



**Try NetVault: Backup today.**  
Free product downloads available at [www.bakbone.com](http://www.bakbone.com)

HOME TOP STORIES HEADLINE NEWS TECHNOLOGY IN DEPTH WHITE PAPERS HOT COMPANIES/COOL PRODUCTS REVIEWS & VIEWS LATEST PRODUCT LAUNCHES

[Home](#) » [Compliance & eDiscovery](#) » The Litigation Hold: Why You Don't Have to Hold Everything

Wednesday August 20, 2008

## The Litigation Hold: Why You Don't Have to Hold Everything

TUESDAY, 05 AUGUST 2008 02:58 W. LAWRENCE WESCOTT II, ESQ. AND RANDOLPH A. KAHN, ESQ., KAHN CONSULTING



The advent of electronic discovery has introduced new terms into the IT vocabulary. One term, which now seemingly strikes fear into the hearts of IT managers, is the "legal or litigation hold." Failure to implement a legal or litigation hold can result in sanctions for "spoliation," or destruction of evidence, which may result in fines or even loss of the lawsuit.

A common reaction of those who have not had experience with electronic discovery is to hold everything. This approach is sometimes taken by outside counsel whose concern is making sure that necessary information is preserved; their concern is winning the suit, not with the costs, inconvenience, or business impact that saving everything can impose. In other cases, "hold everything" is imposed out of fear—companies don't know where all of their information is, how the information is managed, who manages it, and how to preserve it. In still other instances, not knowing what content exists on company computers may also play a major factor in the "blanket" preservation approach.

There is never a legal requirement for a litigant to save all company information for a lawsuit. In fact the court in *Zubulake v. UBS Warburg*, 217 F.R.D. 212 (S.D.N.Y. 2004) made clear the point: "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no'. Such a rule would cripple large corporations." Courts have upheld the right of companies to destroy information they no longer need pursuant to records retention policies, prior to recognizing the threat of litigation. The Supreme Court, in the case in which Arthur Andersen was accused of misconduct in destroying documents relating to Enron (*Andersen v. U.S.*, 544 U.S. 696 (2005)), stated, "[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances."

The duty to preserve documents arises when the company recognizes or anticipates the threat of litigation, audit or investigation. The usual circumstances might be a lawyer's letter, notice of a lawsuit or investigation or something else. With changes in the laws such as SOX, Federal Rules of Civil Procedure and cases like *Andersen*, some lawyers ensure that preservation happens at an earlier point in time, (but that is beyond the scope of this article.) The key concept is relevance. Federal Rule 26(b)(1) states that "[p]arties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense."

What steps should the enterprise take to preserve data?

**Promptly cease disposition of data until the proper scope of the hold can be determined.** Make sure the IT department stops any automatic processes so that possibly relevant data is not lost. All retention periods in any retention schedules should be suspended for the same reason. Courts have penalized parties for recycling backup tapes or the routine "innocent" purging of data when they were aware that a lawsuit was pending. Determining the scope of discovery should take place as quickly as possible so that regular retention and disposition practices for unaffected data can continue.

**Determine the relevant time period that information must be kept.** All states and the federal system have cutoff periods for claims, so that claims cannot be brought if a certain time period has passed. Called "statutes of limitation," these cutoff periods act as limits so that claimants cannot wait indefinitely before they decide to bring a lawsuit. This is an issue for lawyers to address as there may be circumstances or exceptions that extend the period. It is wise when developing retention schedules to incorporate statutes of limitation for expected types of legal claims the business may face.

**Determine the key players.** The "key players" are the individuals likely to have information relevant to the case. Preserving information of the "key players" is much less onerous than saving all of the company's documents. In some cases, it may be challenging to preserve documents of certain individuals; particularly e-mails. The configuration of the e-mail system may not lend itself easily to the preservation of the e-mails of certain individuals. In that instance, it might be necessary to over-preserve rather than risk losing relevant information. If that is unduly burdensome, try to determine if there are reasonable alternatives. For example,

Search our site!

Search...

### TECHNOLOGY IN DEPTH

[Backup & Recovery](#)  
[Cables & Connections](#)  
[Compliance & eDiscovery](#)  
[Data Security](#)  
[Disaster Recovery](#)  
[Disk Based Backup](#)  
[Disk-to-Disk to-Tape](#)  
[Hard Drive Duplication](#)  
[IP SANs](#)  
[Network Storage](#)  
[Small-to-Mid-Sized Businesses](#)  
[Software](#)  
[Virtualization](#)



Our twice weekly email newsletter  
[Sign up](#) or see the [current issue](#)

[Subscribe to CTN](#)

capturing "snap shots" of relevant employees' hard drives early on may help demonstrate to the court the party's willingness to take the necessary steps to preserve relevant data.

**Engage the opposing party in preservation discussions as early as possible.** As mentioned above, the relevant time period for the suit may not be obvious. In that case, it is wise to come to an agreement with the other side as to the relevant time period, what information needs to be preserved, and in what form, etc.

**After determining the proper scope of the hold, resume disposition policies for data not affected by the hold.** Make sure you follow through and purge information that has exceeded its periods of retention or is ready for recycle according to the retention schedule. In other words, if there are no other legal or business requirements for keeping information or it has met its period of retention, then the information should be properly disposed of. For example, the defendant in *Murphy Oil USA Inc. v. Fluor Daniel, Inc.*, 2002 U.S. Dist. LEXIS 3196 (E.D. La. Feb. 19, 2002) learned this lesson the hard way. Fluor had a policy of recycling its tapes every 45 days. However, for some reason, it had kept the backup tapes for 14 months. The plaintiff wanted Fluor to examine all 14 months of tapes for relevant information or documents, which Fluor estimated would cost over \$6 million. The court stated that had it followed its 45 day recycling policy, the issue would have been moot; however, it required Fluor to search all of the tapes.

The key to successfully preserving information for litigation is reasonableness and good faith. A frank and open dialogue between the legal and IT departments is critical. In addition, resolving preservation disputes with the other side is equally important. It's not necessary to preserve everything, but with a little effort and common sense, the right information can be preserved. Resist the temptation to preserve everything—it is almost never required and almost always creates a burden for the business and the employer alike. Having and following retention and preservation rules allows the business to be more efficient in normal business times and helps to make sure that a company will be legally compliant when litigation happens.

*W. Lawrence Wescott II, Esq. and Randolph A. Kahn, Esq. of Kahn Consulting, Inc.*



Your critical  
or converged  
network closets  
at risk of  
downtime?

**APC**  
Legendary Reliability