

WHITE PAPER

Proactive Information Retention and Disposition Management: When Faced with Litigation Events, Readiness Is Your Best Defense

Sponsored by: Iron Mountain

Vivian Tero
March 2010

IDC OPINION

The confluence of increasing data volumes, budget and operational constraints, and expectations of increased regulatory oversight and actions from the plaintiff bar underscores the importance of sound enterprisewide information retention and disposition programs. This program, in combination with formalized legal hold protocols, is a corporate litigant's critical line of defense during a litigation event. An effective program requires close coordination among key stakeholders — corporate counsel, compliance officers, and IT managers. Having formalized policies isn't enough. Corporate stakeholders need to work closely together to ensure that technical processes are in place to document the consistent enforcement of these policies. To demonstrate consistency in the enforcement of protocols and to manage ever-increasing data volumes, corporations should also consider the technical architecture required to support various information retention and legal hold activities. These technical protocols and solutions should address the retention and disposition of electronically stored information (ESI) across distributed data stores and centrally managed repositories such as archival systems. When executed effectively, the corporation's information retention and legal hold program would align the information risk management objectives of legal counsel and compliance with the operational efficiency and cost objectives of the CIO.

IN THIS WHITE PAPER

This IDC White Paper discusses the role of the legal function in driving down the cost of compliance and eDiscovery through the execution of a proactive information retention and disposition program. It also highlights the value of close collaboration across the legal and IT stakeholders in successfully executing this proactive program.

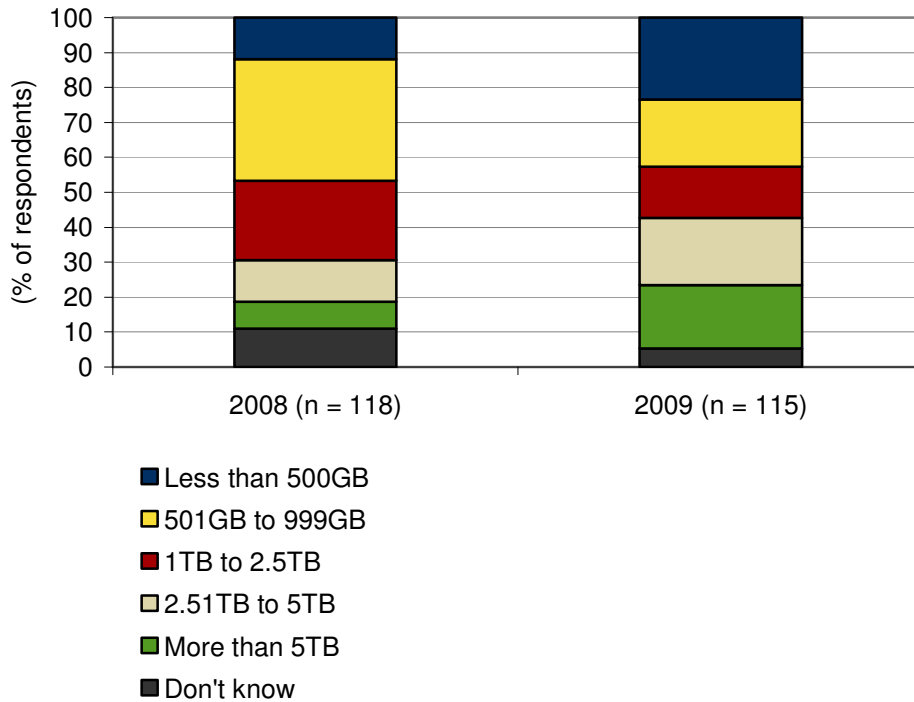
SITUATION OVERVIEW

Corporate counsel and compliance officers today find themselves caught between the proverbial rock and hard place. The amount of digital data continues to grow aggressively, thus increasing the volume of content that must be evaluated for and managed in accordance with its data retention, eDiscovery, privacy, and security profile. In 2009, IDC's Digital Universe research concluded that data and content will grow at a compound annual growth rate (CAGR) of 60% from 2008 to 2012. IDC forecasts that worldwide IT spending will post a CAGR of 12% over the same period.

Today, the explosion in digital content is already impacting the average volumes of data that are being collected and processed per litigation event. The results of IDC's 2009 survey of IT executives and eDiscovery project managers from the most litigious and highly regulated industries point to an increase in the size of the average data collections per matter (see Figure 1). In the 2009 study, 52% of the panel reported average ESI collections of more than 1TB per matter, up 10 points from the 2008 survey results. Within this group, there was a notable 11-point rise in the percentage of panelists who said that their average ESI collection per matter is more than 5TB.

FIGURE 1

Comparison of Average Volumes of ESI Collected per Matter, 2008 Versus 2009



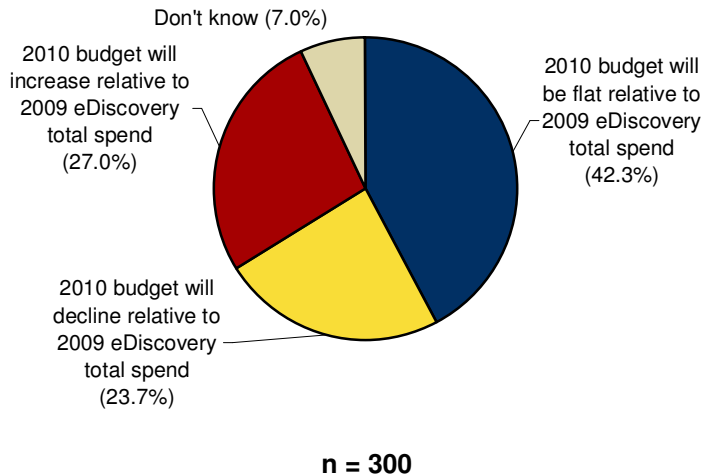
Source: IDC, 2008 and 2009

2010 is expected to be another banner year for government investigations, regulatory audits, and actions from the plaintiff bar. Among the 2010 IDC survey panelists, 44% are expecting a rise in the number of litigation events, while only 31% said that they expect the total number of litigation events to decline. The panel also said that while average ESI collection volumes continue to grow, IT budgets for eDiscovery are declining (24%) or remain flat (42%) (see Figure 2). These trends underscore the pressure on corporations to do more with less. Corporate counsel, records managers, and compliance officers have to reassess their current reactive stance to litigation events and take a more proactive and unified approach to information retention,

disposition, and management. They also need to work closely with their IT counterparts to ensure that the organization's information infrastructure can effectively execute the retention, disposition, privacy, and search and retrieval objectives.

FIGURE 2

2010 eDiscovery Budgets Are Flat or Declining



Source: IDC, 2010

Understanding the Cost of Compliance and eDiscovery from the Corporate Legal Counsel's Point of View

The following considerations impact the assessment of the cost of compliance and eDiscovery programs from the legal counsel's point of view:

- ☒ Litigation profile such as the number and types of litigation events per year, the average volume of ESI collection per event, the content types and content stores where ESI is typically collected, and the process and organizational maturity of the corporation's information management and ESI legal hold management programs.
- ☒ Technology infrastructure capabilities to automate eDiscovery and compliance efforts — such as data retention and privacy — including information, storage, and security infrastructure topology. The eDiscovery infrastructure components include the technical abilities to conduct legally defensible search and information retrieval, preservation, collection, media restoration and content migration (if needed), deduplication and processing, content migration, and document review and production platform application.
- ☒ eDiscovery review and production services, which includes attorney review and professional services for project management of the review and production process.

Industry research concludes that technology infrastructure costs account for 10% to 20% of the total eDiscovery costs per matter, while eDiscovery review and production services make up 80% to 90% of the total. However, organizational and process maturity, in combination with eDiscovery technology infrastructure capabilities, has the ability to impact three value levers that can significantly lower eDiscovery review and production costs:

- ☒ Significantly lower the volume that a corporate litigant must preserve, collect, and send to outside counsel for review. Litigants garner these savings from effectively employing technology to legally defend their search and preservation protocols and improve the precision of their preservation and collection scope. Corporations are also in a better position to plan for the 26(b) and 34(d) discussions around phased collection and forms of production.
- ☒ Gain early visibility into the case facts and mine historical information from litigation to better forecast the true cost of eDiscovery efforts, assess the risks, and determine the appropriate legal response to a dispute.
- ☒ Gain better visibility into the business and legal value of content and data through the effective classification of data. The investment in classification and content-aware technologies can be extended to enforce and demonstrate compliance with security compliance and privacy programs.

To take advantage of these value levers, legal counsel must work closely with the IT organization. They need to do this because a typical corporate litigant's information and storage infrastructure is complex. As data volume grows and as new applications are deployed in the environment, manual approaches to conducting data retention, eDiscovery, and data privacy can become unwieldy and prone to error. IT can translate the legal function's retention, disposition, privacy, and reporting requirements into technical protocols and controls. This will ensure that policies are consistently enforced. These efforts would lower the risks of future challenges to preservation and collection efforts and from inadvertent spoliation of relevant ESI.

Also, despite the best intentions, a porous and complex IT environment also means that there will be gaps between formalized policies and IT operational realities. The IT organization will advise legal of what is practically doable given the organization's process, technology, and budget constraints. The IT organization can work with legal to discover and assess the process and capability gaps in the existing information retention and disposition programs. Legal can identify and define the business and legal risks associated with specific content types, information repositories, and IT processes. Legal would also provide guidance on which gaps and risks to address first.

FUTURE OUTLOOK

In the recent landmark opinion, *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Secs, No. CIV. 05-9016, 2010 U.S. Dist. LEXIS 1839 (S.D.N.Y. Jan. 11, 2010)*, Judge Shira Scheindlin reaffirmed her Zubulake opinion, stating:

In an era where vast amounts of electronic information is available for review, discovery in certain cases has become increasingly complex and expensive. Courts cannot and do not expect that any party can meet a standard of perfection. Nonetheless, the courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed, and produced to the opposing party. As discussed six years ago in the Zubulake opinions (*Zubulake v. UBS Warburg, 229 F.R.D. 422, 2004 U.S. Dist. LEXIS 13574, 94 Fair Empl. Prac. Cas. [BNA] 1, 85 Empl. Prac. Dec. [CCH] P41,728 [S.D.N.Y. 2004]*), when this does not happen, the integrity of the judicial process is harmed and the courts are required to fashion a remedy. Once again, I have been compelled to closely review the discovery efforts of parties in a litigation, and once again have found that those efforts were flawed. As famously noted, "[t]hose who cannot remember the past are condemned to repeat it." By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records — paper or electronic — and to search in the right places for those records, will inevitably result in the spoliation of evidence.

The 2004 Zubulake opinion set the standards for robust eDiscovery requirements, and its implications on the breadth and scope of the obligations of litigant corporations remain even more relevant today. It underscores the value of sound information retention, disposition, and legal hold practices.

Given the volume of digital content that corporations generate daily, it is important for corporations to preserve and collect potentially relevant ESI smartly. Corporations need to find the right balance between overpreservation and collection with underpreservation and collection and do so in a legally defensible way. To help organizations do this effectively, IDC has identified best practices, which are discussed in the following sections. Success in executing these practices hinges on close collaboration between the key internal stakeholders — corporate counsel, records managers, compliance officers, and the IT function (primarily from IT storage, IT security, and IT operations). The overall objective of these collaborative efforts is to ensure that corporate information management and eDiscovery protocols are aligned with the CIO's cost containment and operational efficiency objectives.

Adopt a Consistently Enforced Enterprisewide Information Retention and Disposition Practice

A sound and consistently enforced information retention and disposition program enables the corporation to meet the Rule 37(j) requirements of the Federal Rules of Civil Procedure (FRCP) for eDiscovery. Under this rule, the corporate litigant can avoid sanctions if it is able to demonstrate that its data destruction policies are legally defensible. Corporations with mature enterprisewide information retention and disposition practices demonstrate the following attributes:

- ☒ **Enterprisewide information retention policies that recognize the distinction between records, nonrecords, and convenience copies.** Corporations have enterprisewide retention programs, where retention schedules are defined in accordance with business, regulatory, and legal obligations. Policies address both physical (or hardcopy) and digital versions of the records. These policies also reflect the business and legal requirements in the geographic boundaries in which the business operates. Corporations recognize that information could reside in various incarnations throughout the enterprise. For example, copies of a contract can be found as a PDF attachment in several authorized employees' emails, as a document inside an electronic records management system, as draft versions of said contract in a SharePoint site, and as a physical document stored in the company's offsite storage facilities. Mature corporations are clearly defining the distinction between records, nonrecords, and convenience copies. Given the fluid and persistent nature of digital information, mature organizations are establishing protocols for the disposition of the nonrecords and convenience copies (including their scheduled destruction), in addition to defining and consistently enforcing retention practices for corporate records.

- ☒ **Protocols to discover, identify, define, and enforce retention, disposition, and privacy policies for the corporation's strategic information assets in high-risk content stores.** Instead of boiling the digital ocean, corporate counsel, compliance officers, and records managers are working closely with their IT counterparts to develop a programmatic approach to enforcing retention, disposition, and privacy policies for nonrecords and convenience copies in high-risk repositories. Budget and operational constraints compel these corporations to prioritize their efforts and focus on addressing the most common eDiscovery collection targets and most strategic information assets. Active content — files that are created and stored in shared files and file systems; in distributed endpoints such as desktops, laptops, and removable storage devices; and in messaging and collaborative applications — is the most common target source during eDiscovery. For many corporations today, the retention and the disposition of files in these content stores are loosely imposed. Copies of strategic information assets (such as employee and customer PHI and PII and product design and engineering plans) can exist across loosely managed content stores. Protocols for authorized access and secure sharing of information also tend to be loosely enforced in these repositories. IDC security research notes that these content stores are among the most likely sources of security breaches and data leaks.

- ☒ **Clearly defined protocols to suspend and override scheduled destruction schedules in the event of a litigation event.** A litigation event is a reasonable anticipation of or an actual legal action, investigation, or audit. In *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Secs, No. CIV. 05-9016, 2010 U.S. Dist. LEXIS 1839 (S.D.N.Y. Jan. 11, 2010)*, Judge Shira Scheindlin reiterates the importance of legal hold protocols. Among the most litigious and regulated industries, 85% of corporations claim that they have legal hold policies. (See *State of Play: Litigation Readiness of Corporate IT Organizations*, IDC White Paper #211625, April 2008.) The most mature corporations not only have taken steps to document the legal hold notification communication life cycle but also have instituted technical processes to manage the ESI in fulfillment of these legal hold obligations. Key to this is the ability of the organization to suspend and override scheduled disposition when the legal hold notification is in place.

- ☒ **Data privacy policies are enforced consistently throughout the life of the record.** The most mature corporations have policies and programs in place to ensure secure sharing of records among authorized users and the timely destruction of records at the end of their retention period. Data privacy policies also guarantee the proper disposition of files that are deemed nonrecords and convenience copies but contain sensitive information. These policies also extend to the handling of failed or decommissioned storage media containing sensitive information.

- ☒ **Encourage retention and privacy as part of the corporate culture.** The most advanced corporations take steps to ensure a culture of records and privacy compliance. New employee training and periodic classes in aspects of the corporate records management program are offered. Corporations also include measures of records compliance awareness in the performance review of system owners and records custodians.

- ☒ **Audit regularly for compliance with policies.** To reinforce the records and privacy aware culture, corporations have started to audit and systematically monitor system compliance with formal retention and disposition policies. Audit reports also include remediation plans.

Develop Legal Hold Protocols

Formal Legal Hold Notification Life Cycle

The most advanced corporations have instituted best practices for the legal hold communications life cycle. These best practices include protocols for creating the legal hold notification, identifying and interviewing the records and system owners of the information stores, suspending scheduled data deletion upon notice of the legal hold, actively monitoring compliance with the legal hold on an ongoing basis, releasing the legal hold (when appropriate), and actively managing and monitoring preservation and collection activities. The most advanced corporations are documenting these activities. Compliance with legal hold protocols is audited periodically.

Management of ESI for Legal Hold

Given the fluid and persistent nature of digital data, the most advanced corporations have also started to define and enforce policies for the identification, preservation, and collection of ESI in fulfillment of their legal hold obligations.

Corporations with sound information retention and disposition practices typically employ content archiving and records management systems to enforce retention policies. These applications have the ability to preserve in place, obviating the need to store legal copies in a separate repository and purchase additional storage. These applications also provide case management workflows for eDiscovery, including early case assessment and first pass review. Increasingly, these applications also have the ability to export relevant ESI to the most popular attorney review platforms.

When it comes to enforcing legal hold for active content in distributed and loosely managed content stores — such as desktops, file servers, and SharePoint sites — a sound retention and disposition practice also protects the corporate litigant from the risks and costs associated with overpreservation and overcollection. Legal counsel is in a better position to discuss the accessibility and inaccessibility of content in distributed data stores when the corporation has legally defensible data destruction protocols.

IDC research notes that corporations are employing several approaches to enforce legal hold on active content from distributed data stores, including any of the following:

- ☒ A search application to find the relevant ESI and make legally defensible copies to be stored in a secure server, storage, or archiving system
- ☒ A data loss prevention (DLP) application to find the relevant ESI in combination with a forensics collection tool to collect and preserve the ESI
- ☒ An application that can forensically image the entire drive
- ☒ An early case assessment application to find, preserve, and collect ESI from the distributed repositories; conduct eDiscovery early case and first pass analysis; and forecast eDiscovery costs
- ☒ A backup application with eDiscovery and classification modules to find, monitor, and selectively retrieve relevant ESI from mobile PCs (In this scenario, the corporation has made a clear distinction between its archiving and backup operations. Here, the policy clearly defines that backup operations are used for business continuity purposes. Disposition schedules are consistently followed. However, policy is also written to allow the corporation to use the backup engine for targeted, event-driven search, classification, and collection of relevant ESI for eDiscovery. Not all backup applications have the ability to support eDiscovery. Those that do should be able to provide content search, document and report the search and retrieval activity, and avoid altering critical metadata information. In other words, the backup application should be able to demonstrate that the operations can meet legal chain of custody requirements.)

CONCLUSION

A sound enterprisewide information retention and disposition program, in combination with legal hold protocols, enables the corporate litigant to make informed decisions on the appropriate response to a litigation event. Close collaboration between corporate counsel, compliance officers, and IT managers is a must under the Federal Rules of Civil Procedure. These practices would also allow the corporation to limit the scope of eDiscovery, resulting in smaller, more precise data sets, thus containing the costs of eDiscovery and attorney reviews. Close collaboration would allow the stakeholders to develop innovative approaches for taking advantage of existing investments in records management, archiving, search, and backup solutions to automate the corporation's eDiscovery activities.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2010 IDC. Reproduction without written permission is completely forbidden.