proofpoint. LOGIN

/ Glossary / What Is E-Discovery?

What Is E-Discovery?

Download the E-Discovery Trends & Challenges E-Book

Compliance and E-Discovery Insights Webinar

Definition

E-discovery is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation.

How E-Discovery Works

Like any other form of investigation, e-discovery is a process with several stages and techniques. There is no one-size-fits-all methodology. Most e-discovery law firms perform an investigation using their own procedures.

But most processes include a few common stages. These e-discovery stages were created to improve collection, preservation and presentation of potentially relevant information. E-discovery typically includes nine stages. Here’s how they work:

IGRM model, which provides a framework for all e-discovery agencies to follow.

- **Identification:** When litigation is imminent, all parties must attempt to preserve evidence. But how do you know what data to save? In the identification phase, a team determines what data must be preserved by interviewing key stakeholders, reviewing case facts and analyzing the digital environment.
- **Preservation:** After data is identified, data owners are formally instructed to preserve data (and to not delete it).
- **Collection:** Several technologies exist to collect data, but the chosen application must follow a defined legal process. The team responsible for collecting data must ensure that digital assets are preserved without altering essential metadata such as file creation dates, size, and audit logs attached to each file.
- **Processing:** Raw collected data is usually unorganized and ill-suited to present to attorneys or the court. The processing phase of electronic discovery involves organizing data and finding the right assets for analysis. This phase can also be automated using software to extract important information from a sea of irrelevant data.

- **Review:** Reviewing documentation and digital assets can be done manually or by using artificial intelligence. During the review stage, pertinent information is separated from unnecessary data that is not relevant for the ongoing litigation. This phase also identifies documents subject to client-attorney privilege.
- **Analysis:** At this stage in e-discovery, digital assets become more organized for presentation. Reviewers identify patterns and key information critical for litigation and design a presentation layout used during trial or deposition.
- **Production:** Digital assets must be turned into physical documentation. After key data is identified, attorneys turn it into presentable evidence.
- **Presentation:** Evidence in litigation must be presented to other attorneys, judges, juries, mediators, and deposition participants. During the final presentation phase, data is organized in a way that makes it easy to parse and then convey to an audience.

Why Is E-Discovery Important?

The nine stages of e-discovery seem simple on paper. But the process can take months, and it gets more complex during higher-profile lawsuits.

Attorneys handle the e-discovery phases, so you might wonder why you should care or be interested in the way it works. The answer: e-discovery is critical for your success during lawsuits. Tampering with digital evidence or poorly executing any of these stages during e-discovery could lead to losing the lawsuit.

many of the regulatory standards that oversee private data storage and processing.

An audit trail helps identify who accessed data and at what time. E-discovery would help determine whether any inappropriate data access was due to an insider threat or system compromise. If the system was compromised, then the organization should consider investigating further to identify the vulnerability and contain the threats.

Why Do Some Organizations Struggle with E-Discovery?

E-discovery is often misunderstood, and often, doesn’t become important until a lawsuit is filed. Whether the organization is the complainant or the defendant, the process of e-discovery is often new territory as they work through each stage. Even with in-house staff, investigating data privacy violations and digital compromise can difficult. Even if the organization identifies an attacker, law enforcement needs proper evidence to file criminal charges.

Complicating matters, companies are often completely unprepared for the e-discovery process. It’s not an optional part of an investigation; all litigants must go through e-discovery procedures. Staying prepared, having the right controls in place, and keeping accurate audit trails are critical to identify and preserving relevant data.

Another issue is the sheer volume of data that must be collected. Organizations with large systems must know where data is stored and have access to retrieve it. This means that several people might be involved in finding and collecting data. It can take months to search large databases, and the right data must be made available to investigators in a timely manner.

And even if all data is identified, employees must be warned not to tamper or delete any of it. The team responsible for e-discovery will collect and preserve it. Still, it’s the responsibility of the entire organization to keep it intact and unaltered until it can be moved to a safe storage location. Data might not be on the network; it could be on an employee’s smart phone or mobile device. In these cases, the device must be surrendered and kept safe until data can be extracted.

Finding E-Discovery Solutions

E-discovery a decade ago was a manual process. But new software tools give organizations an automated solution. Some of these solutions incorporate artificial intelligence to help with the identification and review stages of e-discovery.

The e-discovery solution you choose should be easy to use and should integrate well with your system. If it works in the cloud, be sure to select a solution that has the right security controls on

If software automation is not an option, the organization must work with a law firm that will guide it through each stage. When choosing a solution, make sure that you find a law firm or a vendor experienced with digital analysis and electronic discovery, one that understands proper security controls to preserve data privacy.

Proofpoint Discover: E-Discovery Analytics Software

Proofpoint Discovery tools reduces risk with streamlined litigation readiness insights for investigations. Learn more about e-discovery analytics software.

Read More ›

Proofpoint Archiving and Compliance Solutions

Find out how Proofpoint's Enterprise cloud, data, and email archiving solutions help simply e-discovery and retain critical data across your organization.

Read More ›

Empower Legal Teams with Proofpoint e-Discovery Analytics

Proofpoint E-Discovery software reduces risk with streamlined litigation readiness insights for investigations. Learn what E-Discovery data analytics can do for you.

Read More ›

The ROI of Enterprise-Wide e-discovery: How To Save 5 Million Dollars

This blog explores the potential impact an enterprise-wide eDiscovery strategy can have on your bottom line, leveraging a study from Osterman Research.

Read More ›

Addressing e-Discovery & Compliance Requirements in Office 365

Download and read our white paper to get a comparison of key features between Exchange Online Archive and Proofpoint Enterprise Archive to see the Proofpoint difference.

Read More ›

Proofpoint Enterprise Archive and its optional e-discovery analytics with advanced e-discovery machine learning and analytics capabilities, let customers expedite early case assessment to help with proactive litigation readiness.

Read More >

< Previous Glossary

Next Glossary >

About

Overview

Why Proofpoint

Careers

Leadership Team

News Center

Nexus Platform

Privacy and Trust

Threat Center

Threat Hub

Cybersecurity Awareness Hub

Ransomware Hub

Threat Glossary

Threat Blog

Products

Email Security & Protection

Advanced Threat Protection

Security Awareness Training

Cloud Security

Archive & Compliance

Information Protection

Digital Risk Protection

Product Bundles

Resources

White Papers

Webinars

Data Sheets

Events

Customer Stories

Blog

Free Trial

proofpoint. LOGIN

+1-408-517-4710

Contact Us

Office Locations

Request a Demo

Support Login

Support Services

IP Address Blocked?

proofpoint.

Terms and conditions

Privacy Policy

Sitemap