

# A 30(b)(6) Can Sink Your Ship

Good records management policies and knowledge of the law will help records managers keep their companies afloat in the face of possible litigation

**Kirke Snyder, JD, and David Isom, Esq.**

In several recent court cases, corporate IT representatives have incorrectly testified under oath that their company positively had or did not have certain potentially relevant documents or other data. When the truth was revealed in court that their original testimony was not accurate, the judge handed out stiff fines and other damaging sanctions. In a more recent case, Morgan Stanley's sanction for failure to preserve and produce certain electronic records contributed to an adverse \$1.4 billion damages judgment. *Coleman v. Morgan Stanley*, 2005 WL 679071 (Fla. Cir. Ct. March 1, 2005); 2005 WL 674885 (Fla. Cir. Ct. March 23, 2005)

Why are we seeing more and more court sanctions imposed against companies for failure to meet their litigation discovery obligations? A lack of preparation, a sharp attorney, or even a mediocre IT background, can make the most experienced IT or records and information management (RIM) staff look incompetent, or worse, deceptive.

## 30(b)(6) Deposition

Federal Rule of Civil Procedure 30(b)(6), as well as the corresponding state rules, are the new "weapon of

choice" in the battle for electronic discovery, and IT directors and RIM managers are in the cross-hairs of the controversy. Rule 30(b)(6) requires a company faced with electronic discovery to designate one or more officers, directors, managing agents, or other persons to testify under oath as to matters known or reasonably available to the organization, e.g., information management and document retention. Depending upon the counsel's goal and strategy, the questioning may be used for routine information gathering or rather it may be aimed at uncovering intentional or negligent spoliation of data potentially relevant to the litigation.

These 30(b)(6) depositions can be a nightmare for the unprepared because the court now places a big burden on

companies to save potentially relevant documents and other data when they face the threat of litigation. A court may impose severe monetary sanctions against a company whose representative testifies that certain documents have been retained when they in fact have been destroyed or who testifies that certain documents were destroyed when they in fact were not destroyed. This means that a company must have reliable systems in place to know what documents have been retained and what documents have been destroyed.

## Duty to Preserve

A legal duty to retain documents may arise from a number of sources, including:

### 1. Statutes and Regulation

- Internal Revenue Code
- State and federal environmental statutes
- Labor and employment laws
- Criminal statutes that punish obstruction
- Sarbanes-Oxley Act of 2002 and related SEC regulations, which, among other requirements, man-

### At the Core

This article

- ▶ Describes the importance of a 30(b)(6) deposition
- ▶ Explains the possible spoliation sanctions
- ▶ Offers questions to help RIM managers prepare their companies for possible litigation

date that auditors maintain workpapers and other audit or review records for seven years from the conclusion of the audit or review

- Industry-specific statutes and regulations that impose unique document retention requirements
- USA PATRIOT Act and related regulations, which impose obligations for financial institutions, such as banks and credit unions, to collect and maintain information relating to customers, customer accounts, and certain types of transactions

## One of the most important common law document retention obligations arises out of the doctrine of "spoliation."

- Statutes of limitations that indirectly impose document retention obligations by making certain documents, such as contracts and personnel files, relevant to potential disputes that may remain dormant until the statutory period for bringing suit passes

### 2. Contracts

Many contracts contain provisions requiring that certain materials be preserved for future use. For example, consulting agreements frequently require the consultant to retain analyses and data prepared as part of the contract for a specified period of time.

### 3. Common Law and Judicial Prerogative

Court decisions may also impose duties to retain documents. One of the most important common law document retention obligations arises out of the doctrine of "spoliation," which is the improper destruction of evidence relevant to a pending or reasonably foreseeable lawsuit or legal proceeding.

This is a very important concept for RIM and IT managers because the penalty for spoliation can call for both civil (money) and criminal (jail) consequences. A company has a duty to preserve documents relevant to the issues in a governmental investigation, audit, or civil action as soon as the company knows that the investigation, audit, or action has been commenced or is reasonably likely. Prudent attorneys will advise clients to preserve electronic evidence once a conflict reaches the stage that litigation appears likely.

The essential elements of negligent spoliation are:

- Existence of a potential civil action
- A legal, regulatory, or contractual duty to preserve evidence that is relevant to the potential civil action
- Destruction or alteration of that evidence
- Significant impairment in the ability to prove or defend the lawsuit
- Causal relationship between the evidence destroyed and the inability to prove or defend the lawsuit; and resulting damages

Note that a company must be in compliance with the vast array of regulatory agency retention requirements or risk the potential sanctions of spoliation.

There are several possible spoliation sanctions. These include dismissal, issue preclusion/preclusion of expert, adverse inference, and criminal sanctions.

#### *Dismissal*

A judge has the authority to dismiss a case if the parties have failed to preserve crucial evidence. For example, in the case

of *Restaurant Mgmt. Co. v. Kidde-Fenwal Inc.* (N.M. 1999), the restaurant brought a claim for breach of implied warranty and negligence against Kidde-Fenwal, a company that inspected, repaired, and manufactured a fire suppression system. The fire suppression system allegedly failed allowing a grease fire in a restaurant to become more destructive than it should have been. Before filing suit, the restaurant allowed the fire suppression system to be destroyed during renovation of the restaurant. After learning of the loss of the fire suppression system, defendants moved for summary judgment or dismissal. The trial court granted the motion because the restaurant had permitted the destruction of evidence that should have been preserved.

#### *Issue Preclusion/Preclusion of Expert*

This sanction forbids the spoliating party from using specific evidence or bringing issues before a jury. Generally, it is used when one party's expert has had an opportunity to view the item in question and in the process has destroyed it, altered it, or misplaced it. In short, courts have determined that it is simply inherently unfair to allow one party to have an expert testify to an item that he has had the opportunity to examine and then, through that party's own misconduct, prevented the opposing party from having the same opportunity.

#### *Adverse Inference*

As an alternative to dismissal or issue/expert preclusion, a jury may be instructed to presume that the evidence, if produced, would have been adverse to the party who destroyed it. For such an instruction to be given, there must be a connection between the inference and the lost evidence. In short, altering, destroying, or misplacing an item must have a causal relationship to the inference sought to be obtained. The purpose of giving such an adverse inference is to restore the aggrieved party to the same position as if the spoliation had not occurred and also to deter others. Generally, before an adverse inference is

## Normal Course of Business Document/ Data Retention Questions

### Typical General IT Questions

- In how many different locations do you have operations?
- Where are they located?
- How many servers does your company use?
- Are all servers backed-up for disaster recovery purposes?
- Can you identify which server(s) support each application?
- Can you identify which backup tapes contain data from a selected server?
- Can you identify which IT assets (hardware and software) are being used by each employee?
- Is there a published set of IT compliance rules? Is the document available?

### Data Retention Questions

- Who is the person in charge of your data retention policies?
- Are this person's responsibilities regional, national, and/or international?
- Are the data retention policies published and is the document available?
- Do you always follow the published data retention policies? If not, why not?
- Are you aware of the regulatory rules concerning document retention for your organization (SOX, SEC, HIPAA, etc.)?
- How long has it been since the data retention policy has changed?
- Has the policy changed as a result of any pending legal actions?
- Is this retention policy in place across all locations within the company?
- Has this been audited across the company? When and by whom?

### E-mail Questions

- What is the current retention policy as to electronic documents and other data?
- What e-mail systems are you using? What versions?
- Who is the person(s) in charge of the company e-mail systems?
- Are all sites using the same e-mail package and version?
- What other e-mail packages have you used historically?
- When did you migrate from the previous version to this version? Over what time frame?
- Were all sites using the same package at that time?

- Were the old mail boxes converted or did the users simply have an old and new mail box?
- What happened to the old e-mail? Was it deleted or allowed to stay on the server?
- Do those servers still exist?
- Were the disks ever imaged or copied other than to tape?
- Does that media still exist today?
- Can a user have multiple e-mail accounts?
- How are these accounts tracked?
- Where is e-mail saved when a user saves it?
- Does the user have options as to where to save e-mail? What are the options?

### Tape Backup Questions

- What backup systems are you currently using?
- How long have you been using them?
- Is the same version in use across all sites? If not, why not?
- What other systems have you used historically?
- When you migrated from one system to the other system, what happened to the old data?
- What types of storage media are you currently using?
- Are all sites using the same generation of technology?
- What other types of technology have been used historically?
- When you migrated from the older technology to the new technology, what happened to the old tapes?
- Did you retain the old tape drives and software to allow access to this technology?
- How do you keep track of which tapes you own and which tapes are onsite or offsite?
- Have you always used this system? If not, what system was used previously, and how was the information migrated when the new system went into place?
- When you move a tape offsite, how do you reconcile the media move?
- How often do you perform a physical media audit to ensure that all tapes are accounted for?
- How is your media stored?
- Is it on a rotation cycle?
- How is the cycle determined?
- Do you have a policy of verifying that backups are accurate?

- Have you ever stored data onsite?
- If you now store data offsite, have you physically audited these old locations to ensure that they no longer contain media of any kind?
- Who is your offsite storage vendor?
- How long have you used this vendor?
- Do all sites use the same vendor?
- What other vendors have been used historically?
- Have you performed an audit to ensure you have the data you think you have?
- Do you maintain historical tape catalogs that allow you to see what files are on what tapes? If so, how far back can you tell what information is on which tape?

### Evidence Preservation Questions

- When were you instructed to preserve potentially relevant documents/data relating to the litigation?

- What actions were taken to:
  - preserve potentially relevant electronic and paper documents?
  - notify employees or third parties to stop deleting or altering potentially relevant documents/data?
  - prevent key users' PCs from being recycled should they leave the company or be given new equipment?
  - prevent key users from destroying or altering their network files?
  - prevent e-mail from being destroyed or altered?
  - prevent backup tapes from being overwritten?
  - suspend normal document destruction of offsite documents?
- What changes did you make to your tape rotation and retention policy to accommodate litigation hold requirements? When were these changes made?
- How do you determine what tapes needed to be held?
- How did you confirm you held the right tapes?

given, the aggrieved party must show that the spoliator acted with bad faith or some other type of willful intent or willful behavior.

### Criminal Sanctions

One of the hammers available for judges to swing to enforce civil litigation document discovery is the charge of criminal contempt of court for a party failing to produce the evidence ordered by the court. All federal and state jurisdictions recognize this judicial prerogative and the potential penalty of time in jail for the offending party.

### The Impact of Sarbanes-Oxley

The Sarbanes-Oxley Act (SOX) has also had significant impacts on the requirements relating to document retention, including criminalization of the destruction, alteration, and falsification of records in federal investigations, bankruptcy cases, and official proceedings. Sections 802 and 1102 of the act amended the federal obstruction of justice statute, Title 18 of the United States Code (Crimes and Criminal Procedure), to significantly increase penalties for the destruction, alteration, and falsification of records in certain circumstances.

Section 802 provides for a fine and imprisonment for up to 20 years for anyone who knowingly "alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry" in any record or document with intent to impede, obstruct, or influence the investigation or administration of any matter within the jurisdiction of a federal department or agency or any bankruptcy case.

Section 1102 establishes the same penalty for anyone who corruptly "alters, destroys, mutilates, or conceals" a record or document with intent to impair its integrity or availability for use in an official proceeding. Significantly, the official proceeding need not be pending or about to be instituted at the time of the offense.

### How Prepared Are You?

Is your company vulnerable to a charge of spoliation? It may be based on how well your IT or RIM manager responds to the sample questions in the

sidebar, "Normal Course of Business Document/Data Retention Questions." The questions are designed to uncover how records and information management processes work within your company and to determine how effectively they operate on a day-to-day basis. RIM managers would do well to notice that electronic records are emphasized and that answers to the questions could be very complex for large companies with highly decentralized operations.

Opposing counsel will use the answers given by the IT manager or RIM manager as the foundation to support an allegation of spoliation related to a litigation matter. There is no substitute for preparation. Role play with legal counsel several times before answering any question under oath. Do not accept the excuse, "We are too busy" or "We don't have the budget." As one veteran litigator said, "If you don't have the time or budget to do it right, you sure don't have the time or budget to do it over." ■

*Kirke Snyder, JD, is the San Francisco Director of the e-Discovery Practice at LECG, Inc. He can be reached at kirke.snyder@lecg.com; David Isom, Esq., is Chair of the National eDiscovery & eRetention™ Practice Group of the international law firm Greenberg Traurig. He can be reached at isomd@gtlaw.com.*