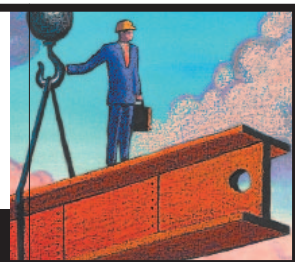


Litigation Support A Special Report

## Bone Up on Backup

Courts are getting tough when it comes to searching backup tapes.



BY ATIBA D. ADAMS AND MICHAEL R. FINLEY

**T**he law on electronic discovery is developing rapidly. In the past few months, federal courts have issued several groundbreaking decisions against parties for discovery misconduct or negligence. And the U.S. District Court for the District of Columbia has developed a pioneering “marginal utility” analysis for determining when information from backup media must be restored in an effort to locate potentially responsive documents.

Sanctions for failing to preserve and produce data from backup tapes have ranged from monetary penalties to adverse jury instructions and judgment on the merits. In recent cases, attorneys have been required to demonstrate that personal attention was paid to the proper identification and review of information stored on clients’ computer systems.

The greater emphasis on electronic documents means that companies must have a sensible plan for the retention, identification, review, and production of information stored on backup tapes. It also means that litigators should have a basic understanding of backup protocols and procedures.

A backup tape is a copy of information, generally made for the purpose of disaster recovery in the event of a system failure or natural disaster. Backups of computer data may be created with operating system commands or through use of a backup utility. Backup programs often compress data to reduce the amount of physical space required on the backup media. The result of this compression is that unusually large volumes of files may be stored in a significantly smaller amount of space.

Backup tapes typically contain documents created by system users—e-mail messages, word processing documents, spreadsheets, database entries, and the like—but also often include copies of the system files required to make the computer’s operating systems function properly. Attorneys generally are interested only in the actual documents created by the company’s computer users, but it’s important to understand the nature of other types of files that may be on a system backup.

A volume of information that may seem enormous at first glance usually contains a manageable amount of readable data for purposes of discovery. To gauge how much data is contained on a backup tape, you need to know what kind of backup was performed:

**Full backup.** A complete backup of all information contained on the system. This is the simplest type of backup, and it yields the most complete backup image.

**Selective backup.** Specific files and directories are selected for backup procedures when backup space is limited, or to avoid backing up unnecessary program or system files and to focus on data files in known user directories.

**Incremental backup.** Only those files that have changed since the last backup are copied. This procedure is like a selective backup, but the files are selected automatically based on whether they have changed recently, instead of being arbitrarily selected based on directory or file names. This method offers the time- and space-saving advantages of a selective backup while ensuring that all changed files are included.

A mix of full and incremental backup is common in many companies. Backup schedules and rotation of tapes depends on the type and volume of files stored, the company’s level of sophistication with regard to technical (and legal) matters, and numerous other factors.

### REVIEWING BACKUP PROTOCOL

In preparing any discovery response, you must ask about information stored on backup tapes. The following questions will serve as a starting point for understanding the company’s backup protocol, schedules, volume of information stored, and location of information that could be responsive in litigation.

- Does the company have a formalized backup protocol?

If formalized in writing, obtain a copy, and determine whether the written protocol is followed. If not set forth in writing, determine which company employee is responsible for backup procedures and immediately interview the employee to understand the

backup protocol. This employee also should be prepared for the likelihood of a 30(b)(6) deposition.

- What is the company's backup schedule?

A typical schedule might include a full backup once per week, with incremental backup performed to capture new data on other days. At the end of each month, the weekly backups for the month might be replaced with one complete monthly backup. The tapes used to create the weeklies may then be put back into rotation (or "recycled") to store new data. This procedure is typically followed annually, so that the company ends each year with 12 full monthly backups, and, ideally, no other incremental or partial backup.

Determine whether the schedule is followed rigorously or whether variances are common.

Find out what would be the burden (financial and otherwise) to the company if it must suspend its process of rotating or recycling backup tapes. This will usually involve increased costs for the purchase of replacement tapes, tape storage costs, and other incidental expenses.

- Does the company have a provision in its backup protocol for adhering to a document retention plan for electronic data?

The IT department's definition of a "retention plan" (the period of history covered on backups) is likely very different from the legal definition of "document retention." An early conversation with the company's IT staff will help prevent confusion on this vital issue.

Ask whether the company has a formal document retention plan. If so, obtain a copy of any written guidelines and immediately determine whether they are being followed.

If no document retention plan is in place, meet with technical staff immediately to learn whether computer data is being overwritten or otherwise deleted in accordance with the company's backup protocol. Be sure that procedures are in place to avoid any claims of negligent or intentional spoliation.

A document retention plan typically includes a procedure for halting the rotation or recycling of backup tapes on the daily, weekly, or monthly schedule, to avoid claims of spoliation. Consider the company's practices and immediately determine whether the usual procedures must be interrupted so that no potential evidence is destroyed.

- Where is the company's backup data stored?

Many companies store more than one copy of backup data. If this practice is followed by your client, find out where each copy is stored.

Ideally, backups are kept locked in a location away from the company's primary place of business. Ask about offsite storage as well as any "interim" storage facilities.

## RESPONDING TO DISCOVERY REQUESTS

Once you have a working knowledge of the company's backup practices, you are prepared to consider the legal issues relevant to discovery of information from the backup tapes. Although court rulings regarding duties related to the identification, preservation, and production of information contained on backup tapes are somewhat inconsistent around the country, courts will generally apply a reasonableness standard in determining whether a party has met its discovery obligations. Unfortunately, the interpretation of "reasonable" varies from court to court.

For example, when a company follows a longstanding "document retention and destruction policy" by which it regularly recy-

cles backup tapes, one judge may find it reasonable for the company to continue to recycle backup tapes in the absence of a specific preservation order or discovery request, while another judge may determine that the usual procedures must be halted once the party is on notice of litigation. Prepare for the possibility of either ruling.

**1. Anticipate requests for backup data.** The best way to avoid a discovery dispute concerning information on backup tapes is to prepare for all possibilities. Armed with information about the company's backup protocols, you will be ready to confer with opposing counsel about the electronic discovery issues in the case.

While you may initially be reluctant to raise the issue of backup data to opposing counsel (hoping that the request for such data will never arise), the consequences of failing to address the issue early in the case can be disastrous. In fact, the "mandatory disclosure" provision in Fed. R. Civ. P. 26(a)(1) specifically requires parties to identify, in advance of a discovery request, any computer-based information that may be used to support the party's claims or defenses in the case.

**2. Document your electronic discovery plan.** Once you understand the client's backup procedures, it is wise to document the protocol you will follow in conducting electronic discovery. This plan should include an outline of the electronic discovery issues considered, employees consulted, and conclusions reached. If you determine that the client can continue its regular backup procedures (including recycling tapes on a predetermined schedule), be prepared to defend the decision. Likewise, if you determine that regular procedures must be halted, be ready to provide information about the potential costs to the company.

You will be better positioned to seek relief from undue burden and extraordinary costs if you are well-informed about the company's backup protocols and can present opposing counsel with a proposed plan for handling electronic data in discovery. The best-case scenario is when all parties agree to electronic discovery protocols early in the case.

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

Recent federal court rulings underscore the importance of a coordinated plan for electronic document discovery. While natural instincts typically prevent attorneys from delving too deeply into technical matters, in nearly every case, a basic understanding of the nature of the information stored on backup tapes is essential to the preparation of an effective discovery response.

---

*Atiba D. Adams is corporate counsel for Pfizer Inc., where he manages product liability and commercial litigation matters. He can be reached at atiba.d.adams@pfizer.com. Michael R. Finley is an attorney in the D.C. office of Applied Discovery Inc. He formerly practiced in the Washington office of Crowell & Moring. He can be reached at mike.finley@applieddiscovery.com. The views expressed here are the personal views of the authors and are not intended to reflect the views of any organization or entity.*