

**ESI Risk Management Part III**

**Best Practices for General Counsel**



**WHITEPAPER**

# Table of Contents



Introduction **page 3**

Quick Review of Legal Principles **page 3**

Recommendations for Best Practices **page 6**

Choosing a Vendor **page 7**

Conclusion **page 8**

## ESI Risk Management Part III: Guidance for General Counsel

*In today's post-Enron and post-9/11 business environment, there is a growing obligation to proactively preserve any data potentially relevant to litigation that is produced for internal and external consumption by corporations and to communicate those obligations to all employees, especially IT departments. To cite National Association of Radiation Survivors v. Turnage, 115 F.R.D. 543, 547 N.D. Cal.1987, "The obligation to retain discoverable materials is an affirmative one; it requires counsel or corporate officers having notice of discovery obligations to communicate those obligations to employees in possession of discoverable materials."*

### **Introduction**

As a matter of risk management, it is becoming increasingly more important for companies to preserve electronic data not previously considered subject to possible litigation. With the myriad of data touch points, formats, and electronic systems used in current business transactions, general and inside counsels of corporations must be aware that legal exposure encompasses a much wider scale among various communications media that go beyond ordinary email and typical office documents.

Current trends in case law, as well as recent definitions set forth by federal rules, define electronically stored information (ESI) in very broad terms, essentially including any type of electronic and paper data imaginable. According to FRCP Rule 34(a)(1)(A), ESI is defined as "...including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained – translated, if necessary, by the respondent into reasonably useable form..." and deems ESI as potentially discoverable.

In the IT-dominated world of modern business practices, backup tapes are commonly considered a reliable data storage method. However, it is precisely this "offline" data safely stored in backup tapes, archives, or inactive servers that is becoming a cause for alarm, as it has been the

source of numerous notorious case law and judgments. The problem lies in the surprise potential of unmanaged data often "off the radar" of corporate IT departments and for which there is no available inventory or standard policies and procedures in place.

This white paper addresses some of the legal principles governing discoverable information, the corporate challenges, common mistakes, and dangerous pitfalls of information management, and recommended best practices for proactive litigation preparation, or what is aptly termed e-discovery readiness.

### **Quick Review of Legal Principles**

#### **Case Law**

##### **Zubulake v. UBS Warburg (2003)**

In 2003, we saw the beginning of a call for backup tapes as discoverable information with the landmark Zubulake v. UBS Warburg case. Some of the early rulings on this matter suggested one could no longer ignore backup tapes and archival data as inaccessible, too costly, or not relevant to the proceedings of a lawsuit.

*"As a general rule, a party need not preserve all back up tapes (e.g. those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth by the company's policy."*

*Zubulake IV 220 F.R.D. 212, 218 (S.D.N.Y. 2003)*

## ESI Risk Management Part III: Guidance for General Counsel

“Emails stored on backup tapes (via NetBackup), however, are an entirely different matter. . . . those tapes are not currently accessible. In order to search the tapes for responsive e-mails, UBS would have to engage in the costly and time-consuming process detailed above. It is therefore appropriate to consider cost shifting.”  
*Zubulake v. UBS Warburg* 217 F.R.D 309 (S.D.N.Y. 2003)

The one exception states that if the data on the backup tapes are not otherwise available, then the backup tape becomes important.

“It does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of ‘key players’ to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes.” id @218

### FRCP 26(b)(2)(B)

“A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.”

“It is not possible to define in a rule the different types of technological features that may affect the burdens and costs. . . .”

### Precedence & Implications

Despite the *Zubulake* rulings, many organizations are now routinely restoring backup tapes in response to litigation, since they are becoming more practically accessible. New technologies and standards introduced in the past several years have made the restoration process relatively easy and inexpensive. Therefore, even though the primary source of electronic data should be “active” data, it is now becoming more common to use off-line data including backup tapes.

Ideally, a proactive data retention program should exist inside corporations to ensure processes, people, and tools are effectively preserving data from the active systems, as well as reducing the risk and cost of e-discovery by inventorying and managing all archival data on an ongoing basis. In other words, as one of The Sedona Conference Institute’s principles states:

### Principle #8:

The primary source of electronic data and documents for production should be active data and information purposefully stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resorting to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

### Implications to Corporations

In a volatile era of mergers and acquisitions coupled with rapid technological advancements, major corporations have gone through many changes that impact data retention practices. Frequent system upgrades and high IT staff turnover, for example, have made it increasingly difficult to successfully maintain historical knowledge. There are multiple types of email servers, shared drives, and data sets that are constantly changing – all contributing to a complex IT environment. It’s no wonder lawyers are spending a growing amount of time on IT-related issues, a predominantly binary, black and white area quite opposite from the legal arena where many gray areas reside. This contrast and the ensuing complications it fosters further highlights the need for a set of data retention policies and procedures to establish a standard practice with a common understanding between IT and general counsel, especially in an e-discovery context.

### Resulting Effects Over Time

Backup tapes and ESI archives are not going away for the time being. In fact, backup tapes are being sold at the rate

## ESI Risk Management Part III: Guidance for General Counsel

of 50 million new cartridges every year. While near-line RAM-based storage SAN and NAS are highly effective active storage devices, companies are not likely to replace their backup systems with them anytime soon. Relatively affordable price and ease of use, especially considering the minimal requirements for integration and implementation, keep tape media heavily entrenched in the vast majority of corporations' ESI backup policies.

In the next several years, new media formats will no doubt be developed, making the data storage process even more efficient and affordable; thus, the lines of distinction between accessible and inaccessible data will all but disappear.

### Corporate Challenges

Per the 2006 Amendments to the FRCP, corporations must be more aware of what data exists, where it is located, and whether it is readily accessible for discovery. While organizations are currently implementing sound "go forward" strategies for document management, there is still some concern about ESI created and stored prior to these strategies being put into place.

### Archival Practices vs. Disaster Recovery

General uncertainty about ESI content and the related fear of sanctions if data is wrongly deleted have resulted in "keep everything" retention policies. However, it is critical to distinguish between implementing and maintaining a solid corporate retention program and a good faith operation of electronic systems. Backups are typically created for disaster recovery, not archive retrieval.

- **Disaster recovery tapes** are for system recovery. The retention/over-write period is usually defined in days, weeks, and months.
- **Archival tapes** are generally used for long term storage of critical records that are required to be maintained by corporate policy, statute, or regulation.

### Rising IT Costs

IT departments must budget for physical storage resources and costs associated with retrieving and returning media that are subject to discovery or investigatory requests. While archive tapes are not that expensive, moving through different types of systems, tape types, backup software, various methodologies, and keeping up with technology can be costly particularly if historic equipment and software are also maintained.

### Vendor vs. In-House Archival Solutions

IT departments already struggle for resources, and yet this is often one of the first places corporations cut back in tough economic times. Problems of becoming overwhelmed are likely to develop if this same staff has to apply their IT mindset to legal problems such as e-discovery readiness and responsiveness.

In evaluating the effectiveness of in-house archival solutions, one must ask what processes are in place and determine whether or not they are repeatable. Some common constraints faced by companies trying to go the in-house route are: chain of custody, process control and quality, defensibility of restoration, utilizing IT departments, security and controls over data process might be missing, and native restoration requires software licensing as well as re-creation of native environments.

ESI vendor assistance makes sense because such firms have a highly documented process that includes defensibility restoration, security controls, chain of custody, and maintenance of tape index catalogs or re-cataloging of tapes. They can mitigate substantial business disruption, loss of time, and drain on resources. With the tendency to over collect data, companies benefit from having specialists who can also cut attorney review costs by knowing what should be retained and recovered for legal purposes.

# ESI Risk Management Part III: Guidance for General Counsel

## **Recommendations for Best Practices**

### **Litigation Readiness**

You should advise your clients to become “litigation ready” so they are able to more effectively and efficiently address discovery of ESI while avoiding the sanctions that are now commonly associated with delayed productions of evidence. Use the knowledge gained from the development of the data map to identify which media is likely to contain ESI that must be retained.

To do this, corporations should consider migrating relevant historical ESI from older, disparate media sources and archive systems into a format that can be managed using modern tools. Using the knowledge gained from the development of your data map, you can identify which media is likely to contain ESI you must retain. The steps below can drastically reduce the total volume of data to be archived, keeping the archive at a cost-effective and manageable size.

- Advise your clients to complete a physical inventory (or “data map”) of all media with potential ESI content. Media type, label, condition, and media location should be gathered for all media and a report generated that can become part of your data map used in response to any e-discovery requirements.
- Eliminate exact duplicate files wherever possible. Work with your Legal and Records Management teams to determine if a single copy of a document is acceptable or if you need to retain a copy per location, custodian, or other level that Legal specifies as necessary. If you have historical ESI on tapes, it is likely it was created through a backup process. Eliminating exact duplicates residing on full or incremental backups can yield significant reductions in data volumes.

- Eliminate unnecessary operating system and application data files that are static in nature. These include ‘readme’ files provided with software applications, executable files, and other file types your organization determines is not necessary.
- Enhance the value of your archiving strategy by converting necessary historical ESI into a format compatible with your archiving solution. This is primarily relevant for email archives that were originally departmental in nature or that were inherited during a merger or acquisition.

### **Benefits of a Proactive Approach**

As you continue to migrate your historical ESI into your archiving platform, you will find the value of your archive increases as its ability to effectively support discovery requests grows. However, the IT function also receives direct benefits, including:

#### **Reduced Storage Requirements**

Consolidating data across thousands of pieces of media into a single archive can dramatically reduce the internal costs and burdens of retaining historical data that must be preserved. For companies using offsite storage facilities, eliminating the bulk of antiquated storage media in favor of a consolidated repository alleviates much of the expense and delays associated with moving tapes to and from the storage facility, which could add hundreds of dollars per month during a litigation cycle. By consolidating and eliminating your inventory of backup media, immediate and recurring savings can be realized, which leads to overall improved management of your IT budget.

#### **Quicker E-Discovery Response Times**

By understanding what is on your media, you can quickly identify responsive data if or when discovery orders arise. Maintaining an inventory of your media which maps out which data is where, in addition to having an easily accessible archive of normalized ESI, allows your IT department to react promptly when Legal starts asking for data or when new litigation holds are put into effect.

## ESI Risk Management Part III: Guidance for General Counsel

### ***Less Involvement with Legal***

In addition to improved responsiveness, proactively managing your organization's historical ESI can mitigate the level and duration of IT's involvement throughout the e-discovery process. By standardizing, consolidating, and ingesting ESI into a single archive, IT has effectively set the stage for Legal to manage the e-discovery process with minimal resources required of IT. In short, IT can enjoy less business disruption once the initial, preparatory heavy lifting is completed.

### ***Data Security***

The systematic elimination of unnecessary files – and of removable media in general – diminishes the potential for sensitive or confidential information getting into the wrong hands. Implementing a comprehensive ESI plan that is well documented and rigorously implemented helps your organization to mitigate these risks by reducing the chance of data tampering or spoliation. It also enables you to assert claims that ESI was managed in a manner consistent with the “routine good faith” specified in rule 37(e).

### ***Choosing a Vendor***

As can be seen, IT now has a vital role to play in ensuring the organization properly collects, categorizes and manages its necessary ESI to meet legal and regulatory requirements. When making critical decisions such as this, utilizing a third party should be given serious consideration. Among other practical reasons, external vendors are not likely to be constrained by internal organizational issues, can provide a perspective based on their experience from working with similar organizations, and they provide some level of risk-sharing.

### ***Legal Heritage***

Remember what you are dealing with is evidence – not simply data – and what you are solving is a legal problem that requires technology as a part of the solution. Therefore, look for service providers who have a strong legal pedigree and who understand technology. For the purposes of mitigating the risks associated with ESI, vendors with a particular focus on e-discovery processing and data archiving are particularly well suited to help.

### ***Comprehensive ESI Support***

Look for a vendor who can help you with all of your ESI: operational and historical. For historical ESI, verify the prospective vendor can process standard media types (i.e. DLT4, LTO1, 4MM tapes) as well as the most common forms of backup software (i.e. Backup Exec, NetBackup, Legato Net Worker, Tivoli Storage Manager, ArcServe, CommVault Galaxy and HP Omniback) that are likely present within your historical ESI inventory. Be sure your vendor of choice can convert the data in its current format into the desired format for loading into your archive – and within the time frame needed. Also, if your organization uses (or has used) a variety of messaging systems, such as Lotus Notes, Novell GroupWise or others, verify the vendor can perform these conversions. Keep in mind the possibility of unknown or outdated media and software that may exist in your inventory of historical data, so choosing a vendor with a full range of supported media types and backup formats is critical.

### ***Capabilities and Capacity***

For your archive, know your scalability requirements. Calculate your current average email size, daily volume, and projected growth over the period of the average retention period your organization will use. Then you need to factor in your historical ESI. This resulting data will be the largest single addition into your archive.

## ESI Risk Management Part III: Guidance for General Counsel

Most likely, this segment of older data will need to be analyzed and restored off-site by the vendor in order to extract it from its current media, format, and convert it into a form compatible with your archive solution. Ask each prospective vendor to provide you a preliminary plan and timeline for processing this data. The longer it takes to get this data into your archive, the greater the risks and costs to your organization.

### **Secure Facility**

Trusting a service provider with your corporation's ESI means your data will likely need to leave your facility. The last thing your organization needs is a breach in security caused by a vendor, compromising your organization legally or causing a public relations disaster. Perform due diligence on all prospective vendors to assess their ability to safeguard and account for your data throughout the entire process. The ability to maintain secured Chain-of-Custody at all times, provides you the legal defensibility your organization needs.

### **Conclusion**

Encouraging your clients to manage ESI as far in advance as possible can minimize the level of exposure and overall risk associated with retaining large volumes of information. Eliminating data that is not required for preservation in the wake of retention policies or litigation holds helps you and your client remove much of the dormant liability that resides within mountains of historical data – especially data found in large inventories of historical backup tapes. Retain only the data that must be kept, and eliminate the rest.

### **Proactive ESI Risk Management**

There are numerous cases where ESI on magnetic tape was determined to be reasonably accessible. It is likely this trend will continue as new technologies and e-discovery services continue to target backup tapes. A sure way to reduce the need to make this argument is to be proactive. Evaluate your historical data ahead of litigation. Identify business records on the media, move it to an archive, and apply the appropriate retention periods. When you do this, be sure to include any data subject to litigation holds. Doing so will allow you to make a better case to your legal department that all required ESI is now under the control of an archive and that the historical ESI on backup media can be safely integrated into your tape rotation policy. When seeking a neutral third party to assist the management of electronic data, careful evaluation of a firm's capabilities, background, and expertise cannot be compromised. Once "data" becomes "evidence," preparation and due d

---

## About RenewData

---

RenewData is a leading provider of e-discovery and ESI (electronically stored information) risk management services to assist corporations and law firms responding to lawsuits, investigations, and audits. Superior legal expertise, scalable technology, and a state-of-the-art facility featuring government level physical security enable RenewData to provide clients with secure, accessible, and manageable data in a cost effective and timely manner. RenewData's e-discovery services cover the five critical steps of the e-discovery process, including planning, preservation and collection, processing, review, and production. RenewData's ESI risk management services, which include backup tape liability management, data migration, and evidence storage, provide corporations with a proactive means of managing the risks associated with ESI. RenewData has been ranked a "top provider" in the Socha-Gelbmann Electronic Discovery Survey Report for three consecutive years and was ranked in the 2006 and 2007 Inc. 500 lists of fastest-growing privately held companies in the U.S.



512.276.5500  
888.811.3789

[www.renewdata.com](http://www.renewdata.com)

Copyright © 2008 Renew Data Corp. All rights reserved. RenewData and ActiveVault are registered trademarks and ESIRM and "Single-Pass Processing" are trademarks of Renew Data Corp. RenewData disclaims any proprietary interest in the marks and names of others.