Legal and Financial Considerations in Information Management

A guide to cost-effective discovery preparedness, records management, and privacy protection
Legal and Financial Considerations in Information Management

A guide to cost-effective discovery preparedness, records management, and privacy protection

John D. Martin
Jon A. Neiditz
Lucie H. Cohen

Table of Contents

> FRAMING THE ISSUE  2

It is economically and legally imperative that companies do a better job of managing information

> ANALYZING THE PROBLEM  3

The legal risks and costs of managing information

Discovery  3
Storage  4
Privacy and information security  5
Trade secrets and company-confidential information  5
Information management as a core competency  5

> THE TAKEAWAY  7

Successfully managing information mitigates risks and controls mounting costs

Organizational structure  7
Developing a framework  8
Technical capability  9
Moving forward  10
FRAMING THE ISSUE

It is economically and legally imperative that companies do a better job of managing information

The increasing role of discovery preparedness, records management, the protection of company-confidential information, and privacy and information security concerns in business requires companies to do a better job of managing and disposing of their electronic and paper records. The majority of litigation costs for the Fortune 500 – $210 billion, or about one-third of Fortune 500 profits – relates directly to managing and maintaining these records.

Organizations customarily retain records longer than the period of time required by business purposes or dictated by law. This exposes a company to significant risks, including:

- **Exorbitant discovery costs and risks**: Plaintiffs’ attorneys know that failures of either preservation or production can increase the settlement value of a case that might be substantively deficient. Moreover, discovery process management failure can result in the inadvertent production of documents highly damaging to a company’s claims or defenses.

- **Expense of maintaining information**: A company that keeps records beyond the retention period increases compliance risks as well as the cost of records storage and of accessing important business information.

- **Breach of privacy**: Simply by attempting to respond to a discovery request, a company risks violating various privacy laws, especially in non-U.S. jurisdictions where privacy laws can be particularly demanding. Accordingly, disclosing personal information can negatively affect a company’s profits and tarnish the company’s reputation. As Warren Buffett once said, “It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.”

Although these issues should concern any general counsel or chief financial officer, many companies do not consider information management a core competency. Instead, companies often assign discovery preparedness, records management, privacy protection, and information security to distinct management units.

Successfully addressing discovery preparedness, records management, information security, and privacy and trade secret protection requires skilled advice in these areas, and includes robust policy, supporting technology, and process knowledge. This paper explores these challenges and offers proposals for organizing these functions under a single business function that manages information from creation to deletion.
ANALYZING THE PROBLEM
The legal risks and costs of managing information

Many companies do not have a defined process to dispose of a record when business needs or legal mandates no longer require its retention. This exposes companies to threats and costs in the following areas: discovery, storage, information security, trade secrets, and privacy.

Discovery

As plaintiffs’ attorneys become more technically astute, they are beginning to leverage the size and intricacy of corporate data against the corporation. Records retained well beyond their retention period are especially enticing targets, in part because as data increases and becomes more disparate across the system, it becomes more likely that the corporation will fail to meet some aspect of its preservation or production requirements. These failures can result in unwanted press and sanctions ranging from expensive monetary fines to termination of the action.

Changes in the Federal Rules of Civil Procedure

In December 2006, the Federal Rules of Civil Procedure (FRCP) were amended to specifically address electronic discovery. The modifications to the FRCP mean that electronically stored information (ESI) is now subject to discovery. The term ESI is meant to include any type of information that can be stored electronically. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments. The Federal Rule of Civil Procedure revisions affect corporations in a number of ways, including:

- All of a company’s data is discoverable in litigation, unless the company can specifically show that the data is inaccessible and the data’s production is too costly or too burdensome.

- The massive volume of data on corporate networks results in greatly increased attorney review costs for privilege and relevance. Some sources estimate that costs associated with document review can account for anywhere between sixty and ninety percent of total litigation expenses.

- Discovery disputes can sometimes swallow the merits of a case, and result in unfavorable settlements even when the corporate defendant has a strong case on the underlying facts.

As these illustrations show, the volume of a company’s data has a direct correlation to the burden and cost it will face in litigation. The more data the company retains, the more data it must identify, preserve, process, analyze, and review. Further, companies must have the technology and capability on hand to swiftly search, retrieve, and produce records upon a request by a party or upon an order of the court.
Discovery in the International Context

International discovery can have a large effect on companies, especially in European countries, which have some of the most exacting data protection laws. For example, the European Data Directive, which sets a floor for governance of personal data within the European Union, restricts processing of information in any way and information transfers to countries that fail to provide what the European Commission has determined to be adequate legal protection, which do not include the United States. The Commission considers U.S. protection policies inadequate. All members of the European Union and countries in the broader European Economic Area have privacy laws that build further on the protections of the Directive.

Because lawsuits filed in the United States often seek information regarding citizens from other countries, a company can find itself facing the paradox of trying to process and obtain data from a country that will not allow its release while a U.S. court is simultaneously mandating the company produce the same information.

Storage

Storing information can carry large costs for companies that fail to properly maintain records or do not destroy records after they are no longer needed for business and litigation. Specifically, one of the greatest costs incurred by a company comes by way of storing unstructured documents, including spreadsheets, database files, and presentations, on file servers, company shared drives, email servers, and other repositories.

These systems often contain data that is neither structured nor sorted by class. Typically, the files and records are organized based on the varying decisions of thousands of individual users. Accordingly, companies operating these storage environments can encounter numerous difficulties, such as:

- **Repetition and waste**: Multiple copies of the same file can be stored in several distinct locations across the network. For example, e-mail can be dispersed across e-mail servers, local archives, and backup tapes.

- **Unclear record coding**: A document’s creator, creation date, or last edited date are not clearly coded. This makes it difficult to determine whether a document has passed its retention period. Further, these file repositories can contain business records, personal documents, or inaccessible files.

- **Search problems**: Because documents are not uniformly organized, they cannot be easily searched or centrally indexed.
• **Unproductive**: Accessing documents in these repositories for knowledge-sharing is virtually impossible. Most departing employees leave behind filing systems that are typically meaningless to anyone else, resulting in the loss of valuable data.

Without appropriately addressing these challenges, a company will find itself paying increasingly more money to store business records while losing the capability to access and manipulate these records.

---

**> Privacy and Information Security**

As mentioned in the context of discovery, individual states, the federal government, and other countries impose various legal obligations on a company to guard against the unauthorized use or disclosure of personal information under its control, to require safeguards on that information, and to require notification of individuals and regulators when breaches occur. Maintaining personal data beyond its business needs and retention period unnecessarily increases the amount of protected personal data, and by extension increases the company’s exposure if a breach of that data occurs.

This risk of breach is compounded by propensity of some companies to treat certain information, such as an employee’s HR file, as less important than other types of records such as intellectual property. Some companies will outsource the handling of HR and other similar records without an appropriate agreement outlining a procedure for ensuring that the privacy and security of these records is protected and any breaches carefully and jointly addressed.

The evolving technological landscape also implicates privacy concerns. Advances in technology, such as more innovative marketing through social media, raise the risk that a company might disclose protected information.

---

**> Trade Secrets and Company-Confidential Information**

Many organizations see their electronic information as a critical asset that must be protected against insider and growing outsider threats. As news organizations around the world create anonymous electronic drop-boxes to encourage anonymous whistle-blowing and the black market for trade secrets and other confidential information continues to expand, organizations are expanding their information management programs to include confidential information.

---

**> Information Management as a Core Competency**

Given the overlap of discovery preparedness, records management, and privacy protection, companies should consider these concepts as a group of linked information management issues critical to a
company’s financial wellbeing. A company should approach information management in the same way it would approach any of its central business functions.

Companies might be able to identify their wage and benefit costs per employee, but many companies do not know their per employee information cost. In the litigation context, these information costs per employee include the cost of identifying key custodians, preserving relevant records created by that custodian, hosting and reviewing those records in the event of litigation, and producing those records.

As part of managing its litigation costs, Chief Financial Officers (CFOs) and General Counsel (GCs) should know:

• the cost to the company of producing information for a single custodian;
• the amount of savings to the company if the number of custodians was reduced;
• the per-record cost of production; and
• an estimate of the cost of discovery and in which financial period those costs will be incurred.

Managing Costs by Examining Tools and Pricing
The various costs of discovery are not always apparent. A company’s litigation costs can be spread over a number of outside vendors and legal providers and can be reflected in various distinct invoices. Pricing models for discovery tools can also be different from one vendor to the next, hampering the ability to perform an adequate price comparison. It is therefore essential to legal data management budgeting that a company employ or develop or retain expertise in both pricing models and the functionality of discovery tools.

For pricing models, there are several options. When having data collected, companies could pay a flat price per custodian, or retain a service that charges a per-hour fee for data collection. Companies also need to examine processing costs, and make various decisions early in the data collection process that will drive the overall expenditure. In some cases, it may make more financial sense to license a culling tool that would produce only targeted data for ultimate review.

Price will also be driven by data storage costs. Charging methods for data storage can vary wildly, with some vendors charging flat rates and other charging fixed prices per gigabyte. How the vendor defines stored data can also vary. It might include only that information produced from a keyword search, or it could include the total amount of data loaded onto a review platform. Loading the data into storage can also create significant costs. For example, it may only cost a few cents to create an image file from a document, but in a large company, it is not uncommon for these projects to involve millions of pages. The costs of reviewing data, when examined over the context of the entire project, can be quite expensive.
Importance of Disposal
Regardless of how efficiently a company manages its information, it will never be able manage its discovery costs if it does not properly dispose of its information. There is simply no substitute for reduction of data that is no longer needed for business or legal purposes.

It is common for many divisions within a company to express hesitation when being asked to delete long-held records and data. This is why companies need to be careful to define a procedure that specifically delineates the records subject to retention, defines the record’s life, approves disposition of data not subject to a legal hold, and establishes a process for the actual purging of data.

THE TAKEAWAY
Successfully managing information mitigates risks and controls mounting costs

Properly addressing discovery preparedness, records management, information security, and protection of privacy and confidential information is vital to successfully managing legal, business, and reputational risks and controlling mounting data storage and discovery costs. Companies who have successfully addressed these issues have done so by understanding the information they collect, retain, and use.

Companies risk billions of dollars by not properly managing their information. Our extensive experience in litigation, technology, privacy protection, and vendor management enables Encompass to help clients anticipate and manage information-related risks. Based on years of helping clients meet these challenges, below are our suggestions to help your company gain control over its information:

> Organizational Structure

- **Appropriately delineate information management responsibility:** Several groups within a company have responsibility for effectuating a comprehensive information management policy, including executive level leadership, the legal department, privacy compliance officers, and information technology. It is critical that a company define the roles for the personnel in each group.

- **Information management should span the entire corporation:** Companies must ensure that individual business units, who often employ their own internal practices, understand their role in the company-wide information management plan. Executive level leadership plays an important role in providing a meaningful dialogue with other business unit leaders throughout the company.
• **Train employees:** At its core, an information management system will fail if the personnel who create and handle records do not understand the company’s information policies. A company must effectively train these employees to ensure compliance with its policies.

Many employees will be reluctant to delete long-held records and data. Companies must make sure that their information management strategies operate in tandem with their overall business strategies.

> **Developing a Framework**

• **Information classification:** Discovery-ready companies use data maps, arranged by comparative risk, to locate their data and have written processes in place to document its preservation, collection, and production. They follow their processes consistently, regardless of whether corporate or retained counsel is leading the production process.

• **Build powerful compliance programs:** Create information management programs that address business needs and legal requirements. A sound records policy, retention schedule, electronic resources policy, and preservation program is the solid foundation of a robust data remediation program. This foundation will support the disposition of legacy data, including legacy tape remediation, and the disposition of boxes of outdated paper records stored in warehouses.

Properly disposing of unnecessary documents will also be of high value in future litigation. Fewer documents will be produced, inherently reducing the cost of discovery and increasing the quality of the produced information. A well-established retention policy also operates as a defense in litigation. For example, the presence of an effective records management system before litigation can result in a court finding that inadvertent production of a privileged document does not constitute waiver of attorney-client privilege.

• **Institute detailed controls:** Through proper data organization and framework, companies can develop controls that tie together records management, security, and privacy. Companies are routinely developing data-specific safeguards, including the following:

  o Creating a review and management procedure for non-U.S. data that is compliant with international privacy laws.

  o Developing best practices and requirements for the coordination of outside counsel on electronic discovery issues to ensure consistency, defensibility, and efficiency.
Creating a central location, often a web-based portal, where employees can research the retention periods for certain types of records, view legal holds, or log instances of data purging.

Developing preservation and collection strategies for emerging data sources, including voicemail, instant messaging, outsourced data hosts, PDAs, and other portable storage devices.

Developing efficient remote, deskside, and network-level collection procedures utilizing both in-house and outsourced personnel.

Utilizing a method for purging legacy data, such as information from retired servers or paper documents.

> Technical Capability

- Even the most well-developed information plan is useless if it is not accompanied by reliable and effective technology. This requires companies to evaluate the capability of their existing systems, and either scale back the technology to accommodate the system or, as is most often the case, upgrade the systems to accommodate the technology.

- There are several tools that can facilitate information management and discovery.
  
  - **Review platforms**: There are hundreds of software vendors willing to host a company’s data and sell that company the software needed to review the data. Different review strategies may require different review platforms. Some platforms offer a tediously conventional database that merely lists all of a company’s documents, while other platforms feature innovative visual interfaces that can perform multiple searches that return responsive documents by searching through available fields.

    Companies might also look to single provider to manage its document review. For example, Encompass offers a full-scale document review service on a fixed-per-unit basis, which provides predictable review cost and shifts the risk of inefficiency from the client to Encompass.

  - **De-duplication tools**: Data de-duplication techniques rid systems of extraneous versions of the same information, be it across custodians or by threading email. This results in data that is qualitatively the same, but quantitatively less voluminous, making it easier and less expensive to store and review.
Legal hold technology: Web-based legal hold tools can integrate the legal hold process with a legal department’s information. Companies can automatically monitor progress, set reminders, and enforce a policy to escalate the request to higher levels if needed. A full audit trail of notices and responses proves measures are being followed.

Archiving e-mail: E-mail archiving tools allow companies to centrally manage email, and retain those emails without involving the individual account holders. Archiving systems can also save space on enterprise mail servers by moving older messages and attachments to inexpensive storage, leaving behind a ‘stub’ or placeholder.

Network crawlers: These tools continually analyze network resources and can identify content residing on file shares that is unstructured or uncategorized.

Given the pace at which technology evolves, and the rate of employee turnover at large companies, organizational and information management technologies should be regularly reviewed.

Moving Forward
In today’s business landscape, litigation is a reality. The ubiquity of personal data and electronic records means that discovery preparedness and privacy protection should drive the way a company thinks about and approaches information management. Responding to a discovery request, a regulatory investigation, or a subpoena should be a routine business practice, and not an unplanned emergency. A dedicated, qualified, interdisciplinary team, with clearly defined roles and responsibilities, should lead company efforts.

A growing movement is to employ a single provider to address discovery preparedness, records management, information security, and privacy protection. A company can lower costs, gain efficiency, and increase defensibility of its processes by centralizing responsibility with one firm that has a deep knowledge of information-related legal issues and an understanding of the technology and transactions that create those issues, informed by a robust, trusted complex litigation practice. At Encompass, we have that expertise, and we work with clients across a multitude of industries to develop and customize defensible e-discovery, records management, security, confidentiality, and privacy protection strategies, with a heavy emphasis on cost reduction.

If you have any questions about the Encompass approach to information-related legal issues, please contact John Martin at (803) 255-9241 or john.martin@encompassediscovery.com.

Encompass is a wholly owned division of the law firm of Nelson Mullins Riley & Scarborough LLP located at Meridian, 17th Floor, 1320 Main Street, Columbia, SC 29201.