

# Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW



<http://ddee.pf.com>

Reprinted from Vol. 5, No. 12 | December 2005

## BEST PRACTICES

### Managing Litigation Holds in the Face of New Compliance Duties

By Stacy O'Neil Jackson

Prior to *Zubulake v. UBS Warburg LLC*, 229 FRD 422 (SD NY 2004) (*Zubulake V*), the litigation hold letter was just one item among many on the general litigation checklist. In the post-*Zubulake V* era, the rules have changed for paper, as well as electronic data. (Hereinafter, paper and electronic data will be referred to collectively as data.)

The litigation hold letter can no longer be just an item on the checklist. It demands an entire checklist all its own.

Indeed, the proposed changes to the Federal Rules have reinforced the post-*Zubulake V* litigation hold duties. Several of the proposed amendments to the Federal Rules are geared to force the parties to pay attention to electronic discovery issues early in the game.

It is no longer acceptable to “stick your head in the sand” and pretend your case does not have e-data issues.

Specifically, proposed amended Rule 26(f) requires parties to discuss any issues relating to preserving discoverable information. Additionally, proposed amendment to Rule 37(f) will protect a party from sanctions for data deleted during the routine, good faith operation of its computer systems.

“Good faith” may require that a party suspend certain features of its computer system, and the steps taken to implement an effective litigation hold will determine if a party acted in good faith.

Here are the areas to address when considering your duties with regard to litigation holds.

#### Review Document Retention Policy and Mechanisms for Enforcement

In the late 1980's, document shredding conjured up images of Fawn Hall and Ollie North at the shredding machine during the Iran-Contra Affair. Today, we have a dif-

ferent imagery: the specter of Arthur Andersen employees shredding documents while they were on notice of a federal investigation involving Enron. Since that time, Congress enacted the Sarbanes-Oxley Act, which makes it easier for the government to prosecute wrongful document destruction. Judge Scheindlin brought all of this home to us when she advised counsel to “become fully familiar with her client's document retention policies, as well as the client's data retention architecture.” *Zubulake V* at 432.

But how do you get familiar with “data retention architecture”? At first blush it sounds painful, but really, the most painful part is learning the lingo and accepting the fact that maybe you don't know everything.

First, get a copy of your client's document retention policy, if they have one. It is estimated that only 59 percent of companies have e-mail retention policies. Sue Reisinger, *Electric Company, Corp. Couns.*, October 2005, 100 at p. 104. Review the policy before there is even the faint aroma of litigation, for what it does and does not cover. Pay special attention to electronic data. Most corporate retention policies do not currently address electronic data, and if they do, they do not do so adequately. If there is no ongoing or anticipated litigation, help your client improve upon their document retention policy with an eye toward how it will affect you during the discovery phase of any future cases.

Second, find out if a litigation hold has been instituted since the policy was written. Interview major stakeholders to see what went right and what went horribly wrong with the implementation of the litigation hold. Were there recalcitrant employees, were there technical difficulties, or were there cost issues? If you have the time and the money, you might try and implement a mock litigation hold and test

what the company already has in place. Painful as it may be, in the end it may become a valuable learning tool for exactly how things will happen in a real world scenario.

Third, you will need to sit down with the major business units that may be affected by the litigation hold. Departments like Human Resources, Accounting, Purchasing, departmental managers, or the company executives will need to explain to you how they create data, where they store the data, and how they destroy their data. Make sure they have seen the document retention policy and operate their business unit in accordance with that policy. Often, you will encounter employees who have read and understand the company's document retention policy but whose implementation of that policy at the daily operations level of the company is vastly deficient.

Understanding the data flow, storage devices, and retention issues will give you a running start if the new Federal Rules amendments become effective in December 2006, as anticipated. The Committee Note to the proposed amendment to Rule 26(f) states that it may be important for the parties to discuss their systems and for counsel to become familiar with the systems before the Rule 26 scheduling conference. Taking all of the above steps will allow you to effectively implement a litigation hold.

### Assess Your Data

In a post-*Zubulake* and amended Federal Rules era, we have to assess our data and determine its accessibility. When a party reasonably anticipates litigation, it must issue a litigation hold to ensure the preservation of relevant data. This general rule, as enunciated in *Zubulake IV*, *Zubulake v. UBS Warburg, LLC*, 220 FRD 212 (SD NY 2003), applies only to accessible data. Accessible data is defined as data that is stored in a readily useable format that does not need to be restored or manipulated to be useable. *Zubulake v. UBS Warburg LLC*, 217 FRD 309 (SD NY 2003).

A real-world, albeit paper, example of accessible data would be the trash can, dumpster, and landfill analogy. A piece of paper that is thrown into the office trash can is an accessible data item. Once that trash can is emptied into the office building's dumpster—and becomes commingled with other office waste—it becomes near-line data. Near-line data is data that is between accessible and inaccessible data, but it is definitely recoverable. After the dumpster is emptied into the landfill, it becomes inaccessible data.

In the electronic world, the analogy would flow as follows: an e-mail is read and deleted into the "deleted items" folder. That e-mail is considered on-line and accessible data. If the user copies the e-mail to a CD-ROM for future use, the e-mail becomes near-line data. If that same e-mail remains in the "deleted items" folder overnight and is copied to the nightly disaster recovery backup tape, and is then deleted from the "deleted items" folder, it has become inaccessible data. But take note that data from tapes *can* be considered

accessible if corresponding accessible data has been destroyed after notice of the litigation, *or* if the backup tapes are used for purposes other than disaster recovery, *i.e.*, recovery of data from backup tapes occurs regularly.

Sit down with the Information Technology people. First assess whether they have ever seen the document retention policy and what it means to them in their daily lives. Then ask them how they implement and track the policy. Ask them to explain to you, in easy terms that a fifth grader could understand, how information is processed through their system. Send your IT "dude" an e-mail and then have him explain how that particular e-mail flows through the system. Have him show you the servers that e-mail resides on, the backup tapes that it will be copied to, the off site storage area where the tapes are housed in case of disaster.

While the IT person explains this to you, create a flow chart and record how information—both e-mail and electronic documents—flows through the system, and identify all of the storage points. Once the storage points are identified, inquire as to how long the item will reside on that particular tape, server, CD-ROM, etc.

Once you've gone through the tutorial with one or more of the IT people, ask yourself who would be the best witness for the 30(b)(6) deposition. It's usually the person that made the subject matter easiest for you to digest in the initial stages of your IT education.

### Issue and Reissue the Preservation Letter

Even in a pre-*Zubulake* world, we all issued litigation hold letters. More often than not, they were boilerplate letters. Today's litigation hold letter is vastly different.

The litigation hold letter should be specifically tailored to the facts and circumstances of the case. It should educate the data custodian about the records retention policy of the company, the types of data that must be preserved, how it will be preserved, and the ramifications for the failure to preserve.

Most importantly, the preservation letter should provide contact information if the data custodian has any questions or requires assistance. More than likely, you will need two points of contact: an attorney contact for the legal and subject-matter issues, and a technical contact to assist with hardware or software issues. The preservation letter should be reissued periodically as the issues or key players in the case change.

### Oversee Compliance and Monitor Efforts

Monitoring the efforts of those actually implementing the litigation hold takes several forms. First, you must educate the masses. You must ensure that the everyday data custodians who are creating and storing data understand what the litigation hold is. It also helps to educate them on the ramifications of their actions for failing to preserve the data, *i.e.*, the company could be sanctioned millions of dollars.

For instance, sit down with the IT person who actually

runs the backup tapes. Address any specific labeling issues with them and make sure the label contains enough data that would make a search or restoration of that tape more economical. Make sure they have enough tapes to ensure they won't have to reuse tapes. Often, there is a set amount budgeted for backup tapes and if you cannot recycle tapes for a certain timeframe, this could increase that budget exponentially. Most day-to-day IT people aren't aware of the IT budget, much less how it will be impacted.

Second, follow up. In order to capture day-forward e-mails, we once set up a special mailbox, and whenever a key player had certain key words in their e-mail, a copy was automatically forwarded to the special mailbox. However, this required all of the key players to turn on some Outlook rules. After a month, we ran a report, only to discover that there were some key players who never had any mail sent to the special mailbox.

It turns out that some of them had hardware problems that had required a new install of Outlook; but they forgot to reset their special rules. Had we not followed up with these key players, we would have lost relevant day-forward e-mail.

Often, requiring a person to sign a form stating that they have read, understand, and will comply with the rules of your request to the best of their ability will tend to make them take their role in data preservation a little more seri-

ously. These forms can serve as backup documentation of your good faith effort to enforce the litigation hold.

## Document, Document, Document

Finally, if you have done all of the above, don't let it all go to waste! Remember to document your good faith efforts to implement and monitor the litigation hold. Create trip reports that record who you spoke with, the topics you discussed, and the documents and educational materials that were provided to each key player or data custodian. Finally, make sure to keep all of this data in one centralized location.

In the modern era of litigation holds, counsel's duty to implement and monitor the litigation hold is greater than ever, raising the monetary stakes for failure to adequately implement the hold. It pays to take the time to review the current status of your client's data architecture and records retention policy, and the sooner the better. Once litigation is on your doorstep, take the time to assess, inform, educate, monitor, and document the situation. Although it feels like it will take a lot of time and money up front, in the end, this approach will more than pay for itself.

*Stacy O'Neil Jackson is Corporate Counsel at IE Discovery, a provider of comprehensive discovery management solutions. She can be reached at [sjackson@iediscovery.com](mailto:sjackson@iediscovery.com).*

## ABOUT IE DISCOVERY

### Who is IE Discovery?

IE Discovery is the first legal services provider offering comprehensive Discovery Management and other litigation support services to corporate law departments, outside counsel, and government agencies. Comprised of legal professionals, technologists, and document specialists, the IE Discovery staff creates solutions for a wide range of complex, information-intensive litigation.

### What is Discovery Management?

Discovery Management is a sophisticated methodology for collecting and transforming disparate documents and data - both in electronic and paper forms - into a unified system that enables attorneys to quickly analyze relevant information for more effective advocacy. Encompassing the complete discovery cycle, from collection to production, IE Discovery's robust services rely on the InfoDox(tm) platform-a secure, Web-based system for searching, organizing, and producing discovery documents.

**discovery**  
ie discovery, inc.

IE Discovery offers solutions for all areas of Discovery Management:

- Planning - Legal and technical consultants assist clients to devise a Discovery Management strategy, for ongoing litigation and future cases.
- Collection - Identification and acquisition of discovery data and documents, both electronic and paper, from multiple sources.
- Processing - Staffed with experienced document professionals, the Data Processing Center follows rigorous quality assurance guidelines.
- Review - Legal professionals, using platform tools, perform reviews for relevancy, privilege, and issue coding, as required.
- Production - The identification, organization, and output of production documents to opposing counsel.

[www.iediscovery.com](http://www.iediscovery.com)  
1.800.656.8444