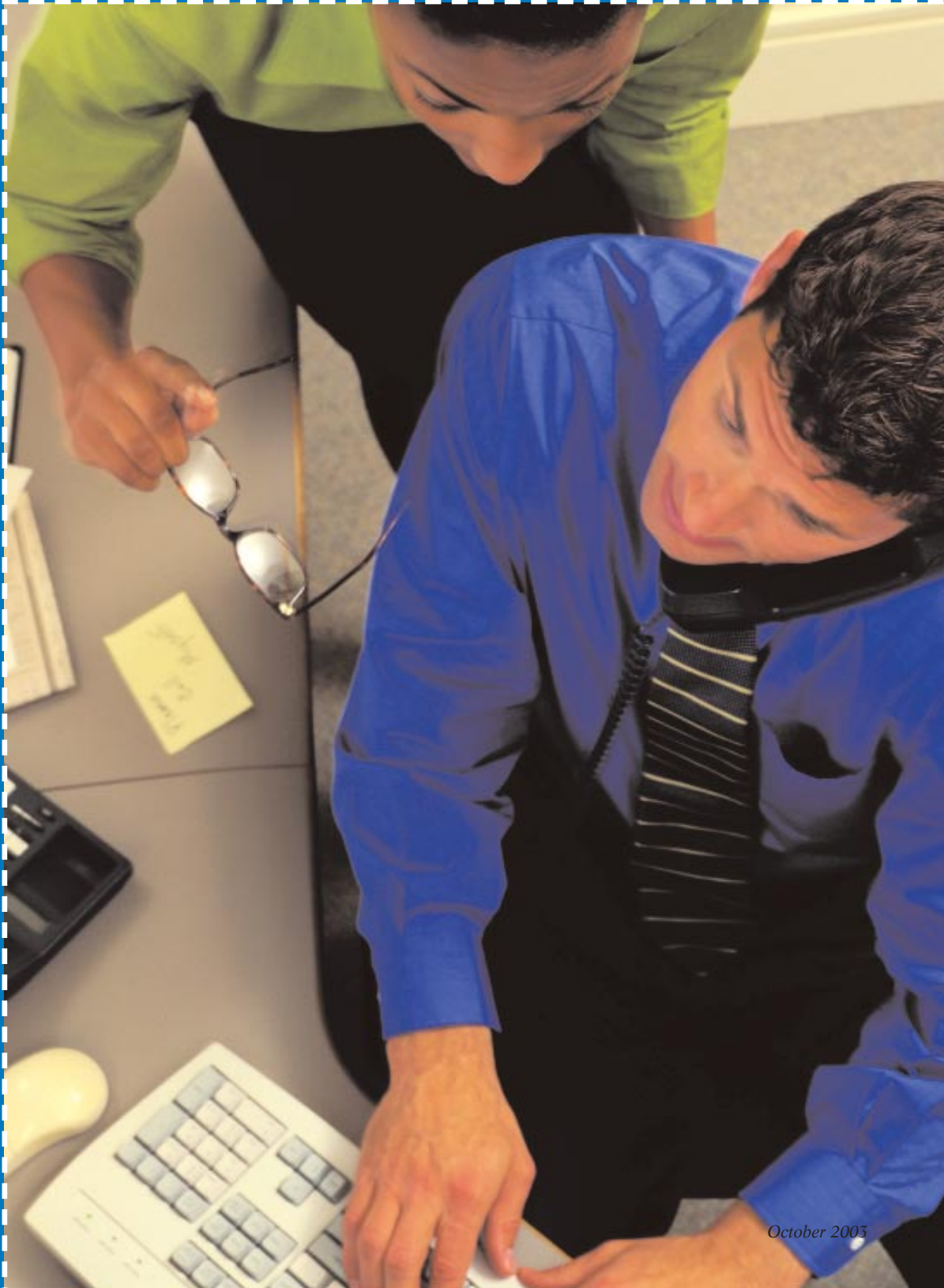


The next



discovery frontier

Preparing for Backup Data Requests

BY RICHARD J. CORBETT
AND VIRGINIA R. LLEWELLYN

Your company is named in a class action lawsuit in federal court. Plaintiffs' first document request seeks information from the company's computer systems dating back five years. Served with the document request is a Rule 30(b)(6) deposition notice, requiring testimony from the person most knowledgeable about your company's information technology ("IT") infrastructure.

You attended a CLE course about electronic discovery nearly a year ago, and you knew that the day would come when you would have to face these issues. Even though you recognized that your company was unprepared for electronic discovery, you took no action, attending to more urgent business. Now, with the electronic discovery request in hand, you must scramble to respond.

You call the chief information officer and learn that the company's backup protocols were completely overhauled last year in response to Sarbanes-Oxley concerns. You discover that the prevailing course of action since that time has been to retain nearly all electronic data to avoid the appearance of impropriety. A bit more investigation reveals that the company's IT groups in seven regional offices—in their zealous pursuit of compliance with the company's document retention plan—have retained more than 850 tapes consisting of various daily, weekly, and monthly backups.

Your law department works hard to enforce sound electronic document management protocols, but you dread the thought of putting your procedures to the test in court. The electronic discovery tidal wave is upon you. Where do you begin?

If you haven't already faced an electronic discovery request, you likely soon will. Some corporations escape relatively unscathed, with a request for a reasonable volume of information made by rational opposing counsel and overseen by a judge experienced in electronic discovery. Others do not fare so well, confronting demands by overly aggressive opposing counsel for years of information from backup tapes that a judge afraid to be resolute declines to limit. Still other corporations wait nervously for their first foray into the world of electronic discovery.

No matter which situation parallels yours, it is likely that you are not entirely satisfied with your company's level of preparedness for an electronic discovery request—particularly where backup data are at issue. In light of plaintiffs' increased discovery requests for backup information and the developing caselaw governing corporations' duties to preserve and produce electronic documents in litigation, in-house counsel must be familiar with their company's backup protocols and anticipate backup data requests. This article will help you prepare for such a request.



Richard J. Corbett is cofounder, executive vice president, and general counsel of Applied Discovery®, a Seattle-based developer of electronic discovery solutions. Previously, he was an attorney with Lucent Technologies, Inc., and Mosaix, Inc. He is available at richard.corbett@AppliedDiscovery.com.



Virginia R. Llewellyn is corporate counsel with Applied Discovery, Inc. A former litigator, she previously served on the board of ACCA's Washington State Chapter. She is a frequent speaker on the topic of electronic discovery. She is available at virginia.llewellyn@AppliedDiscovery.com.

TECHNOLOGY NUTS AND BOLTS

In the “early days” of electronic discovery—roughly 1995–1999—most requests for electronic information focused on documents stored on individual users’ hard drives or on company networks. As litigants’ technical knowledge increased, however, so did the scope of electronic discovery. Document requests now commonly seek production of backup information dating back several years and consisting of hundreds of thousands and even millions of pages of information. To respond effectively and properly to such requests, you must know some technological nuts and bolts.

Backup Procedures

A backup is a copy of information made generally for the purpose of disaster recovery in the event of a system failure or a natural disaster. You can create backups of computer data by using operating system commands or backup utilities. Backup programs often compress data, resulting in an unusually large volume of files stored in a relatively small amount of physical space. System backups are most commonly stored on tape, but also may be stored on other portable media, such as DVDs or CDs.

Backup tapes contain documents created by your company’s system users, such as email messages, word processing documents, and spreadsheets, but also commonly include copies of the computer’s operating system files. Opposing counsel usually are interested only in the documents created by your

system users. The presence of large system files on backups often distorts the actual volume of readable data. A volume of information that may seem intimidating at first glance may actually contain a manageable amount of readable data for purposes of the discovery process.

In order to assess the volume of readable data contained on a backup tape, you must consider the type of backup performed. Some common options include the following:

- Full backup, which backs up all information contained on the system. This type of backup is the simplest, yielding the most complete backup image.
- Selective backup, which selects specific files and directories for backup procedures. Selective backups avoid backing up unnecessary program or system files, focus on data files in known user directories, and effectively use limited backup space.
- Incremental backup, which copies only those files that have changed since the last backup. Incremental backup is like a selective backup, except that it copies only recently changed files, instead of copying files chosen on the basis of directory or file names. This method offers the time- and space-saving advantages of a selective backup while ensuring backup of all recently changed files.

Rotation and Recycling

Many companies perform a mix of full and incremental backups as part of their overall data management protocol. Throughout this process, backup tapes are typically rotated or “recycled” for storage of new data. The primary reason for recycling backup media is to avoid the expense of purchasing hundreds or even thousands of tapes. A sensible tape rotation plan also prevents unnecessary accumulation of multiple copies of the same data—another situation that can greatly increase a company’s costs if backup data must be reviewed in discovery.

Rotation results in destruction of older data as newer data are copied onto the media. Backup and rotation schedules can vary greatly, depending on the types and volume of files stored, the company’s level of technical and legal sophistication, and numerous other factors. The continuation of routine

tape recycling may give rise to spoliation issues in litigation, so you must understand your company's procedures well enough to be able to assess whether you should alter the procedures when litigation is pending or imminent.

ELECTRONIC DISCOVERY LAW

The stakes are high in electronic discovery. Typically, you will facilitate communications between your law department and outside counsel, as well as between your IT department and the electronic discovery service provider that you hire to help you gather and organize the data for review. A discussion of the service provider's role is beyond the scope of this article.¹ To assess the potential effect of electronic data storage on your company's litigation strategies, you must analyze the discovery rules and relevant caselaw in the context of your company's backup protocols.

Discovery Rules

With a few exceptions,² the discovery rules within the Federal Rules of Civil Procedure apply to electronic information in the same way that they apply to paper. Several provisions of the federal rules are particularly relevant to discovery of information from backup tapes, including the following:

- Rule 26(a)(1)(B). This rule requires each party to a lawsuit to disclose information about the existence and location of evidence that may be relevant, even before a discovery request issues.³ Your duty to investigate the physical location of potentially relevant information begins here. Fed. R. Civ. P. 26(a)(1)(B) requires you to state whether the information is stored in paper or electronic format. A court may find a violation of Rule 26 disclosure obligations if you do not provide such descriptive information at the outset of the case.⁴ You should consider the mandatory disclosure document an important part of both your offensive and your defensive litigation strategy, regardless of your posture in a case. Failure to identify electronic data favorable to your position at this juncture may preclude you from using it to support your claims and defenses later.
- Rule 26(f). Fed. R. Civ. P. 26(f) mandates that the parties make arrangements for Rule 26(a)(1)(B) disclosures and develop a proposed discovery plan. At the Rule 26(f) discovery conference, you should discuss the following matters:
 - Parameters for discovery of information from backup tapes.
 - Suggested guidelines for carrying out the parties' preservation obligations while litigation is pending, including possible suspension of routine backup procedures.
 - Request for a cost-shifting or cost-sharing protocol if you anticipate extraordinary discovery expenses.
 - Recommendations for narrowing the scope of electronic discovery requests, such as a suggestion to limit requests to certain date ranges, custodians, keywords, and so forth.
 - Format for document production.
- Rule 34(a). Fed. R. Civ. P. 34(a) defines "document" broadly to include information in any tangible format and any "electronic data compilations."⁵ After a discovery request has issued, electronic documents often take center stage. You must read any request for documents to include electronic data, even if not specifically stated.⁶ In-house counsel and outside attorneys are held to a high standard as they investigate the company's computer systems and system backups to determine the format of responsive documents.⁷
- Rule 30(b)(6). Another common vehicle for discovery of electronic information is a Rule 30(b)(6) deposition of a designated IT witness. A 30(b)(6) deposition generally seeks substantive information about systems and document management protocols and shapes further discovery.⁸
- Rule 26(b)(2). When parties cannot agree on the scope of discovery, Fed. R. Civ. P. 26(b)(2) provides protection from an unduly burdensome request.⁹ In electronic discovery, questions of undue burden and expense typically arise when a request calls for restoration of information from backup tapes or suspension of a company's routine document retention and destruction protocols. In such circumstances, producing parties often argue that the costs of production should shift to requesting parties. Courts' early electronic discovery decisions offered little relief for a corporate defendant under Rule 26(b)(2) and

put the burden of producing electronic information squarely on the shoulders of any company that “enjoys the benefit of technology.”¹⁰ Recent cases demonstrate a more moderate approach, acknowledging that electronic communications and storage are routine in nearly every business, not just large companies with deep pockets.¹¹ (See “Duty to Produce Backup Information,” below.)

ALTHOUGH RULINGS ABOUT THE DUTIES TO PRESERVE AND PRODUCE BACKUP INFORMATION ARE SOMEWHAT INCONSISTENT NATIONWIDE, COURTS GENERALLY APPLY A REASONABLENESS STANDARD IN DETERMINING WHETHER A PARTY HAS MET ITS DISCOVERY OBLIGATIONS.

Developing Caselaw

Although rulings about the duties to preserve and produce backup information are somewhat inconsistent nationwide, courts generally apply a reasonableness standard in determining whether a party has met its discovery obligations. Naturally, courts differ in their interpretation of what constitutes “reasonable.”

Duty to Preserve Backup Information

The duty to preserve evidence arises or increases when you (1) reasonably anticipate litigation, (2) receive prelitigation correspondence, or (3) receive service of a complaint, an answer, or a discovery request. Information contained on backup tapes is subject to this preservation duty. The measures that you must take to meet your obligations depend on several factors, including the jurisdiction and facts of your case, such as whether relevant evidence centers on a particular time period, and the specificity of document requests.

Some courts have ruled that a company’s failure to halt rotation of backup tapes immediately may be considered tantamount to destruction of evidence.¹²

Other courts have similarly held that spoliation sanctions may be appropriate when a party fails to preserve backup tapes that are the only source of relevant information.¹³ Courts may enter sanctions, even in the absence of an allegation of willful destruction, such as when routine recycling of backup tapes destroys backup information,¹⁴ or they may impose electronic discovery sanctions for ordinary negligence in the absence of bad faith.¹⁵ One court imposed an independent preservation duty on a company despite the fact that the requesting party had had notice of backup rotation procedures and the potential loss of relevant evidence and had failed to request specifically that the company halt those procedures.¹⁶

Affirmative requests for preservation of computer information are on the rise. At least one court has allowed injunctive relief requiring “freezing” of a party’s computer systems before a discovery request issued.¹⁷ Other courts have rejected the need for such relief in the absence of a showing that the company or its attorneys were likely to “flaunt their obligation under the federal rules” if they were not so ordered.¹⁸

Duty to Produce Backup Information

In August 2001, the U.S. District Court for the District of Columbia surveyed the caselaw about discovery of backup information and found “no controlling authority for the proposition that restoring all backup tapes is necessary in every case.”¹⁹ It adopted a “marginal utility analysis” for evaluating the costs associated with producing backup information. The court reasoned that, in cases in which it was likely that a backup tape would contain information relevant to a claim or defense, it would be fair to require the responding party to search at its own expense. The less likely it is that backup file production would yield relevant data, the more unjust it would be to make the responding party pay the costs of a search.²⁰ A number of other courts have observed this analysis.²¹

In May 2003, the U.S. District Court for the Southern District of New York applied the marginal utility analysis in the course of establishing a broader three-step analysis for deciding disputes about the cost and scope of electronic discovery.²² In a far-reaching decision, the court suggested that all electronic discovery disputes should be decided

From this point on . . .

Explore information related to this topic.

ONLINE:

- ACC's committees, such as the Law Department Management Committee, the Litigation Committee, and the Small Law Department Committee, are excellent knowledge networks and have listservs to join and other benefits. Contact information for ACC committee chairs appears in each issue of the *ACC Docket*, or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or windley@acca.com or visit ACCA OnlineSM at www.acca.com/networks/ecommerce.php.
- Applied Discovery, at www.applieddiscovery.com.
- Lisa M. Arent, Robert D. Brownstone, and William A. Fenwick, *E-Discovery: Preserving, Requesting and Producing Electronic Information*, 19 *COMPUTER & HIGH TECH L.J.* 131 (Dec. 2002), at www.fenwick.com/pub/lit_pubs/lit_pubs.htm.
- Berkman Center for Internet and Society at Harvard Law School, at <http://cyber.law.harvard.edu/digitaldiscovery/>.
- Richard Corbett and Virginia Llewellyn, "eDiscovery: Managing Digital Data with a Smart Document Retention Policy," *ACCA Docket* 19, no. 9 (October 2001): 18–37, available on ACCA OnlineSM at www.acca.com/protected/pubs/docket/on01/ediscovery1.php.
- Daticon, at www.daticon.com.
- "Electronic Discovery: Litigation and Antitrust Enforcement in a Digital Age," *ACCA Docket* 20, no. 2 (February 2002): 76–87, available on ACCA OnlineSM at www.acca.com/protected/pubs/docket/fm02/ediscovery1.php.
- Kroll Ontrack, at www.krollontrack.com.
- "Electronic Discovery: A How-to Guide for Litigators," at www.law.com/special/supplement/e_discovery/.
- Electronic Evidence Discovery, at www.eedinc.com.
- *Records Retention*, an ACC InfoPAKSM available on ACCA OnlineSM at www.acca.com/infopaks/retentent.html.
- Hon. Shira A. Scheindlin, and Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?* 41 *B.C.L. REV.* 327 (2000), at www.bc.edu/bc_org/avp/law/lwsch/journals/bclawr/41_2/03_FMS.htm.
- Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 *FED. CTS. L. REV.* 2 (2000), at www.fclr.org/2000fedctsrev2.htm. Withers, a research associate at the

Federal Judicial Center in Washington, DC, maintains a helpful website at www.kenwithers.com.

ON PAPER:

- Mary Kay Brown and Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 74 *PA. BAR ASS'N Q.* 1 (Jan. 2003).
- Corinne L. Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 *WASH. & LEE L. REV.* 257 (2000).
- Steven Lubet, *Document Destruction after Arthur Andersen: Is It Still Housekeeping or Is It a Crime?* 4 *J. APP. PRAC. & PROCESS* 323 (Fall 2002).
- Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material*, 64 *L. & CONTEMP. PROBS.* 253 (2000).
- Michael Marron, *Discoverability of "Deleted" E-Mail: Time for a Closer Examination*, 25 *SEATTLE U. L. R.* 895 (Spring 2002).
- Julius Melnitzer, *Keeping Track of the Invisible Paper Trail: What Legal Departments Can Learn from Boeing's Experience*, *CORP. LEGAL TIMES*, Feb. 2003, p. 15.
- Carey Sirota Meyer and Kari L. Wraspir, *E-Discovery: Preparing Clients for (and Protecting Them against) Discovery in the Electronic Information Age*, 26 *WM. MITCHELL L. REV.* 939 (2000).
- Mark D. Robins, *Computers and the Discovery of Evidence—A New Dimension to Civil Procedure*, 17 *J. MARSHALL J. COMPUTER & INFO. L.* 411 (1999).

AT ACC'S 2003 ANNUAL MEETING:

- Are you looking for even more information on this topic? If so, plan to attend ACC's 2003 Annual Meeting October 8–10 at the San Francisco Marriott. Visit www.acca.com/education03/am to learn more about the meeting.

If you like the resources listed here, visit ACC's Virtual LibrarySM on ACCA OnlineSM at 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 Staff Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or palmer@acca.com. If you have resources, including redacted documents, that you are willing to share, email electronic documents to Managing Attorney Jim Merklinger at merklinger@acca.com.

in the context of whether data are “accessible” or “inaccessible” and recommended a seven-step test for determining when a party must produce inaccessible data, including backup tape data, and which party should pay for the production.²³

In another recent case, the Second Circuit reversed a jury verdict after having specifically examined the veracity of a company’s claims that it could not recover data stored on backup tapes.²⁴ The appeals court found that the trial court had not fully evaluated one party’s claims of months of purported technical difficulties in recovering emails from the time period at issue. The court determined that the company’s contentions, which continued past the start of trial, drew suspicion in light of the opposing party’s consultant’s ability to recover 950,000 emails from the relevant time in just four days.²⁵ This case highlighted the importance of blending legal expertise with competent electronic discovery technical assistance.

In the most extreme case reported to date, a federal district court in New York granted judgment against a defendant because of its wholesale failure to “establish a coherent and effective system to faithfully and effectively respond to discovery requests.” Among the shortcomings noted by the court was a lapse in counsel’s duty to “cause a retention policy to be adopted to prevent destruction of responsive documents, both paper and electronic.”²⁶

ANALYSIS OF YOUR COMPANY’S BACKUP PROTOCOLS

When anticipating litigation, you must consider whether you will have to preserve, review, and potentially produce certain backup information. It is more prudent, however, to analyze your company’s backup protocols outside of a lawsuit’s context. The following questions will serve as a starting point for understanding your company’s backup protocols, schedules, the volume of information stored, and the location of data that could be responsive in litigation, and armed with the answers, you will be able to guide your company effectively when litigation is imminent:

- **Does your company have a prescribed backup protocol?** If your company’s backup procedures

are in writing, you should obtain a copy of them and determine whether the IT department is observing the protocol. Do not assume that written guidelines are an accurate reflection of actual practices; variances are common in most companies. If protocols are not in writing, determine which company employees are responsible for backup procedures. Regardless of whether written guidelines exist, you should interview these employees to gain an understanding of backup procedures. In addition, you should identify at least one key IT employee to be responsible for a 30(b)(6) deposition. See the sidebar on page 127, “Rule 30(b)(6) Deposition Questions,” for details about the knowledge and information that this employee should have and be able to discuss.

- **What is your company’s backup schedule?** A typical backup schedule includes a full backup once a week, with incremental backups performed to capture new data on other days. At the end of each month, one monthly backup usually replaces the previous four weekly backups. The tapes that created the daily and weekly backups may then be rotated or recycled for storage of new data. At the end of a year, a company typically has 12 full monthly backups and, ideally, no other incremental or partial backups. Whatever your company’s schedule, you must determine whether staff observes it rigorously or whether variances are common. You also should gather information to calculate the burden—financial and otherwise—to your company in the event that it must suspend its usual recycling procedures in anticipation of litigation. Monies required for the purchase of replacement tapes, tape storage, and other incidental expenses can quickly add up to substantial sums.
- **Where are your company’s backup data stored?** Many companies store more than one copy of backup data. If your company does so, you should determine the location for each copy. Companies frequently keep backups locked in locations separate from their primary place of business. Ask your IT department about offsite storage, as well as the use of any “interim” storage facilities. You do not want to be surprised in the course of litigation by the appearance of backup media that employees forgot.

- **Does your company have a document retention plan for electronic data?** A document retention plan prescribes the practices by which your company elects to retain and destroy certain kinds of documents—both paper and electronic—in the ordinary course of business. It gives the company’s records managers and IT personnel guidelines for carrying out their duties and protects the company from the burdensome accumulation of massive amounts of unnecessary data. When drafted and enforced correctly, a document retention plan also can shield the company from extraordinary burden and expense in responding to a discovery request by ensuring that it keeps only those documents that it is required to keep for business or legal purposes.²⁷ All document retention plans should be drafted with prelitigation obligations in mind, including the duty to preserve records pursuant to federal regulations, such as Sarbanes-Oxley, the Fair Labor Standards Act, the Health Insurance Portability and Accountability Act, the Occupational Safety and Health Act, and so forth, and their state law equivalents.²⁸ Companies commonly create a task force dedicated to considering these prelitigation business obligations and drafting a plan suited for those needs. Daily, weekly, and monthly backup rotations—and the concurrent recycling of backup media and resulting destruction of company documents—are acceptable practices as long as there is no affirmative legal duty to preserve the data. Many companies unwittingly store millions of pages of unnecessary information simply because no one has analyzed and updated their document retention practices. If your company has a formal electronic document retention plan, you should examine the guidelines that apply to the IT department and immediately determine whether the staff is observing them. If no document retention plan is in place, meet with IT staff to determine whether data are commonly overwritten or otherwise deleted in accordance with the company’s backup protocol. An electronic document retention plan must include a procedure for notifying the IT staff when it must halt the recycling of backup tapes on the daily, weekly, or monthly schedule. Sound prelitigation practices should enable your company to stop document destruction immediately while you assess the needs of a case.

DATA RETENTION IN ANTICIPATION OF LITIGATION

There is no secret recipe for mixing sound business judgment, legal acumen, and fiscal responsibility to craft the perfect electronic data management plan in anticipation of litigation. But courts do not expect perfection. In almost all cases, they simply want to see a demonstration of well-reasoned, legally defensible business practices.

Notification

When litigation is pending or imminent, you must immediately notify those employees who are responsible for enforcing data backup procedures and rotation schedules. Many companies make the mistake of waiting to involve the IT department until after an electronic document request has issued. By that time, spoliation—usually unintentional—may already have occurred.

Your notification to the IT staff should include the following elements:

- Written notice of the pending or imminent legal action.
- Identification of physical company locations, particular custodians, or time periods known to be at issue.
- Clear instructions on whether to immediately suspend or continue routine rotation practices.
- Any other company-specific logistical directives to ensure that IT staff does not destroy or overwrite relevant data while the legal team determines the most prudent plan for proceeding. (See “Strategies,” below.)

Time is of the essence for this first notification. A delay as brief as even one day can result in accusations of spoliation if backup tapes are recycled or discarded. If you carry out a simple communication plan like this one, you will position your company favorably when a court examines the reasonableness of your company’s document preservation actions.

Suspension of Backup Tape Rotation

The most conservative approach to document retention during litigation would dictate immediate halting of backup tape rotation at the first sign that you might need to do so. Thus, your notification to the IT department should include a directive to freeze all tape recycling. The company’s backup protocol then would occur as usual except that every

RULE 30(B)(6) DEPOSITION QUESTIONS

Your designated IT deponent should be able to answer questions about the following aspects of your IT system:

ORGANIZATIONAL STRUCTURE

- Identities of all current and former personnel who had access to network administration, backup, archiving, or other system operations during any relevant time.
- Company's use of third parties for maintenance and service of computer systems.
- Role that the deponent has had in the past or will have in the current case in responding to electronic discovery requests.

RECORDS MANAGEMENT AND DOCUMENT PRESERVATION

- Instructions about preservation of electronic documents relevant to the lawsuit:
 - Who provided notification of pending litigation.
 - How notification was disseminated.
 - What procedures were in place for verification of receipt and so forth.
- Deletion of any electronic documents since the lawsuit commenced or since the deponent received notification about pending or imminent litigation.
- Company's electronic records retention plan:
 - When it began.
 - Who manages the plan.
 - What enforcement or auditing procedures are in place.
 - How the company trains IT employees with respect to the plan and so forth.
- File-naming and location-saving conventions.

ALTERNATIVE SOURCES OF ELECTRONIC INFORMATION

- Any regular destination locations for electronic documents outside of the company, including employees' home computers, as well as other business entities.

- Details about the company's website:
 - Content developers.
 - Revision intervals.
 - Access by third parties and so forth.

BACKUP PROCEDURES

- Details about company's backup procedures:
 - Intervals.
 - Media.
 - Recycling of backup media.
 - Location of backups.
- Description of backup procedure modifications made to comply with earlier discovery requests.
- Destruction or recycling of any backup tape since the lawsuit's filing.
- Backup tape labeling conventions (to identify relevant time periods).

HARDWARE

- Number, types, and locations of computers.
- Details about disposal/recycling/sale of hardware.
- Procedures for departing employees, including the copying and storage of their data and the "wiping" of their hard drives.

SOFTWARE AND EMAIL

- Application software in use on desktops and laptops.
- Identification of any legacy systems in use during relevant time period.
- Details about digital storage of company voicemail.
- Details about use of personal digital assistants, such as BlackBerries and Palm Pilots.
- Details about email retention:
 - Retention period.
 - Auto-delete features.
 - Deletion instructions given to employees and so forth.

backup would be a new tape. Depending on the size of your company, the number of physical locations of business operations, and the rate at which data are created, this change could translate into the creation of dozens and even hundreds of new tapes every day during the pendency of the litigation.

ALTHOUGH YOU INITIALLY MAY BE RELUCTANT TO TALK WITH THE OPPOSITION ABOUT BACKUP DATA, HOPING THAT THE REQUEST FOR SUCH DATA WILL NEVER ARISE, THE CONSEQUENCES OF FAILING TO ADDRESS THE SUBJECT WITH OPPOSING COUNSEL CAN BE DISASTROUS.

A less conservative—but still prudent—approach would include temporary cessation of recycling, followed by a careful analysis of whether recycling should continue with regard to information from certain locations, certain network servers, or for certain time periods unrelated to the anticipated legal action. This approach also should include an early effort to secure opposing counsel’s agreement about the scope of backup information that will be at issue and a stipulation that your company’s actions with regard to preservation of backup information are sufficient. In the absence of such an agreement, a request for court intercession would ensure that the court and opposing party are put on notice of your company’s intended plan. This notice would weaken any later allegation that the company had engaged in negligent or intentional spoliation.²⁹

The least cautious approach would entail continuation of customary backup procedures and rotation schedules until otherwise ordered. Although some courts might find no problem with this tactic—so long as the fundamental obligations of the discovery rules were observed³⁰—there is a significant likelihood that spoliation allegations would arise at a later date.³¹

STRATEGIES IN LITIGATION

The federal court system consists of more than 1,200 district and magistrate judges who regularly face complex legal issues in more than 250,000 civil cases pending at any given time. With this extraordinary workload, judges have little patience for routine discovery disputes. If you take an active approach to electronic discovery issues, you will have a significant positive effect on your company’s position in litigation. The strategies set forth below will help you make the early decisions that will profoundly affect your company’s financial and human resources while a case is pending:

Anticipate Requests for Backup Data

Although you initially may be reluctant to talk with the opposition about backup data, hoping that the request for such data will never arise, the consequences of failing to address the subject with opposing counsel can be disastrous. In many cases, backup data will not play a significant role, and you will be able to resume routine practices very quickly. In the situations in which backup data are important, however, your failure to raise the issue, as discussed in “Developing Caselaw,” above, can have devastating consequences, including significant monetary penalties, an adverse inference jury instruction, or even a directed judgment. It is important to give your outside counsel information about your company’s backup protocols so that they will be able to confer with opposing counsel about electronic discovery and potential backup issues early in the case.

Prepare an Action Plan

You should document the backup protocol that you will observe in the lawsuit. This action plan should include the following elements:

- Procedures for giving IT staff appropriate directives with regard to halting tape recycling.
- Procedures for notifying all employees of essential document preservation duties.
- List of case-specific factors to be considered in determining whether routine recycling activities must be halted and when they may resume.
- Process for involving outside counsel in decisions about any variance in standard backup protocols.
- Method for providing notice of your document preservation activities to opposing counsel.

You also must plan how you will access and review backup information that is deemed potentially responsive in a case. This critical step is often overlooked in planning stages, but can have a considerable effect on your overall litigation strategy. You need an effective method for reviewing information from backup tapes to identify only those documents that you must produce. Leveraging available electronic discovery technologies through your service provider, your legal team should be able to review backup data in electronic format without spending the time and money to print the documents for manual review. You will want to search rapidly for relevant information and set aside irrelevant documents, which constitute the vast majority of materials contained on backup tapes.

In the event that the opposition raises spoliation issues or otherwise questions your strategy with regard to backup data, the details outlined in your action plan will serve as valuable evidence of your company's efforts to diligently discharge all discovery obligations.

Meet and Confer


The discovery mantra of judges around the country is the same: "Meet and confer." Few things harm a litigant's position in a case more than a demonstrated unwillingness to meet and confer about the potential areas for disagreement in discovery. Your outside counsel will be much more confident in carrying out the duty to confer with opposing counsel if you have included outside counsel in your action plan from the outset. In-house and outside counsel can then present an organized, unified front in addressing any issues related to discovery of backup data.

Seek Guidance from the Court

Discovery is contentious in many cases, and opposing counsel may be unwilling to agree to a proposed plan. If this situation arises, you would be wise to seek guidance from the court rather than to wait for a motion to compel. Courts look with favor on a party that is aware of its electronic discovery obligations and has taken necessary steps to educate everyone involved about the relevant issues in a case. The simple act of setting forth an electronic discovery action plan and seeking approval from the court will make a significant difference in your company's position if discovery disputes arise.

CONCLUSION

The opening hypothetical illustrates a situation that could happen to any company. Its outcome depends in large part on the amount of advance work done by in-house counsel.

First, you must understand the basic nuts and bolts about the technology involved in creating backup data, as well as your company's specific backup policies and tape recycling procedures. Second, you should analyze the company's practices in light of the discovery rules applicable to backup data and the developing caselaw governing retention and production of backup information. This information will enable you to determine whether your company should alter its backup and rotation procedures when litigation is pending or imminent. Third, you should outline strategies and prepare an action plan for handling a backup data request so that you have a comprehensive, legally defensible discovery approach. Companies that demonstrate a sincere effort to address these issues at the outset should fare well in any jurisdiction. 

NOTES

1. See Richard Corbett and Virginia Llewellyn, "eDiscovery: Managing Digital Data with a Smart Document Retention Policy," *ACCA Docket* 19, no. 9 (Oct. 2001): 18-37, available on ACCA OnlineSM at www.acca.com/protected/pubs/docket/on01/ediscovery1.php. The following companies can assist you in the process of identifying, retrieving, reviewing, and producing electronic information:
 - Applied Discovery, Inc., www.applieddiscovery.com.
 - Electronic Evidence Discovery, www.eedinc.com.
 - Daticon, www.daticon.com.
 - Kroll Ontrack, www.krollontrack.com.
2. The following courts have implemented rule changes with regard to electronic discovery: (1) federal courts for (i) the District of Wyoming, via U.S.D.C.L.R. 26.1(d), which requires parties to file a Rule 26(f) report that includes specific information related to electronic discovery; (ii) the Eastern and Western Districts of Arkansas, via Local Rule 26.1(4), requiring counsel, in preparation for a Rule 26(f) conference, to disclose whether he/she will ask any party to disclose or produce information from electronic or computer-based media or information about the anticipated scope and cost of electronic discovery; and (iii) the Middle District of Florida, Local Court Rule 3.03(f), requiring attorneys to use technology to the maximum extent possible in all phases of litigation; and (2) state courts in California, Illinois, and Texas. California provides

that discovery may be conducted in electronic media and by electronic communication and authorizes courts to enter orders regarding use of technology in discovery. (Code of Civil Procedure §2017.) Illinois defines “document” to include all retrievable information in computer storage and provides a mechanism for requesting production of information from computer storage. (Illinois Supreme Court Rules 201(b)(1) and 214.) Texas determines that only responsive information “reasonably available to the responding party in the ordinary course of business” must be produced. The responding party has an opportunity to object to any request calling for information that it cannot produce by “reasonable efforts.” If the court then orders production, it must order that the requesting party pay costs of “extraordinary steps” required for production. (Tex. R. Civ. P. 196.4.)

3. Fed. R. Civ. P. 26(a)(1)(B) states:
 - (1) Initial Disclosures. Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties: . . . (B) a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment
4. See *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437 (D.N.J. Feb. 4, 2002).
5. See FED. R. CIV. P. 34, “Notes of Advisory Comm. on 1970 Amendments to the Rules.”
6. See *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355, *4 (S.D.N.Y. Nov. 3, 1995) (“It is black letter law that computerized data is discoverable if relevant”).
7. See *GTFM, Inc. v. Wal-Mart Stores, Inc.*, No. 98 Civ. 7724, 2000 U.S. Dist. LEXIS 16244 (S.D.N.Y. Nov. 9, 2000). Relying on information from a senior executive, Wal-Mart’s counsel told the court and opposing party that the company’s computers could not produce information aggregated as the plaintiffs had requested. As a result, Wal-Mart produced a large volume of nonresponsive information for plaintiffs’ review. It came to light later in the deposition of Wal-Mart’s vice president of Management Information Systems (“MIS”) that the company could have produced the information as requested. The court sanctioned Wal-Mart, noting specifically that the MIS vice president was an obvious person for counsel to have contacted firsthand upon receiving a document request. See also *Tulip Computer Int’l v. Dell Computer Corp.*, 2002 U.S. Dist. LEXIS 7792 (D. Del. Apr. 30, 2002).
8. See, e.g., *Alexander v. FBI*, 188 F.R.D. 111 (D.D.C. 1998) (court permitted deposition to learn about email systems and system for acquisition, location, and disposition of computers to guide substantive discovery); *Carbon Dioxide Industry Antitrust Litigation*, 155 F.R.D. 209, 214 (M.D. Fla. 1995) (court ruled depositions aimed at acquiring information about data maintained on defendants’ computers, as well as hardware and software needed to access the information, necessary to proceed with substantive discovery).
9. FED. R. CIV. P. 26(b)(2) states in part:

The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).
10. See, e.g., *Linnen v. A.H. Robins Co.*, 1999 Mass. Super. LEXIS 240, *17-18 (Jun. 16, 1999); *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 U.S. Dist. LEXIS 8281, *5-6 (N.D. Ill. Jun. 15, 1995).
11. See *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001) (marginal utility analysis). See also *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002) (adopting a balancing approach considering eight factors); *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 U.S. Dist. LEXIS 3196 (E.D. La. Feb. 19, 2002) (using the factors set forth in *Rowe* to determine that plaintiff should bear costs of producing emails responsive to its own requests).
12. See, e.g., *Linnen*, 1999 Mass. Super. LEXIS 240 at *32-33 (granting spoliation sanctions, including a jury instruction permitting the inference that defendant had destroyed potentially relevant evidence because the evidence was unfavorable).
13. See *Applied Telematics, Inc. v. Sprint Communications, Co.*, 1996 U.S. Dist. LEXIS 14053, at *10-11, 14 (E.D. Pa. Sep. 17, 1996) (granting plaintiff’s motion for adverse inference instruction on spoliation and for spoliation sanctions; also awarding reasonable attorneys’ fees and costs).
14. *Id.* at *11.
15. See *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002).
16. See *Applied Telematics*, 1996 U.S. Dist. LEXIS 14053 at *11.
17. See *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley*, 2003 Cal. App. LEXIS 171 (Cal. App. 4 Dist. 2003).

-
18. See *Madden v. Wyeth*, 2003 U.S. Dist. LEXIS 6427, *3 (N.D. Tex. Apr. 16, 2003).
 19. McPeck, 202 F.R.D. at 33.
 20. *Id.* at 34.
 21. See, e.g., *Byers v. Illinois State Police*, 2002 U.S. Dist. LEXIS 9861 (N.D. Ill. May 31, 2002); *Antioch Co. v. Scrapbook Borders, Inc.*, 201 F.R.D. 645, 652 (D. Minn. 2002).
 22. *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y., May 13, 2003).
 23. *Id.* at *43.
 24. *Residential Funding Corp.*, 306 F.3d at 113.
 25. *Id.* at 112–15.
 26. *Metro. Opera Ass'n v. Local 100, Hotel Empl. & Rest. Empl. Int'l Union*, 2003 U.S. Dist. LEXIS 1077, at *5–6 (S.D.N.Y., Jan. 28, 2003).
 27. See *Corbett and Llewellyn*, *supra* note 1, at 25–24.
 28. See *Christopher V. Cotton, Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 IOWA J. CORP. L. 417, n. 22, at *8 (Winter 1999) (discussing retention periods under antitrust laws, OSHA, FLSA, and ERISA).
 29. *But see Applied Telematics*, *supra* note 13 (even when a requesting party has notice of backup rotation procedures and the potential loss of relevant evidence and fails to request specifically that a company halt those procedures, the court may require a company to observe an independent preservation duty).
 30. See *Madden*, 2003 U.S. Dist. LEXIS 6427 at *5.
 31. See, e.g., *Applied Telematics*, 1996 U.S. Dist. LEXIS 14053 at *10–11.
-