A Road Map for Document Preservation

Keeping the Nightmares at Bay

MICHAEL C. MILLER AND JEFFREY M. THEODORE

Michael C. Miller is a litigation partner with Steptoe & Johnson LLP, New York City.

Jeffrey M. Theodore is a litigation associate in the firm's Washington, D.C., office.

We have all heard the nightmare scenarios. The government serves a subpoena on a company in connection with a new regulatory investigation, and while counsel is being retained to handle subpoena compliance, a senior executive starts deleting potentially troubling emails. Or just days before a corporate employee is scheduled to testify at his deposition in a large commercial dispute, he remembers that he has a box under his desk at the office and a thumb drive at home—both containing documents relevant to the litigation that no lawyer has reviewed. Or it turns out that the new French subsidiary of your rapidly expanding multinational corporate client, which is embroiled in a sweeping antitrust lawsuit, has not fully implemented corporate polices for document retention.

In a world where meaningful sanctions can readily flow from a failure to preserve documents relevant to a lawsuit, these sorts of nightmare scenarios do keep lawyers awake at night. Indeed, the Federal Rules of Civil Procedure contain an entire provision—Rule 37—dedicated to sanctioning counsel and clients who fail to comply with their discovery obligations. That is on top of each district court's well-established, inherent authority to impose sanctions for discovery violations, including destruction of evidence.

Although no document retention policy can prevent every potential discovery mishap, counsel might consider employing the basic strategies discussed below to keep these nightmares at bay.

Counsel and client must act to preserve evidence as soon as they are on notice of its relevance to current or future litigation. *See, e.g.*, *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). Although it is sometimes not clear what constitutes notice, typically the more difficult question is fashioning the right action plan once notice has been received.

Finding the right action plan is particularly challenging when the client does not employ a sophisticated document management system or have recent experience with discovery-intensive litigation. For those clients, the conversation about document preservation can be sobering. It starts with Federal Rule of Civil Procedure 34 and its broad view of discoverable documents. Clients are sometimes surprised to learn that they need a strategy for preserving relevant writings, drawings, images, or recordings as well as any other sort of data or data compilations stored in any medium from which information can be obtained either directly or via translation into a usable form.

Further complicating matters with clients, regardless of the sophistication of their operations, is the undeniable fact that the volume of electronically stored information—and the number of devices it is stored on—has exploded. (For a comprehensive treatment of data collection from mobile devices, see Michael R. Arnold's iWitness column on page 53 of this issue.)

Published in *Litigation*, Volume 40, Number 1, Fall 2013.

The obvious first step is to issue a litigation hold letter to the client promptly. It is important that this letter provide enough information to permit the client's employees to identify what documents they need to preserve and how to go about preserving them. It is equally important to get this letter into the hands of the employees who are likely to have documents relevant to the dispute. Because these employees often play very different roles in a large organization and, as a result, touch on a major dispute in a variety of ways, it sometimes makes sense to tailor the litigation hold letter to provide more meaningful notice to these different categories of employees.

Issuing a litigation hold letter is not just a great idea; the failure to distribute such a letter may lead to sanctions when document preservation efforts do not work. The Southern District of New York has described the failure to issue a litigation hold letter as "grossly negligent." *Heng Chan v. Triple 8 Palace, Inc.*, No. 03-CIV-6048, 2005 U.S. Dist. LEXIS 16520, at *7 (S.D.N.Y. Aug. 11, 2005). At a minimum, it is "one factor in the determination of whether discovery sanctions should issue." *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 162 (2d Cir. 2012). Whether or not a litigation hold is itself required, the fact that one has been issued will put a party and its counsel in a much better position in future months if accused of failing to preserve documents.

But mere issuance of a litigation hold does not exhaust the obligations of an outside lawyer. Counsel also must supervise the document preservation process and seek to ensure that client personnel comply with the litigation hold. This supervisory function was always good practice, but a series of recent decisions has given it new importance.

Recent Relevant Decisions

The seminal case is *Zubulake v. UBS Warburg*, in which Judge Scheindlin issued a series of opinions finding both UBS and its lawyers culpable for permitting the destruction of key documents in an employment litigation. Judge Scheindlin emphasized that it is "not sufficient" to issue a litigation hold and expect client employees to comply. Rather, counsel must take "affirmative steps" to monitor and ensure compliance.

In our experience, the client's general counsel is typically a reliable and natural ally in connection with fashioning and taking these required affirmative steps. General counsel tend to know an enormous amount about the client's paper and electronic data systems, and can help outside counsel get up to speed and quickly develop an appropriate document retention strategy. They also run the risk of sanctions if the document retention process fails. Courts have gone so far as to sanction in-house government counsel for failing to meet their preservation obligations, in particular for failing to follow up to ensure that employees complied with preservation instructions that they had received. *See, e.g.*, *Swofford v. Eslinger*, 671 F. Supp. 2d 1275 (M.D. Fla. 2009).

Illustration by Phil Foster

The *Zubulake* decisions offer a good roadmap for the required affirmative steps. For example, as these cases suggest, it is often helpful to reissue the litigation hold letter. This way it stays fresh in the minds of employees who are busy with other matters. In addition, it often makes sense to identify and speak with key employees who are most likely to have relevant information. This helps to ensure that these key document custodians know about the litigation hold and are complying with it.

Electronic Data Loss

Other very useful affirmative steps involve the handling of electronic data and, in particular, the risk that, in the ordinary course of business and for purely innocent reasons, electronic data might be lost or overwritten. We have seen clients take sensible steps to protect against this by segregating and taking physical custody of items such as thumb drives and backup tapes that contain critical information.

Thumb drives, in particular, are dangerous devices from a preservation perspective. They are small, easily lost or overlooked, and infrequently labeled to identify their contents. At the same time, the computers to which they have been connected will retain registry entries recording their use and sometimes even the transfer of files with relevant-sounding file names. Experience shows that this combination can give rise to a powerful spoliation motion.

Courts are split on the bad faith requirement when relevant documents are destroyed.

Backup tapes are less often lost, but clients usually have data retention policies that overwrite backup tapes on a regular cycle. This risk can be mitigated by working with the client to identify accessible backup tapes likely to have relevant information and segregate them so that the data they contain are not lost.

Similarly, active employee file spaces, such as computer desktops or personal folders, are locations from which files are commonly lost. Rather than try to micromanage employees' use of their computers, a good practice is to instruct employees to make copies of their active files and preserve them separately.

Other helpful ways to minimize the risk that a client's employees will not preserve documents is to obtain signed acknowledgments from the employees of their obligation to preserve documents. And counsel should follow up to ensure that employees have actually complied. There is no substitute for continued monitoring. Most important, counsel should document every step so that if some documents are lost, counsel can show that they met their obligations and that the loss of data occurred despite the more than reasonable efforts made to prevent that from happening.

Large corporate clients can present an additional set of challenges. They often have a significant number of employees and very large, sometimes disparate computer systems that store enormous amounts of data across a far-flung range of servers and devices. They have preexisting information technology policies, structures, and bureaucracies. Sometimes the corporations are a product of a wave of mergers and acquisitions that result in decentralized computer systems, inconsistent document preservation cultures, and different legal structures governing issues such as data privacy. Even under the best of circumstances, the data retention systems are often not designed with litigation and litigation-specific retention concerns in mind, which may hinder development of a litigation-neutral process for preservation.

The Reasonableness Test

Luckily, the test for both a client's preservation obligation and counsel's monitoring responsibilities is one of reasonableness. It has been recognized as crippling to require large corporations to preserve every email, shred of paper, and so forth based on the initiation or even mere anticipation of litigation. Thus, reasonable recycling of backup tapes is acceptable as long as you make efforts to ensure that those most likely to contain relevant material are preserved. And so-called inaccessible backups are often excluded from the analysis (though it is wise to preserve even inaccessible backups that are likely to contain relevant data and fight the battle over data reconstruction and production at a later time).

As to our responsibilities as counsel, Judge Scheindlin herself emphasized in the fifth of her *Zubulake* opinions that, "above all, the requirement must be reasonable." *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 433 (S.D.N.Y. 2004). We are not "obliged to monitor [our] client[s] like a parent watching a child." Ultimately, the client bears responsibility for preserving documents. We must ensure that the client understands the obligation and is following a reasonable plan to carry it out.

The first step is to take the lay of the land. We have found it helpful to make an immediate evaluation of existing corporate retention policies and practices to determine their adequacy. This permits a quick assessment of what is being retained at the

very moment and what needs to be changed so that appropriate documents are preserved. This initial evaluation also can form the basis for an efficient, successful preservation strategy. Remember that sophisticated corporate retention programs do not only destroy documents; they preserve tremendous amounts of material. Although they often require modification for litigation purposes, existing corporate policies can form the backbone of a preservation strategy.

Not surprisingly, on occasion, clients' actual practices regarding document retention diverge from their stated policies. This is particularly true when clients are not regularly involved in litigation. Although a corporate retention policy is an excellent way to demonstrate reasonableness and good faith in document preservation, document destruction that results from noncompliance with corporate policy will be invoked as evidence of bad faith and intentional spoliation, or at a minimum gross negligence.

The next key step is to conduct a high-level, enterprise-wide assessment of all systems and software to determine what should be preserved and what is being preserved under existing retention procedures. The key is to identify those areas of large-scale corporate information technology (IT) systems where relevant documents are likely to be found. This may require interviews with key client personnel as well as targeted keyword searches to determine where responsive documents are found.

On rare occasions, counsel is confronted with evidence that an employee is trying to delete emails or dispose of documents to frustrate an investigation or conceal facts in a litigation. Obviously, this information requires prompt action to stop the document destruction by, at a minimum, cutting off the employee's access to the computer system and paper documents. It also requires prompt efforts to identify methods of restoring or retrieving these documents. And, depending on the circumstances, this development may trigger obligations on the part of the company to report these events to the court and regulators.

Working with IT Departments

Throughout this process, coordination with the client's IT department is critical. We find it helps to speak directly with responsible IT personnel who are likely to have the best knowledge regarding the location of critical electronic data. They will know the most about the actual operation of the client's document retention policies and the preservation or destruction cycles that apply to discoverable material.

Large corporations often present unique challenges to document preservation, but just as often they offer state-of-the-art IT departments that can make document retention a vastly more manageable process. The systems run by these companies can be efficiently deployed to accomplish preservation tasks without undue additional costs to the client's legal department or interference with the work of key client employees. In modern corporate IT systems, there also will be access to the vast bulk of the information at issue. We live in a world of shared network folders where employees' own personal desktops are mirrored on servers so as to be accessible from multiple devices. That allows IT professionals to make backups of key employees' active files and desktop spaces without depending on the employees' own preservation efforts. The IT department should also create images of collaborative online workspaces, such as Microsoft's Sharepoint, that are increasingly the repository of large amounts of relevant material. And, of course, the IT department is best positioned to make archives of key employees' emails and suspend routine email deletion.

All of this can be done in a way that ensures that critical metadata are preserved. Ideally, the IT department should be asked to image the relevant drives, spaces, and folders, rather than simply copy the files contained in them.

We have found it helpful to have segregated repositories created by the IT department for data that have been preserved in this manner. This approach secures relevant information and reduces the likelihood of accidental loss or deletion. Creation of a repository can also avoid duplication of effort in subsequent document production efforts. Along these lines, the depository can also include the results of customized searches. Although there is no need to review the documents during the initial preservation process, performing searches for key terms and ensuring that the resulting documents are not lost go a long way toward showing good faith in preservation.

The nightmare scenarios described at the beginning of this article do occur, despite the best intentions of client and counsel. The steps counsel and client take once they are on notice of potential or actual litigation can have a significant effect on whether those scenarios result in meaningful sanctions.

It is important to know, of course, the applicable standards for evaluating spoliation in your court. They vary widely. For example, the courts of appeals are split on the question of whether bad faith is required to draw adverse inferences from destruction of relevant documents. The Second Circuit has permitted courts to impose adverse inferences where spoliation resulted merely from a party's negligence. *See Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2d Cir. 2002). By contrast, the Seventh Circuit requires bad faith before an adverse inference may be drawn. *See Faas v. Sears, Roebuck & Co.*, 532 F.3d 633, 644 (7th Cir. 2008).

Whatever the applicable standard for sanctions, a well-documented, systematized preservation protocol implemented by the client's IT department and supplemented by direct contact with key client employees is the way to approach document preservation. ■