Email Archiving: A Proactive Approach to e-Discovery
This whitepaper addresses the key e-discovery challenges facing legal and IT departments today, form the impact of regulations such as the Federal Rules of Civil Procedure (FRCP) to the technology required to deal with them. Finally, this paper describes how businesses can develop a proactive strategy to deal with e-discovery requests in the event of litigation, saving time and money in the process.
Introduction
Email and other electronically stored documents are now routinely presented as evidence in courts of law. To ensure litigation readiness, both legal and IT departments must address the management of electronic communication in their organization. Without the right tools in place, collecting, processing, and reviewing electronic data for e-discovery can be time-consuming, expensive, and expose a business to significant legal risks.

To effectively prepare for litigation, legal professionals must have some understanding of the technology required to store and retrieve electronic documents. Similarly, IT professionals must be familiar with the laws and regulations that impact their organizations. The most significant and widespread of those regulations are the Federal Rules of Civil Procedure (FRCP), which apply to any business that may be engaged in federal litigation. These rules clearly outline expectations for businesses to apply a consistent retention policy for email, enforce litigation holds and produce relevant or requested email evidence in a timely manner.

This whitepaper discusses the key e-discovery challenges facing legal and IT departments today, from regulations such as FRCP to the technology needed to effectively to address them. It also describes how businesses can develop a proactive strategy to deal with e-discovery requests in the event of litigation, saving time and money in the process.

The Scope of Electronic Discovery
Electronic discovery typically refers to the retrieval of electronic data to meet a legal request. However, the term is also used when data is retrieved for regulatory compliance, HR concerns, validation of client correspondence or other corporate needs.

Recently, the electronic discovery burden on IT organizations has increased both in frequency and demand. In fact, a survey performed by Osterman Research, Inc. found that during the past three years, 72% of IT organizations were required to search through backup tapes to retrieve one or more email in response to a legal or HR request. The same survey found that nearly 38% of organizations were ordered by a court or regulatory body to produce employee email.

These statistics are not surprising when you consider the way email is used for day-to-day business communication. After all, sexist, racist and other inappropriate content—which would be deemed unacceptable in other corporate settings—can often be found in employee inboxes. As a result, email evidence routinely comes to play in HR-related cases and has been the “smoking gun” in numerous cases of illegal corporate activity.

As the number of e-discovery requests continues to grow, virtually every organization requires search and discovery capabilities, even if they are not actively involved in litigation.

The Impact of e-Discovery
There is ample evidence to suggest that if a corporate IT department has not already been involved in e-discovery, they soon will be. In fact, 83 percent of U.S. corporations are engaged in some type of litigation, according to an independent annual research survey by the law firm Fulbright & Jaworski. Since most of those cases involve email, the likelihood of facing an e-discovery request is very high.

Without the right tools and processes in place to effectively search and retrieve requested information, a number of serious consequences can result. These can range from fines and adverse inference judgments based on spoliation (see definition at right), to a damaged corporate reputation or even criminal charges. And this does not take into account the significant costs a business can incur trying to retrieve and search through data.

Meeting Requirements of the Federal Rules of Civil Procedure
The Federal Rules of Civil Procedure (FRCP) were amended in December 2006 to help clarify how electronic information should be handled during federal litigation. Since then, there have been numerous case law examples to support a proactive approach to storing and accessing email for e-discovery. In fact, in the year following the amendments, 105 legal opinions involving e-discovery were reported, making it clear that the courts are taking this issue very seriously.

Email Archiving: A Proactive Approach to e-Discovery
Legal Discovery Defined
Legal discovery is part of the pre-trial phase in a lawsuit. During legal discovery, the parties involved in litigation can request documents and other evidence from the opposing side. They can also compel the production of evidence by using a subpoena or other discovery devices, such as requests for production and deposition. These discovery orders can target any source of data within an organization, but frequently the email system and file servers are at the top of the list. According to Socha Consulting, for the average case, email represents 80 percent of the requested documents for discovery.

Litigation Hold Defined
When an organization expects to be the target of legal action, it is obligated to stop destruction of all documents and records that may pertain to the upcoming litigation. According to the FRCP requirements, this includes email messages and attachments. A litigation hold is a process used by companies to advise their employees of pending or anticipated litigation and ensure that relevant records are not destroyed. Failure to preserve documents for a litigation hold can have very negative consequences during a trial (see spoliation, below). Despite this, few companies have implemented technology to prevent such destruction of records.

Spoliation Defined
When a company accidentally or intentionally fails to preserve evidence during a litigation hold, it is called spoliation. Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for use as evidence in pending or foreseeable litigation. Spoliation is considered a criminal act and may result in fines and incarceration. It can also lead to a negative inference finding that can ultimately lead to a guilt verdict.
**Fast Facts about e-Discovery**

Employee email is subpoenaed with surprising frequency:

In its March 2008 survey of more than 300 email decision makers at US enterprises with more than 1000 employees, Proofpoint found that nearly a quarter (24%) of companies were ordered by a court or regulatory body to produce employee email in the past 12 months alone.

The larger the company, the more likely it is that email will have to be produced. Of companies with more than 20,000 employees, more than one-third (34%) had employee email subpoenaed in the past 12 months.

Osterman Research found that nearly two-thirds (63%) of organizations have been ordered by a court or regulatory body to produce employee email or instant messages. Additionally, two-thirds (66%) of IT organizations have referred to email or IM archives or backup tapes to support their organization’s innocence in a legal case.

**Email Archiving Solutions Save Time—When You Need it Most**

Osterman Research also found that it takes a median time of eight person-hours to satisfy a single request to retrieve data from backups and a median of two days elapsed time.

However, organizations that have an archiving solution in place report that it takes a median of just 30 minutes to conduct a single search across the entire archive.

To understand how the regulations could affect your organization, you must first have a grasp of what the rules require when a potential lawsuit comes up. At the most basic level, FRCP requires a business to be prepared to do the following:

1. Apply a litigation hold to ensure that no relevant data is deleted for any reason before the case is settled or goes to trial.

2. Confirm what data exists, where it is located, and agree on discovery terms at a “Meet and Confer” session (within 99 days of a lawsuit being filed).

3. Search and retrieve requested data and present to opposing counsel within timelines set during the “Meet and Confer” session.

The rules also make it clear that any existing data is discoverable, regardless of the where it is located and how much it will cost to recover. Data that is requested for discovery but cannot be retrieved (including lost or corrupt data files) may result in a finding of spoliation (see definition of spoliation on page 1). The exception to this would be any data that was destroyed according to a stated retention policy, before a litigation hold was put in place.

**The Burden on IT**

While the basic requirements for e-discovery may not sound too difficult, the reality is that many companies are largely unprepared to respond quickly to a legal request for electronic documents. Without an archiving system with search and discovery capabilities, an e-discovery request can add up to significant time, effort, and expense on the part of the IT department. The volume of data for a mid- to large-sized company is often overwhelming, with potentially hundreds of backup tapes and millions of email messages to sift through.

Searching and restoring data from various sources—PCs, servers, and backup tapes—is not an easy process. Every time an organization faces a lawsuit or investigation, IT may be required to take the following steps:

1. Issue a litigation hold notice to employees, requiring them to preserve any email relating to the legal case.

2. Identify and stop routine deletion or recycling of any data source that may contain email covered by the litigation hold. This can include email servers, backup tapes, PST files on PCs and the corporate network, etc.

3. Scan all data sources for relevant content by filename, type, date, custodian or other criteria. Prepare a catalog of original files for legal counsel.

4. Locate and gather data requested for discovery. Restore the email, the associated metadata and attached files. (In addition to purchasing mass storage to house the data, your IT department may need to replicate both the hardware and software used to create the backup tapes, plus the email management system from which the messages were generated.)

5. Convert email to a standardized format such as HTML, PDF, SMTP/MIME, or TIF. Load the restored and converted data to a review system.

If carried out internally, this multi-step process generally falls to the organization’s IT department. The right hand side of Figure 1 (next page) shows the many steps involved in finding, restoring, cleansing and de-duplicating data residing within the corporate network. These steps must be repeated for each backup tape, PST file and email server—for each discovery request.

In addition to the time and cost involved for IT, the typical e-discovery process introduces other challenges. First, it is time-consuming, just at the point when time matters most. The longer it takes to get your legal team access to the data they need, the less time they have to get full command of the facts of your case, and the more you are at risk to be fined for missed deadlines or for production of partial information correspondence. Additionally, the results may have limited evidentiary weight because there is no way to prove that items have not been deleted or tampered with.
Email Archiving—A Proactive Approach

Many businesses continue to deal with e-discovery requests reactively, on a case-by-case basis. As discussed above, this approach can expose an organization to a number of risks, and can end up costing a great deal of money, not to mention time on the part of IT to perform data recovery. In fact, the costs can be so great, that as many as one in five businesses have settled a case simply to avoid searching through and retrieving email data.

As more companies are hit with the high costs of an e-discovery request, the benefits of an alternative, proactive approach become clear. Implementing an email archive can help organizations to easily meet comprehensive legal discovery requests, while providing a number of additional benefits including:

1. **Lower costs:** An archive with advanced search functionality can reduce the overall cost of discovery by tens- or even hundreds-of-thousands of dollars.

2. **Reduced risk exposure:** By automatically capturing all email, an archive can act as an easily searchable, central repository that meets evidentiary standards, complies with FRCP and eliminates the risk of spoliation.

3. **Consistent policy enforcement:** A policy-driven archive ensures that data is consistently retained and disposed of, meeting FRCP requirements.

4. **Improved response times:** As a centralized repository with search functionality, an archive can eliminate the need to mine multiple sources of data in order to meet a discovery request. Advanced search tools can also dramatically reduce the time it takes to complete a request—in some cases from weeks or months to just minutes or hours.

5. **Early case assessment:** Easy search access can allow legal counsel to evaluate the merits of a case before investing time, money and effort in electronic records retrieval. This can make it easier for counsel to make better decisions about whether to fight or settle a case.

6. **Email storage management benefits:** Many archiving solutions provide the added benefit of allowing IT to greatly reduce data storage burdens on email servers, enabling improved email server performance and delivering significant email storage management benefits.

---

**e-Discovery Case Law Examples**

In the year following the amendments to the Federal Rules of Civil Procedure (FRCP), more than 105 court opinions on electronic discovery were issued. A summary of some of those opinions follows:

**Best Buy vs. Developers Diversified Realty (February 1, 2007)**

In this case, the defendants argued that the emails requested by Best Buy were not “reasonably accessible” (they existed only on archived, electronic backup tapes). Diversified cited a cost of $125,000 to recover the information. The judge did not accept the argument and ordered that the information be produced within 28 days, including IT time and legal preparation.

---

Figure 1: Easing the e-discovery process—Proofpoint ARCHIVE (at left) versus the “traditional” approach (at right).
How Proofpoint ARCHIVE Can Help

The Proofpoint ARCHIVE™ solution offers a cost-effective way for businesses to meet the demands of the Federal Rules of Civil Procedure (FRCP), without adding to their existing infrastructure or IT staffing requirements. This Software-as-a-Service (SaaS) solution allows businesses to centrally archive all email, enforce policies and litigation holds, perform enterprise search and easily conduct early case assessment, all for the same—or less—cost as storing and managing the data on premises.

As a SaaS solution, Proofpoint ARCHIVE also offers:
- Minimal upfront capital investment and predictable, ongoing costs
- Fast and easy setup with minimal maintenance by IT
- Real-time search and retrieval of archived email
- Full scalability to grow as your needs increase
- Full preparation for legal discovery on-demand

Forensically-compliant Archived Email

Proofpoint ARCHIVE allows you to securely store all your internal and external communications, in a forensically-compliant way, within minutes of being sent or received. To ensure that archived data meets evidentiary standards, Proofpoint ARCHIVE keeps original copies of all email, and guarantees that records cannot be deleted or altered during their retention period.

Proofpoint ARCHIVE ensures the authenticity and security of all archived data by:
- Storing multiple copies of messages and indexes on spinning disks
- Digitally fingerprinting all messages for authenticity
- Maintaining a full audit trail of system and user activities
- Fully indexing records
- Encrypting data before transmission to the archive and storing data in encrypted form “in the cloud” using patented Proofpoint DoubleBlind Encryption™

Consistently Enforced Policies

To protect your business from legal risks and meet the Federal Rules of Civil Procedure (FRCP), you need to enforce a consistent corporate messaging policy. Proofpoint ARCHIVE’s policy interface guides you through the process with clear instructions and flexible options to help you create, maintain and—most importantly—enforce your policy, right from a Web-based user interface.

Proofpoint ARCHIVE’s policy interface offers:
- Easily customized, industry-specific policy templates
- PDF policy download for easy distribution to employees
- Individual policies can be created to address different roles or individuals, the content of a message (and attachment), date ranges, and whether the communication was internal or external
- Automatic enforcement of policies
- Tracking of every policy change in unalterable form

Litigation Holds

When a message is archived, it is assigned an appropriate retention period based on your policy. In the case of impending lawsuits, you may require certain messages to be preserved beyond their retention period, until the matter is closed. Proofpoint ARCHIVE allows you to easily assign messages to a litigation hold folder using a Web-based interface. Messages assigned to a litigation hold are kept indefinitely until the hold is released.

Rapid Search and Retrieval of Messages

With a distributed search architecture and grid-storage infrastructure, Proofpoint ARCHIVE can guarantee the real-time search and retrieval of data, regardless of how large the archive grows or how often searches are required. Through a Web-based user interface, legal or IT staff can

---

Intel vs. AMD (April 2007)

In this case, Intel claimed that it put a clear retention policy in place once it learned of AMD’s legal intentions. Employees, however, didn’t always follow the instructions. Intel was compelled to search back-up tapes to produce past email messages. In April 2007, the Wall Street Journal reported that Intel “spent $3.3-million to process computer tapes to help recover missing emails and expects to spend ‘many millions of dollars’ in the effort.”

Doe vs. Norwalk Community College (July 16, 2007)

In this case, the court specifically cited the defendant’s failure to “put a litigation hold in place.” The court said that Doe was entitled to an adverse instruction to the jury regarding destroyed evidence. In addition, the court awarded some legal fees and the reimbursement of expert fees.

Qualcomm vs. Broadcom (October, 2007)

In this case, the plaintiff, Qualcomm, failed to produce thousands of email messages. During one of the last days of trial, cross-examination of the plaintiff’s witness revealed the existence of relevant emails that the court later held were “the tip of the iceberg” in an attempt to conceal over 200,000 pages of relevant emails. This revelation resulted in a judgment finding for the defendant plus an award of attorneys fees, sanctions of more than $8 million on Qualcomm and disciplinary sanctions on six Qualcomm lawyers.
quickly and easily meet even the most stringent legal discovery requirements. Search results are returned in seconds and search performance is guaranteed by Proofpoint's unique search performance service level agreement. Real-time access to the archive allows legal counsel to conduct early case assessment which can provide valuable insight into how a case should be handled.

Proofpoint ARCHIVE’s advanced search features include:

- Full-text searches of the subject and body of email and more than 250 types of attachments
- Highlighted search words that make it easy to find relevant data
- Frequently used search criteria can be saved
- Search results can be stored in folders where duplicate messages are automatically removed
- Search results can be printed or exported to a PST file for download
- Retrieve results from several users with multiple email addresses in one search request, dramatically reducing search time

**Improved Email Storage Management**

In addition to the many e-discovery benefits, Proofpoint ARCHIVE’s stubbing feature can significantly reduce the demands on Exchange, improving email storage management. This feature enables organizations to reduce their Exchange store by as much as 80 percent by replacing storage-intensive attachments with a pointer to the archive, providing seamless access to the attachment from Outlook.

**Conclusion**

The growing cost of e-discovery, compounded by new regulations, is forcing businesses to ensure they are prepared for legal discovery. By taking a proactive approach and implementing an email archiving solution such as Proofpoint ARCHIVE, businesses can reduce their exposure to significant financial and legal risks while meeting electronic discovery requests on time, within budget, and without internal disruption.

**Citations**


**For Further Reading**

Proofpoint offers a variety of free educational whitepapers that further describe the risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks. Visit our online resource center at [http://www.proofpoint.com/resources](http://www.proofpoint.com/resources) for the latest information.

**About Proofpoint, Inc.**

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-premises (appliance), on-demand (SaaS) or in a hybrid architecture for maximum flexibility and scalability.