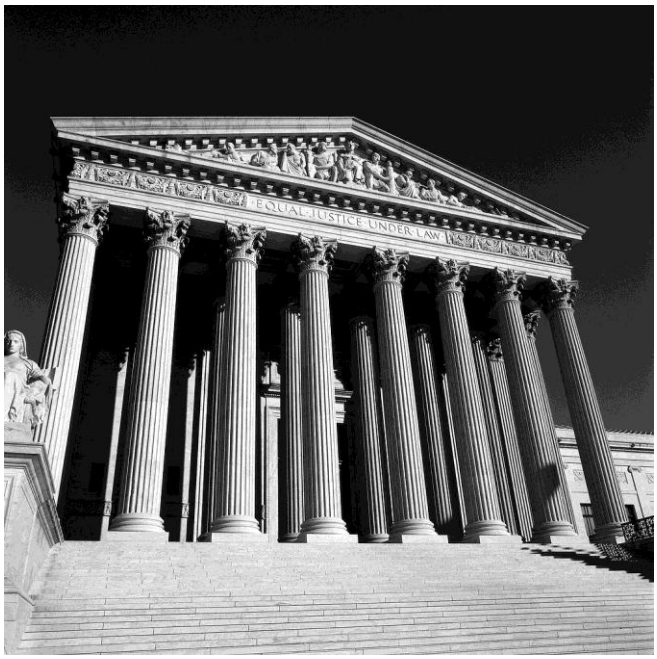
MessageSolution™
Customer Driven Trusted Partner



ELECTRONIC DISCOVERY & LITIGATION SUPPORT

A Primer by MessageSolution, Inc.

The recent influx of federal and industry email regulations combined with the increased use of electronic discovery in court rooms weigh heavily on many organizations today. More than ever, today's businesses must consider the ever-present threat of legal complications. The United States Supreme Court's changes to the Federal Rules of Civil Procedure (FRCP) a few years ago have brought attention to the importance of electronic records to the discovery process in the U.S.

The Federal Rules of Civil Procedure are a set of guidelines set by the U.S. Supreme Court regulating court procedure for civil suits. The Supreme Court made revisions to the FRCP in December of 2006 regarding electronic discovery, which became effective December 1, 2007. The FRCP changes stipulate that potential documents required in a case can originate from any data, as long as it is assembled into a visible form.

Under these revisions, electronic documents such as email, instant messages, or calendar files, and traditional documents stored electronically must be available for timely search and retrieval in the event of litigation proceedings. Discovery must be maintained in its original format. Accidental deletion, misplacement, or any inability to locate data before deadlines will result in court fines.

Data Considered Critical Evidence:
E-mail and attachments
Plain text and documents
Images
Calendar files
Databases
Spreadsheets
Digital faxes
Audio files
Animations
Web sites
Computer applications
Viruses and spy ware

Where Can E-Discovery be Found?

E-discovery can be found on file servers, on email servers, in backup storage, or even on individual employees' desktops. Part of what makes electronic discovery so problematic is the availability of electronic records to employees, who may not always make the best choices as to the final location or format of its preservation…if it should even be preserved at all. Employees may delete or misplace emails, attachments and files based on ignorance, negligence, or willful misconduct.

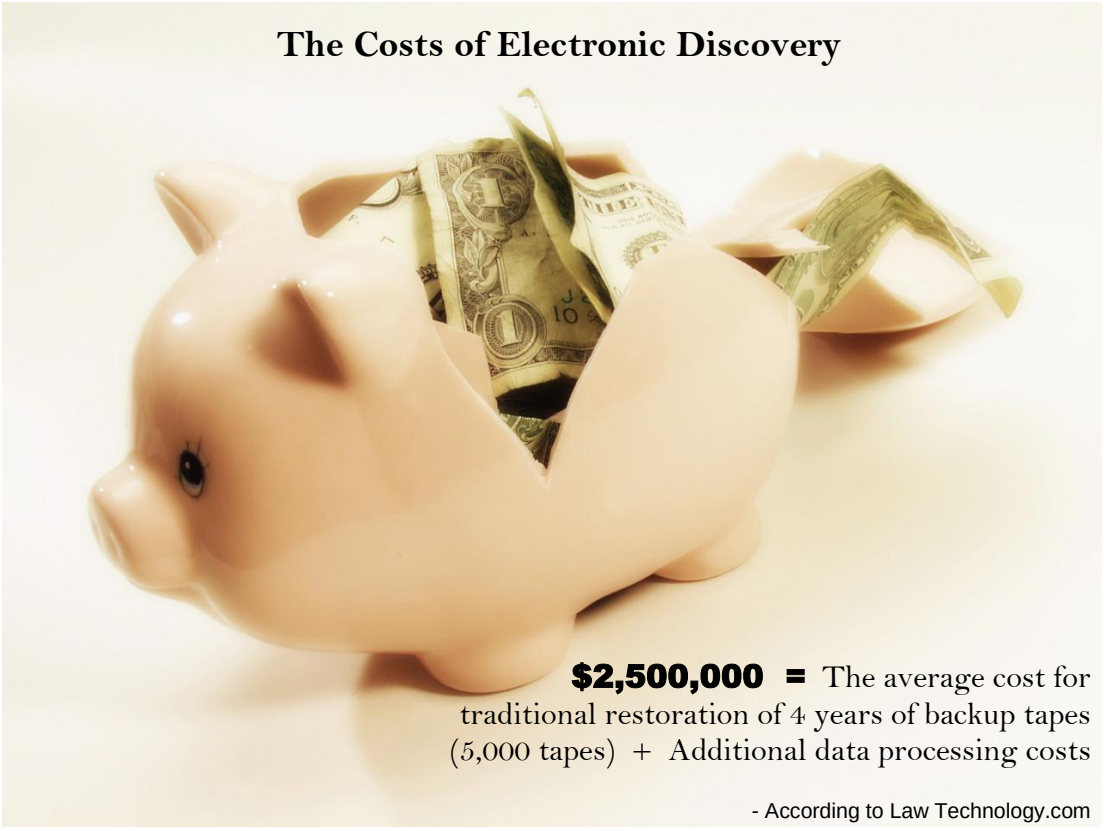
Sometimes employees are worried about the retention of their emails, attachments and files, which they need to carry out their daily activities. When quotas are placed on email inboxes, users often decide to create their own personal storage files (PSTs, NSFs, etc.) to ensure they have access to these records. This seems ideal to users, but from an e-discovery and litigation standpoint, it is inconvenient and sometimes risky.

When users have local archive files, IT and executive management have no idea what kind of information may be found in the discovery process. This is especially dangerous with emails in the case of lawsuits for many reasons:

- If the email in question is between your company and another party, chances are that the other party has a copy of the email, even if you don't. As with many things, in court, information is power. Litigation is hard enough without 'surprises' coming up.
- The alternative to finding incriminating information is *not* finding emails or files that could exempt your company from any implications of guilt in a case. When users have free reign over their emails and files (which are ultimately a company's intellectual property), they may delete emails that implicate them or provide evidence of their own wrongdoing, placing the company at risk.

The Challenges of E-Discovery

The nature of electronic documents makes them especially troublesome to discover. Requested versions of an attachment may have been lost or deleted. Sometimes incriminating emails that employees thought had been deleted forever are recovered. Documents that have been retained may not be centralized; multiple employees' computers may need to be searched, along with corporate servers. Realizing the scope of their needs, many companies turn to expensive legal forensic specialists to perform the traditional legal discovery process.



Electronic discovery can be requested in a lawsuit by the opposing party. The cost of e-discovery is paid by the company producing the discovery, not the company requesting the discovery. This is true even for third parties subpoenaed for evidence; rarely does a company that has never been involved in litigation consider that it may be forced to produce electronic discovery simply for having done business with another company that *is* involved in litigation. Electronic discovery requests can have deadlines of less than a week, causing IT members to halt normal operations to scavenge for discovery.

Electronic discovery requirements can be strenuous, and rarely can the case be made that the evidence is so difficult to retrieve that the request should be rescinded. Outsourcing the project to legal forensic experts can be extremely expensive and still does not guarantee results in time to meet the often brief court deadlines.

Traditional electronic discovery methods can be extremely costly and time-consuming. In fact, very often they fail to produce the required evidence by the date mandated. Judges are increasingly less likely to accept that documents were lost, deleted or not able to be recovered in a timely manner. Some judges will consider late electronic evidence submissions signs of carelessness or willful concealment. Many companies have been levied hefty fines for not producing evidence in time or at all.

Knowledge Really Is Power

Knowing what is contained in your company's emails and files informs the legal department when they decide what should be retained or deleted. Giving individual employees final say on retention can result in unpleasant surprises come e-discovery time.

- **Centralized management of electronic records.** Archive emails, attachments and files on a centralized platform, where you can refine the records to further analysis and distribution. No emails or files can sneak up on your company in court when everything is collected for internal review.

- **Manage desktop archive (PST, NSF) files.** Purge your company of these pesky files forever, which decentralize storage records and are also easily corrupted. Most archiving products today provide migration utilities to import PSTs and NSF files into the archive for centralized management. Archiving data will also eliminate the root cause of PST/NSF creation: email inbox quotas. Archiving allows employees to access their emails and attachments, removing the need for employees to create local archive files.

- **Simplify e-discovery.** Reduce e-discovery labor pains with an archiving solution designed for e-discovery support. When all of your company's emails, attachments and files are easy to search, print, and send, e-discovery becomes less labor-intensive and requires less technical knowledge. The archive gives the legal team the ability to perform and save searches, retrieve data, and email or print discovery without IT assistance.

Archiving for E-Discovery Purposes

Archiving products improve upon traditional discovery practices with improved discovery return times, intelligent filtering of data to reduce data processing time, comprehensive search parameters, and quick and easy export capabilities. Today's archiving products put the power of e-discovery at businesses' fingertips, giving legal counsel the convenience and freedom of searching, recovering and delivering evidence needed for a case without the cost of legal forensic specialists or help from the information technology department.

Businesses can store data on infinitely by simply adding new storage hardware. Archiving solutions with e-discovery features have an edge over typical discovery methods in that most archiving solutions compress storage volumes, which lowers the requirement for additional storage capacity. Online and offline security eliminates the possibility of accidental data deletion, while legal hold capabilities allow businesses to retain case-relevant records for a unique time period.

Steps to Take to Prepare for E-Discovery

The key to avoiding legal fines and last minute scrambling for discovery requests is preparation:

- Having a company-wide email policy is a good start.
- Having a way to enforce that policy is even more important to ensure that critical evidence is not lost or accidentally deleted; archiving your emails and files using products with built-in automated policy application tools is the best way to ensure policy enforcement company-wide.
- Once data is archived, develop a litigation hold game plan.
- The final step is having a fast, accurate pathway to retrieve electronic data; a full-text indexing database and advanced search features are built into all MessageSolution's products.

