVE A SUMMARY DATABASE CONTAINING THE REQUESTED INFORMATION. NOT UNTIL THEY ARE IN THE MIDDLE OF A DEPOSITION DO THEY DISCOVER THAT UNDERLYING DOCUMENTS WERE USED TO POPULATE THAT SUMMARY DATABASE, AND THOSE DOCUMENTS WERE DESTROYED LONG AGO.**

In the fifth opinion in the *Zubulake v. UBS Warburg* case, Judge Shira Scheindlin set out the duty that federal courts and many state courts now impose on both in-house and outside counsel who are handling a lawsuit. First, “[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.”<sup>2</sup>

Second, said the court, counsel must guarantee that all relevant documents are preserved by placing a litigation hold on the documents, communicating to key players the need to preserve these documents, and arranging for the safeguarding of relevant archival media. It is counsel’s responsibility to be certain that all relevant data is safe from inappropriate destruction—whether intentional or accidental.

Finally, counsel is obligated to ensure that all relevant documents are produced when requested.

How can you do all this in a cost-effective manner, with as little interference as possible to your com-

pany’s business operations? You must start by identifying your obligations and taking control of them. You must also know what data exists, where it is located, how it is stored, and how it can best be protected. Listed below are a few tactics that can assist you in proactively reducing your company’s exposure as well as overall electronic discovery costs.

**BUILD A BRIDGE BETWEEN THE IT AND LAW DEPARTMENTS**

**Appoint an IT Liaison**

Day after day, companies are finding themselves hit with spoliation sanctions because there was a chasm between the data the companies’ legal teams intended to protect and the data the IT staff and key employees thought they were supposed to protect. For instance, most businesspeople think it is enough for them to preserve a summary database containing the requested information. Not until they are in the middle of a deposition do they discover that underlying documents were used to populate that summary database, and those documents were destroyed long ago.

To minimize such communication problems, it is vital for your company to have an attorney in the legal department who is responsible for working directly with IT on a regular basis. This individual should be responsible for proactively discussing technical considerations with your company’s IT manager. This liaison to the IT department should:

- become familiar with your company’s RRP and IT architecture;
- communicate with your IT department to learn about backup and recycling procedures; and
- develop procedures for interrupting the automatic deletion of email messages, electronic files, local hard drives, and backup tapes in the event of litigation. The procedures should allow for quick, effective litigation holds that protect relevant data without shutting down your company’s entire network or its routine backup processes.

Your IT liaison should have the technical experience and knowledge to develop carefully tailored preservation requests. This should eliminate the objections often heard from IT about extremely broad requests to preserve massive amounts of data. Such overbroad requests impose significant extra work and costs on the department.

From this point on . . .  
Explore information related to this topic.

## ACC RESOURCES ON ELECTRONIC DISCOVERY:

- Richard J. Corbett and Virginia R. Llewellyn, *The Next Discovery Frontier: Preparing for Backup Data Requests*, ACCA DOCKET 21 (October 2003): 116–131. Available on ACC Online<sup>SM</sup> at [www.acca.com/protected/pubs/docket/on03/backup.pdf](http://www.acca.com/protected/pubs/docket/on03/backup.pdf).
- *Document Retention & E-discovery in a Post-Enron/Andersen World*, ACCA 2003 Annual Meeting course material, available on ACC Online at [www.acca.com/education03/am/cm/704.pdf](http://www.acca.com/education03/am/cm/704.pdf).
- *Document Retention Around the World: A Quick Guide*. A Global Counsel resource, available by searching the ACC Virtual Library<sup>SM</sup> at [www.acca.com/vl/](http://www.acca.com/vl/) under the subject heading “Records Retention.”
- *Electronic Discovery: Litigation and Antitrust Enforcement in a Digital Age*, ACCA DOCKET 20 (February 2002): 76–87. Available on ACC Online at [www.acca.com/protected/pubs/docket/fm02/ediscovery1.php](http://www.acca.com/protected/pubs/docket/fm02/ediscovery1.php).
- *Email and the Internet*, an ACC InfoPAK<sup>SM</sup>, available on ACC Online at [www.acca.com/infopaks/email.html](http://www.acca.com/infopaks/email.html).
- Jeffrey Jacobs and Whitney Adams, *Ghost in the Machine: Legal Developments and Practical Advice in an Age of Electronic Discovery*, ACC DOCKET 22 (July/August 2004): 48–72. Available on ACC Online at [www.acca.com/protected/pubs/docket/ja04/ghost.pdf](http://www.acca.com/protected/pubs/docket/ja04/ghost.pdf).
- *Leading Practices in Information Management and Records Retention Programs* (August 2003). Available on ACC Online at [www.acca.com/protected/article/records/lead\\_infomgmt.pdf](http://www.acca.com/protected/article/records/lead_infomgmt.pdf).
- *Records Retention: Enforced Corporate Records Programs*, an ACC InfoPAK, available on ACC Online at [www.acca.com/infopaks/retentent.html](http://www.acca.com/infopaks/retentent.html).
- *Sample Electronic Discovery Interrogatories and Requests for Production*, an ACC Sample Form & Policy (2004), available on ACC Online at [www.acca.com/protected/reference/litigation/ediscoveryinterrog.pdf](http://www.acca.com/protected/reference/litigation/ediscoveryinterrog.pdf).
- *Ten Tips on Handling Electronic Discovery*, an ACC Quick Reference, available on ACC Online at [www.acca.com/protected/reference/litigation/ediscovery\\_tips.pdf](http://www.acca.com/protected/reference/litigation/ediscovery_tips.pdf).
- *Ten Tips for Electronic Discovery: Judge Shira A. Scheindlin Speaks on Proposed Rules Changes and Surviving E-discovery Without Sanctions*, ACC DOCKET 23 (January 2005): 56–76. Available on ACC Online at [www.acca.com/protected/pubs/docket/jan05/ediscovery.pdf](http://www.acca.com/protected/pubs/docket/jan05/ediscovery.pdf).
- ACC Webcasts are audio presentations available via the internet. The following are available on ACC Online via [www.acca.com/practice/index.php](http://www.acca.com/practice/index.php):
  - *Corporate Protection Through Records Policy Enforcement* (October 2004)
  - *Managing & Controlling Email as a Record* (April 2004)
  - *Proposed Changes to the Federal Rules of Civil Procedure Relating to Electronic Discovery* (February 2005)
  - *Records Policy Enforcement: Best Practices Across Corporate and Email Records* (May 2005)

If you like the resources listed here, visit ACC's Virtual Library<sup>SM</sup> on ACC Online<sup>SM</sup> at [www.acca.com/resources/vl.php](http://www.acca.com/resources/vl.php). Our library is stocked with information provided by ACC members and others. If you have questions or need assistance in accessing this information, please contact Senior Staff Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or [palmer@acca.com](mailto:palmer@acca.com). If you have resources, including redacted documents, that you are willing to share, email electronic documents to Julienne Bramesco, director of Legal Resources, [bramesco@acca.com](mailto:bramesco@acca.com).

The liaison should become familiar with which employees are using home computers or wireless devices to access email remotely, and should be aware of the effect such remote access may have on a preservation hold. Many of these devices are not encompassed within the company's standard records retention procedures, so the data on these devices may well be kept or destroyed in contravention of company policy. For example, your company could be embarrassed if it learned, in the middle of the CEO's deposition, that many business records supposedly purged as part of the company's RRP still exist on the CEO's home computer.

Your liaison should be responsible for understanding the network infrastructure of your company and for analyzing the impact that infrastructure changes would have on existing and future litigation. When IT makes infrastructure changes, their priority is not ongoing or future litigation. They are simply searching for more cost-effective ways to manage huge volumes of data. Unfortunately, failing to account for the legal effects can cost your company dearly.

Having such a liaison also serves several other functions. The liaison will be a valuable resource for outside counsel because he or she will be able to explain the document retention and backup system for purposes of Fed. R. Civ. P. 30(b)(6) depositions, which allow a party to serve notice on a corporation requiring it to designate "officers, directors, or managing agents, or other persons" to testify on its behalf about "matters known or reasonably available to the organization." Having the liaison in place also helps reduce the costs associated with ongoing motions and court appearances because companies will not have to expend time and resources finding and educating a newly designated individual about these issues. The liaison will already be trained in the area and will be a single point of contact for outside counsel. In addition, a liaison will help implement and monitor preservation compliance, reducing the potential for spoliation sanctions if data is not properly preserved.

#### **Tips for Working with IT**

You and your legal team should have ongoing communications with your IT department about where company records reside, how they are maintained, when they are destroyed, and how to best preserve selected records that may be relevant to a prospective

or extant lawsuit. Here are some tips for getting the best results from your IT department:

*Thoroughly interview the IT staff.* Long before a lawsuit surfaces, it is vital that you comprehensively interview the IT team regarding your company's IT topology and systems. The IT department is a valuable resource for identifying records retention practices, hardware and software conventions, and the accessibility of data. An interview can shed light on external data sources (such as personal computers used for remote access to the network) and on other sources of hidden data that might become of crucial importance.

*Interview people at different levels of the IT department* to get a thorough understanding of how things are done. A conversation with the IT director may provide a completely different answer than an interview with someone in the trenches; what the manual requires is not necessarily what is being done in the field.

*Ask extensive questions about the ability of users to save data locally* (as opposed to on the network). In many cases, even if IT has requested that users not save data on their desktop hard drives, users are saving it there anyway. This data sits outside of the backup tape processes and will not be captured. A full and complete data capture may thus require an image of many workstations. *Evaluate key data locations and important file types.* If your company operates in multiple locations, uses different types of technologies, or has employees with disparate access to these technologies, it can be difficult to ascertain where relevant electronic records are being kept. Inquire about all potential data locations, including geographical locations and storage locations (such as shared network drives where multiple employees can save and share documents, email devices, archival tapes, hosted email, and attachments).

*Ask about legacy, archive, or nonstandard data.* It is important to be aware of a company's legacy, archive, or nonstandard data and systems. If not addressed with IT early on, these data types can potentially delay any electronic discovery investigation for weeks or months, owing to the need for some type of secondary conversion or specialty program to interpret this information.

(continued on page 52)

(continued from page 48)

*Your law department's liaison to the IT group should determine if there is a legitimate business or regulatory reason to maintain this old or non-standard data. If there is not, your company should get rid of it.*

*Work with IT to prioritize the data.* When you want to create a litigation hold, you should quickly and clearly inform IT about the scope of the information to be protected and the priority IT should assign to the key players—the individuals in the corporation who probably possess discoverable data. Providing this information as early as possible will avoid unnecessary delays and extra costs down the road.

### **IF DATA IS SAVED ON A PRIORITY BASIS, COUNSEL WILL ALSO BE IN A BETTER POSITION TO ADVOCATE FOR DATA SAMPLING OR COST-SHIFTING MEASURES FOR NON-PRIORITY DATA.**

*You should also work with IT on developing a plan for backing up and segregating priority data (the data likely to be discoverable from key players such as executives or human resources personnel). Many companies use at least five or six backup tapes daily, and the email messages are interspersed with network programs, accounting data, and infrastructure (such as the global address book). By prioritizing the data on a day-to-day basis, companies can save thousands of dollars by collecting and processing the highest priority individuals first when responding to production requests, often eliminating the need to copy and review tapes that merely contain the office word processing and accounting programs. In many cases, it will be unnecessary to process non-priority data, resulting in significant savings. If data is saved on a priority basis, counsel will also be in a better position to advocate for data sampling or cost-shifting measures for non-priority data.*

*Ensure IT maintains a proper chain of custody.* In the event of litigation, IT may be called on to

handle a variety of media, including hard drives, PDAs, and removable media (such as CDs, floppy disks, or DVDs). IT must maintain a documented chain of custody on these media, from the time the item is acquired until it is transferred out of IT's control. The chain of custody should indicate who possessed which media at all times and the reason for that possession. This will allow you to verify which tapes were transferred on a specific date, if data spoliation accusations later surface. In some situations, a third-party vendor may need to take control of the data, removing it from the IT department to ensure no one accidentally reuses or loses those tapes. Should any data be transferred to a vendor, you must be sure to document the chain of custody.

#### **Plan for IT Issues in Mergers and Acquisitions**

When your company participates in M&A activity, the result may be good for your company's bottom line, but bad for your company's ability to protect and recover electronic documents. Problems often arise when network systems are combined and individuals are downsized in order to eliminate redundant positions. The IT employee who assisted in your last electronic discovery project may be gone, requiring you to educate a new employee about the need to preserve and potentially produce documents. Even worse, the terminated individual might have been the only person who could have thoroughly educated you about the acquired company's network infrastructure and what needs to be done in order to put an effective preservation hold in place.

To avoid these problems, you should develop a plan if IT resources are slashed during a merger or acquisition. During this time of upheaval, any pending document retention orders will be on the bottom of the list for the IT department, so you should assemble a planning team made up of in-house counsel, IT representatives from both companies, litigation support staff, and possibly outside counsel who have worked with the companies on past electronic discovery projects. If necessary, ask for assistance from an electronic discovery expert in formulating an integration strategy. The team should identify possible key users from both companies in order to determine which data to prioritize. The IT department should identify legacy or outdated media and data that may require special-

---

ized processing or conversion if subjected to discovery. Both IT departments should also be able to identify and explain key data locations on the network. After examining the differences in hardware and software practices, the team will be able to determine the best ongoing preservation system and methodology. Often legacy data is not transferred to the new, consolidated system owing to financial and storage constraints.

The law department's liaison to the IT department can help avoid any information gaps by becoming familiar with the network protocols for both the acquiring and the target company. Any written documentation regarding the target's automatic deletion programs or procedures should be provided to the acquirer's IT staff.

#### **Issues Relating to Outsourced IT Systems**

An increasing number of companies have little idea where their data is located and how it is

stored, because they have outsourced the processing and storing of their data to other companies. This in no way mitigates a company's duty to protect discoverable data and to provide it upon request. The courts have made it clear that if data is discoverable, relevant, and not privileged, it must be produced—regardless of its location.<sup>5</sup> In other words, you remain responsible for your company's data, even when the data is outsourced to specialized IT vendors.

If your company has some (or all) of its data handled by an outside IT vendor, it is likely that the vendor will report to someone in the IT department—and probably will *not* be notified when you issue a litigation hold. In a situation like this, it is quite likely the vendor will blindly continue destroying records pursuant to your company's RRP. The best way to solve this problem is for your liaison to the IT department to stay well informed about your company's use of outside IT vendors.

## REDUCE DATA PRESERVATION AND PROCESSING COSTS

One important way to save on expenses is to ensure that only relevant records are preserved, and that money is not spent preserving and restoring records that are never going to be used. You can accomplish this by applying the following methods.

## ELECTRONIC EVIDENCE RESOURCES

- The Association of Information Management Professionals: [www.arma.org/](http://www.arma.org/) (includes information relating to document management and retention policies).
- California Civil Discovery Law: <http://CaliforniaDiscovery.findlaw.com> (contains California electronic discovery information).
- Ken Withers: [www.kenwithers.com](http://www.kenwithers.com) (extensive electronic discovery law library).
- Kroll Ontrack: [www.krollontrack.com/legalresources](http://www.krollontrack.com/legalresources) (includes an extensive case law database, sample forms, articles, and free case law newsletter).
- Lange, Michele C.S. and Kristin M. Nimsger. *Electronic Evidence and Discovery: What Every Lawyer Should Know*. American Bar Association, 2004.
- Lange, Michele C.S. and Linda G. Sharp. *Juggling the Worlds of Paper and Electronic Discovery: How can outside counsel make sure they are comprehensive in their search for information while minimizing costs?* ABTL Report (2004).
- Richmond Journal of Law and Technology: <http://law.richmond.edu/jolt/index.asp> (an online law review of technology-related articles from the University of Richmond School of Law).
- The Sedona Conference®: [www.thesedonaconference.org](http://www.thesedonaconference.org) (electronic discovery principles & document retention guidelines).
- The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Sedona Conference<sup>SM</sup> Working Group Series 2004). [www.thesedonaconference.org](http://www.thesedonaconference.org)
- The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery (Sedona Conference Working Group Series 2004). [www.thesedonaconference.org](http://www.thesedonaconference.org)

## Use Document Management Systems

Many in-house attorneys come from large and mid-sized law firms, where they had access to a document management system (DMS). The DMS is used by the law firm's IT department to archive client matters and to provide the firm with the ability to return client files—intact—if the client demands that all its files and records be returned. The DMS assigns destruction dates on a matter-by-matter basis, much like in the paper world. Once the matter is closed, the retention schedule kicks in automatically and the relevant data is systematically removed from the servers.

In response to the volume of legitimate business emails, many law firms today have implemented an email component to their DMS servers, allowing them to track email messages associated with various cases. Law firms are also purging unnecessary email data, such as notices about company picnics, new babies, and donuts in the kitchen.

DMS can also be used profitably in the corporate environment. Much like in the paper world, your company could use a DMS to assign a retention period to each and every matter, project, or deal. When a matter concludes, it is assigned a retention period and set for removal from the servers or backup systems. In the interim, that data may be reasonably and efficiently retrieved.

While it may be impractical for a Fortune 500 company to put all of its employees on a DMS, it may be important to use it for key people within the organization—those individuals whose data is sought on an ongoing basis. Organizations can skip the receptionist or mailroom folks, but should consider using a DMS for the board of directors, executives, people in the legal department, people in the HR department, and other individuals who make significant decisions for the organization.

A DMS allows an organization to accurately and efficiently implement a preservation hold on the documents of key personnel based on product, subject, and so forth (depending on how the DMS is configured). The company can also cost-effectively segregate its data by developing, implementing, and monitoring a retention schedule that fits the business needs. For example, a corporation in the technology industry is going to have different retention requirements than a financial services corporation. Finally, if some backup data needs to be restored, the company

will deliver a carefully limited amount of data to an electronic discovery vendor, avoiding the need for the vendor to hunt through hundreds of backup tapes filled with email about company picnic notices and other irrelevant electronic files.

### **Segregate Backup Systems**

Many companies have segregated servers for email, accounting, customer service, and other business functions. Each of these servers is usually backed up independently. For example, the email backup server is separate from accounting's backup server. This so-called functional backup creates problems for corporations that do not use DMS for their emails, because emails from the receptionist sit on the same tapes as those from the CEO. If a company has 10,000 employees and only needs data for 15 people over a particular period of time, all of the backup tapes for that period will need to be restored in order to produce the documents for those 15 individuals.

## **BY EMPLOYING DATA SAMPLING, COMPANIES MAY SAVE THOUSANDS OR HUNDREDS OF THOUSANDS OF DOLLARS, DEPENDING ON THE SIZE OF THE PROJECT.**

The problems are much worse, however, for those companies which have moved from functional backups to mass backups—where everything from email to accounting to software programs are lumped together on huge backup servers (which are large robotic devices that manipulate tapes with little or no human intervention). In this situation, a single tape or group of tapes might contain emails, accounting databases, and the network-based programs and directory. Sifting through all this information is a huge task, and it is an extremely costly way to recover emails concerning only a few individuals.

Thus, if your company does not wish to use a DMS, you should consider segregating your backup servers by function and/or setting up two separate backup systems, one for line workers with a set retention policy and another separate backup system for key personnel. This segregated

environment allows you to implement a litigation hold for key employees without affecting the backup system that handles the data for the mass of your company's employees. Each system can have a separate RRP, based upon appropriate business and legal considerations.

Segregating your backup tapes should significantly reduce your electronic discovery costs. Your electronic discovery vendor won't have to process hundreds or even thousands of backup tapes filled with irrelevant data, but will instead be able to focus on the tapes backed up for key individuals or subjects potentially related to the litigation. The vendor will do less filtering and, therefore, charge less. Moreover, your company will also slash its costs for attorney review time.

Functional backup systems have their own problems, however. The tapes for these systems are often retained for a short, specified time period and then reused to reduce media and storage costs. This relatively short recycling period puts additional pressure on the company to put in place an effective litigation hold system that can quickly interrupt this process, if need be.

### **Use Data Samples**

Most of the costs for electronic discovery consist of the expenses for processing backup tapes. Such processing puts backup data, which is not in a format that counsel can reasonably review for responsiveness and privilege, into a usable format. Essentially, this processing uses a number of criteria, such as keyword searches and date filtering, to locate potentially relevant data from backup tapes, hard drives, and other electronic media. Both parties will need to agree on the criteria for culling this potentially relevant data. Once the data is found, a copy of it is put into a powerful online database for searching. All this work is referred to as the initial data pass.

After this initial pass is complete, the data is set up in either a native file, TIFF image, or PDF format, so attorneys can review the data and decide which records should be produced. Documents tagged for production are then assigned a Bates number, redactions are burned into the image, and a production set is delivered.

When volumes of data are present, counsel may want to process only a sample of the data. Starting with a sample of the data may reveal relevant docu-

ments do not exist for a particular time period, making it unnecessary to actually process or review the entire data set. If a data sample does not provide the anticipated result, counsel may settle for a dismissal of the action or agree upon the next group of data to be processed. By employing data sampling, companies may save thousands or hundreds of thousands of dollars, depending on the size of the project.

## **TAKE CONTROL OF THE VENDOR SELECTION PROCESS**

### **Start Early**

Electronic discovery is very different from discovery of printed documents. In the old days, when all records were on paper, attorneys did not engage in discovery until the litigation proceedings were well underway. Today, with the majority of the data residing in electronic media, this strategy could result in monetary sanctions, an adverse inference instruction, or even dismissal of the case.

Since electronic documents usually have short retention periods, the sooner an electronic discovery expert is involved, the better. The expert should partner with you through the process, offering ideas on how to save money, ensuring proper chain of custody processes, and being prepared and qualified to testify if necessary.

### **Select a Preferred Electronic Discovery Expert**

Many corporations have adopted preferred vendors for many services, such as airlines, rental car companies, and photocopy services. Similarly, in the litigation context, your company will probably benefit from a preferred discovery vendor for the collection, processing, and hosting of electronic and paper documents.

Should selecting a preferred vendor be left to outside counsel? This is probably the most common and economical solution for companies with smaller or infrequent litigation issues. Outside counsel, at least in the larger firms, probably contract with a preferred vendor or two that offer discounts.

However, for companies with ongoing litigation and/or national or international exposure, having outside counsel pick a vendor may not be the most cost-effective solution. Because many corporations use multiple law firms across the country, they may not benefit from economies of scale if they rely on differ-

ent vendors chosen by different law firms. Moreover, by leaving the selection process up to outside counsel, a company may pay outside counsel to act as a middleman between it and the outside vendor. This will result in frequent and repetitive questions about the data in order to determine appropriate discounts and other processes.

A typical outside counsel vendor selection process starts with counsel considering five to six vendors. Each vendor will have several meetings and calls with outside counsel, who, in turn, will call in-house counsel for the answer and then call the vendor back with the answers. Outside counsel will then narrow down the selection to two or three vendors and present them to the company for final approval. As part of this process, the company should expect to rack up significant costs for paying outside counsel and educating potential vendors on the company's infrastructure.

By limiting negotiations to one or two preferred vendors, your company may be able to save money on the bid process costs and reduce the amount of time it takes to get an outside vendor educated about your system. Moreover, by working closely with your company over time, preferred vendors can become knowledgeable about your company, its IT staff, its systems, and any network infrastructure changes. The vendors thus become better able to assist outside counsel with the nuts and bolts of the case, without being bogged down by technical questions. In the event of impending litigation, the vendor is able to respond quickly and effectively to ensure proper processes are put into place to preserve only relevant data—avoiding the work that would otherwise be spent shutting down backup processes in order to determine data locations and relevancy. Because preferred vendors come to know your company and your systems so well, your company greatly increases its likelihood of properly complying with all discovery requirements—and concomitantly reduces the risk of being slapped with a spoliation sanction for failing to properly preserve data.

When selecting preferred vendors, in-house counsel should consider the following criteria:

- *Experience.* Asking a vendor with relatively little electronic discovery experience to comply with a large, comprehensive electronic data request can be a weighty demand. Make sure your data collection expert is specially trained to understand the various technical arrangements of your IT

---

systems and has experience with almost every one of your hardware and software platforms. The expert should also have experience protecting the evidentiary integrity of data throughout the gathering, sorting, and production processes.

- *Technology and equipment.* A qualified electronic discovery specialist should maintain libraries of out-of-date software so that any data created on antiquated systems is easily restorable. In addition, the expert should maintain its own high-speed systems to provide the fastest and most accurate collection, filtering, and conversion processes.
- *Security.* Your electronic discovery specialist should maintain an extremely high level of physical security, as well as data and document security. The specialist should have internal security procedures that safeguard its discovery processes and that protect the integrity of your hardware, software, and data that are to be held by the specialist for analysis. The specialist's staff should

use strict chain-of-custody procedures on all media and documents. The company should also use state-of-the-art equipment to ensure that no loss or damage to the hardware or data occurs during handling and processing.

If the vendor uses a web-based repository for document review, you need to make sure that the vendor's infrastructure does not leave any residue of your company's trade secret documents on outside counsel's computers, including their employees' home computers or leased equipment. Such precautionary steps will help ensure that your company's confidential information is not inadvertently made public.

*Personnel and training.* Inquire about the vendor's employees and the amount of training they receive. The vendor's personnel should have extensive technical, legal, and industry experience. A company with seasoned professionals will be better able to help determine what information is technically feasible to collect, what information would be

required for production, and what the best format is for that production. They can work with you to demonstrate to the court or opposition that your document production strategy is appropriate. These professionals can reduce costs, save time, and eliminate unnecessary efforts.

A vendor should also assign a project manager or similar individual as a single point of contact throughout the entire project. A qualified project manager will have experience managing complex electronic discovery projects involving multiple storage locations, large volumes of data, and a variety of media types. If expert testimony regarding data collection is necessary, the vendor should be able to provide a testifying individual who has the technical ability and credentials to withstand aggressive cross-examination.

Examine the vendor's hiring policies. For example, does each employee handling your data undergo a drug test and background screening? Hold the vendor to the same standards your company uses when hiring its employees.

- **Pricing.** A vendor's pricing should be competitive with other service providers in the industry. However, an unusually low price often produces poor quality results. An extraordinarily high price generally identifies a misunderstanding of the project scope.
- **Quality.** Quality control is always of utmost importance. Ask if the company has a quality assurance unit. Find out how it is structured and the costs associated with its services. Ask about the vendor's equipment testing procedures. How

does the company assure test procedures are followed? How often does the vendor test its equipment or other tools?

- **Output options.** A qualified electronic discovery specialist should offer multiple output options for legal document review, including printed documents, litigation support software, native review, and online document repositories.
- **Ability to meet deadlines.** Electronic discovery timelines are aggressive, so it is vital that your vendor be able to meet the logistical demands of data gathering and production. Find out if the vendor has a proven track record of meeting tight deadlines by inquiring about previous projects the vendor has worked on. Satisfying the time limits required by the bench or opposing party may not be feasible if your electronic discovery vendor has limited processing capabilities. Ask about the volume of data they can handle and request a tour of their facilities to verify their capabilities. A vendor with a solid business reputation in the electronic discovery community will likely go the extra mile to make sure your project is completed in a timely manner. It is always best practice to ask for references from corporations that have used the vendor's services in the past.
- **Outsourcing.** Determine if the vendor plans on using subcontractors. If so, each and every subcontractor should undergo the same scrutiny imposed on the primary vendor.

### Reuse Discovery Data

Many companies have multiple cases involving the same issues and thus many of the same documents or data. For instance, companies that market one product will probably need the same documentation on that product for nearly every lawsuit filed against it relating to that product. By recycling data used in other cases, companies can often realize significant cost and time savings.

The best way to achieve such savings is to work proactively with a selected e-discovery vendor. By implementing a process before repetitive litigation ensues, you can realize cost savings down the road. You will eliminate the cost of a double collection, processing, and review by simply reusing data already deemed responsive and not privileged in a previous lawsuit. Your goal is to create a process that takes documents that may be used in more than one litiga-

Come and establish your protocol for handling electronic records. Register for ACC's 2005 Annual Meeting on October 17-19 in Washington, DC. Topics include:

- Pitfalls & Landmines in Privacy and the Collection, Use, and Security of Personal Information;
- Workplace Privacy; and
- How to Manage Smoking Guns: The Ethical, Legal and Practical Guidelines for Document Retention.

For more information go to [www.acca.com/am/05](http://www.acca.com/am/05).

---

tion, such as HR and operations manuals, patent and trademark information, white papers, and CEO declarations, and indexes those documents consistently from one litigation to the next.

Your first step is to determine which categories of documents or specific documents and files are repeatedly pulled in case after case. With the help of an electronic discovery vendor, these documents can be maintained in a core litigation database. Not only will many of the key documents be immediately available to outside counsel when the new litigation arises, this core database will serve as the backbone for the case-specific database. Depending on their corporate makeup, some corporations may wish to segregate the data into several core databases. If, for example, there are multiple subsidiaries or the company is routinely engaged in litigation on a number of distinct product lines, they may wish to have a separate database containing documents and data about each product line or subsidiary. Having a core

database of these documents will save time and money spent on collecting and reviewing them for future productions. When production is necessary, the data will already be compiled, reviewed, and found responsive, eliminating the need to recollect, reprocess, re-review, and re-determine responsiveness in case after case.

By eliminating the need to pay multiple law firms to collect, review, and categorize the same document set, a large company could potentially save millions of dollars. Such streamlining would also ensure the declarations of key personnel are consistently presented, minimizing the potential for differing declarations showing up in later litigation.

#### **PLANNING FOR SUCCESS**

As companies continue to increase their reliance on technology, their attorneys need to know more

than simply where their clients' electronic evidence resides. Counsel have a duty to know whether that data is accessible and how much it will cost to restore, search, and produce the data in the event of litigation or a regulatory investigation.


As electronic data continues to grow by leaps and bounds, courts, lawmakers, and regulatory agencies will continue to define and clarify document management, production, and preservation practices and obligations through case law, civil rule changes, and local rule amendments.

The Advisory Committee on Civil Rules recently approved proposed amendments dealing with electronic discovery to Federal Rules of Civil Procedure 16, 26, 33, 34, 37, and 45.<sup>4</sup> The Committee anticipates sending the amendments to the Standing Committee on Rules of Practice and Procedure with a recommendation that they be approved and transmitted to the Judicial Conference for consideration. While the proposed federal rules will help shape corporate digital data practices, in-house counsel also need to stay on top of current and emerging local and state discovery rule changes. Being aware of these electronic discovery rule changes, as well as any case law developments, will put you in the best position to effectively manage the electronic discovery process.

You should also look for a host of up-and-coming high-tech gadgets. Prepare to develop strategies for less-conventional media, such as PDAs, cell phones with email capabilities, USB drives, and instant messaging tools. As technology continues to change, essential sources of electronic evidence will surface, and in-house counsel must keep up with these cutting-edge advances.

In addition to the developments in technology devices, in-house counsel should expect changes in

document production practices. In the last few years, litigators learned that producing electronic data in hard copy format was insufficient because it resulted in lost metadata and the inability to search the data. As online review tools and repositories increase in popularity and become more sophisticated, attorneys are finding it easier and less expensive to produce electronic documents in an online repository. The litigation team can categorize, redact, and annotate the documents in the review tool. When complete, they can copy the relevant and non-privileged documents to a separate production database for the opposing party, court, or government agency to complete its review. You should expect to see increased use of online repositories for producing and managing volumes of both paper and electronic documents.

Courts use hindsight to examine corporate actions, and companies, in-house counsel, and IT departments never want to be in the position of second-guessing what could have been done better or differently. By planning upfront and implementing appropriate processes, in-house counsel will be well positioned to execute a successful, case-winning discovery plan while curtailing excessive electronic discovery costs. 

The authors gratefully acknowledge the assistance of Charity Delich, a Knoll Ontrack law clerk.

#### NOTES

1. [www.uscourts.gov/ttb/oct99ttb/october1999.html](http://www.uscourts.gov/ttb/oct99ttb/october1999.html).
2. *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).
3. See *e.g.*, *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995) ("Today it is black letter law that computerized data is discoverable if relevant").
4. See *Federal Rulemaking*, [www.uscourts.gov/rules/#advspring05](http://www.uscourts.gov/rules/#advspring05).

### ACC Alliance Partners

The following ACC Alliance partners offer services related to e-discovery. Be sure to mention that you are an ACC Member when inquiring about their services to receive your Alliance discount:

**Cricket Technologies'** electronic discovery services help companies manage electronic data for litigation.  
[www.CricketTechnologies.com](http://www.CricketTechnologies.com)

**Jordan Lawrence Group** works with companies to implement records retention programs.  
[www.JLGroup.com](http://www.JLGroup.com)