



Data Preservation: A Checklist

by Gene Klimov
Director, Data Forensics

In the post-Zubulake era, it is understood that counsel must be proactive with their clients in advance of litigation, and they must also follow-up after the initial notice of the litigation hold. We have found that the best way to stay on course is by distributing and adhering to the **Preservation Checklist**:

1. **Have a Litigation Hold and Preservation Plan in Place:**

Similar to a disaster recovery plan, clients need a "Litigation Reaction Plan" which can be quickly executed. The time to consider the costs and disruption to business of such a plan is before litigation commences. Those can include: the suspension of document-destruction protocols, requiring the acquisition of supplementary computer servers; the segregation of relevant back-up tapes, which then need to be replaced and stored; the retention of a consultant, which may be necessary to obtain forensically sound mirror images of hard drives, or devise and perform key-word searches across various sets of data.

2. **Communicate the Litigation Hold and Preservation Duty:**

Once litigation is anticipated, it is counsel's responsibility to instruct the client to preserve all relevant data. A good start is a document preservation letter to all employees, instructing them not to delete anything pertinent, be it an existing document, or data created after the date of the preservation letter. Additionally, a separate "Systems Preservation Memo" to IT personnel should describe the responsibilities of the system administrators, and include specific examples of the information to be preserved. Likewise, individual communication with IT staff and any employees reasonably believed to have relevant information is crucial. These are the data gatekeepers, and must understand their preservation responsibilities if the hold is to be effective.

3. **Identify the Relevant Information:**

This will require extensive communication with those employees directly implicated by the

Join Us

Webcast: **Managing Data in Response to Regulatory Investigations**

This program will outline best practices for storing data, cooperating with investigators, developing a planned response and preparing, in advance, for future investigations. [Click here to attend](#)

New ALI-ABA Course of Study:

[Electronic Records Management & Digital Discovery](#)
May 12-13
Chicago

[Additional](#)

litigation, and with the client's IT personnel. The objective will be to learn what electronic data germane to the litigation has been created and where it is stored. E-mail messages may be the most notorious, but other forms of electronic communication also exist, including instant messaging and voicemail messages. Additionally, lawyers should inquire about system information, computer databases, and typical business files such as word processing documents and spreadsheets. Detailed information about the nature of the client's business, and the details of the litigation, will help counsel customize the inquiry. Carefully tailored keyword searches will also help counsel find the relevant data. Be alert to employees who have moved within an organization as they create particular challenges – different departments will be linked to different computer servers and back-up tapes. Be careful to identify the time-frames these employees were in each department.

4. Preserve the Relevant Information:

This, again, requires careful communication with IT staff to understand the company's document destruction policies – policies which should be suspended until preservation has been effected. To insure preservation, and establish the chain of custody, forensic imaging technology can be used to take "snapshots" of computer hard drives. Additionally, all employees should be instructed to produce electronic copies of their relevant active files to a limited-access central location. Simply forwarding e-mails to counsel is inadvisable, as that will alter the meta-data associated with the communications. Such meta-data would include the date and time the e-mail was originally created and sent. Forwarding the e-mails will also add the attorney's name to the communications as a recipient. This could have the unintended consequence of causing the documents to be categorized as privileged attorney - client communications.

5. Segregate Relevant Back-Up Tapes:

Zubulake V is consistent with most courts and commentators in not requiring that parties automatically include back-up tapes – created for the purpose of disaster recovery – within the litigation hold. Nonetheless, it is good practice to segregate any back-up tapes containing relevant data by taking them out of the back-up rotation. The tapes should be stored in a secure, temperature-controlled environment to preserve their contents and insure they can be found when needed.

6. Communicate the Litigation Hold and

[resources](#) on
EED and
Technology at
Trial

Contact [Paul
Neale](#)



for consultation
on your next
case.

[e-News
Archive](#)



Preservation Duty – Again:

Periodically re-circulate notices about the litigation hold and preservation duty to reach new employees, and to remind others. In *Zubulake V*, the Court comments on the time and tedium associated with establishing the facts relevant to the discovery dispute. Addressing the *Zubulake* parties, as well as other litigants and counsel generally, the court writes: "This Court, for one, is optimistic that with the guidance now provided it will not be necessary to spend this amount of time again. It is hoped that counsel will heed the guidance provided by these resources and will work to ensure that preservation, production and spoliation issues are limited, if not eliminated." Hope is eternal. Nonetheless, the standards for electronic discovery, emerging nationally, and now fine-tuned in *Zubulake I* through *V*, should go a long way towards providing the direction needed to navigate this difficult terrain.

[Go to top](#)

This document is provided for informational purposes only. The information contained in this document is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement. The user assumes the entire risk as to the accuracy and the use of this document.

(c)2005 DOAR - All Rights Reserved

□