# The E-Discovery Path to Litigation Readiness

Published on Alvarez & Marsal (https://www.alvarezandmarsal.com)

With an increasingly strict regulatory environment and a growing number of litigation cases, many corporate legal departments are revisiting their litigation readiness programs and finding that electronic discovery will be their biggest expense in the months ahead. The results of a recent litigation trend survey for 2011 by Fulbright & Jaworski showed that 92 percent of respondents from the United States and 85 percent from the United Kingdom anticipate a rise in legal disputes, reinforcing the critical need to properly interpret growing volumes of complex data and develop an effective discovery response plan.

Discovery–related adverse sanctions and negative outcomes on litigation at hand due to poor preparation are common, and electronic discovery costs are often unnecessarily high due to inefficient management, but all this can be avoided with an effective litigation readiness program. Are you ready for what's ahead?

Depending on the countries and jurisdictions in which your company conducts business, your duties and obligations of discovery will vary. The scope of data preservation and disclosure are typically much wider in the Common Law states, such as the United States and United Kingdom, than in the Civil Law states, such as Germany and France. However, generally across all jurisdictions, electronic discovery requirements are becoming more prevalent and steps should be taken to be "litigation–ready."

Companies often perceive e–discovery as a very costly and time–consuming process. However, with sufficient preparation and planning, discovery processes can be smooth and painless. Becoming litigation–ready does not have to involve large investments with enterprise–wide technologies and dedicated resources. While certain technology solutions can be highly effective, the appropriate level of technology implementation varies greatly from one company to another depending on the industry, company size, level of litigation exposure and the volume of data created.

Within the past 10 years, there has been an explosion of data. Over 90 percent of business is conducted electronically, and the volume of electronic data created and stored is becoming more challenging to manage. In 2010, 107 trillion emails were sent worldwide, which equates to an astounding 294 billion emails per day1. The rate of information creation is far exceeding the development of storage capacity — a recent study has concluded that the world's data is more than doubling every two years2. We need to better understand the information lifecycle process and improve the control of a company's data to perform discovery exercises effectively.

With some preliminary planning, companies can save substantial costs and mitigate liabilities both in the short term and long term. Below are three do–it–yourself (DIY) tasks that can be performed internally with minimal effort, but yield significant returns.

**DIY Step 1: Identify the Relevant Parties and Assign Responsibilities**
Identify the key players required to manage legal mandates and get them in the same room to plan ahead. This group should include team members from Information Technology, Legal, Compliance, Risk, Business and Management. A litigation response committee should be formed to respond to litigation requirements and lead the discovery efforts, as required. The committee should have full support from management to obtain the appropriate level of resources and attention.

Create a litigation response program that specifies clear roles and responsibilities, preservation protocols, data collection methodologies and disclosure processes. The minimum questions that the program should answer include:

- How will data preservation and legal holds be executed?
- How will relevant data sources be identified?
- How will the data be culled and collected?
- How will data be reviewed for privilege documents?
- How will data be processed and produced?
- Who will be responsible for each step?
- What are data privacy and protection considerations?

Document the program and make sure your protocols are defensible and auditable. The committee should meet on a regular basis to reassess the program and verify that it meets the current regulatory landscape and internal requirements.

**DIY Step 2: Know Your ESI**

Given the high volume of electronic information being created, you will need to know where all your electronically stored information (ESI) lies, along with the types of information stored at each of the source locations. The sources of information include employee computers, smart phones, email servers, file servers, backups, voicemails, external media and application systems, as well as hard–copy documents. Create an ESI map showing all such data sources and documenting the corresponding data types, relevant date ranges, backup policies and data lifecycle. Keep this ESI map up–to–date, as this will become a key resource for you in identifying potentially responsive data.

As part of your information governance program, make sure you understand the information lifecycle within your company. Email communications data are often the most difficult to manage because they frequently have high duplication rates. For example, an internal email to a department of 10 employees creates 11 copies of the same email, which is then multiplied to computers, blackberries, email servers and other backups. The recent proliferation of instant messaging and social media usage are also adding to the complexity of data collection and discovery. Depending on the business practices within your company, a centralized content management system with a single instance archiving solution may be beneficial and introduce significant cost–savings, both in ongoing business operations and discovery response.

Consider the accessibility of your data sources. As disclosure requests often come with tight timelines, be ready to produce them quickly when needed. If a data set is available from multiple sources, identify the most convenient source. Also, prevent having to process and disclose unresponsive data simply because the content of the data is unknown. Having a comprehensive understanding of your information lifecycle and a well–planned ESI data map will help you plan and budget your disclosure exercises, and minimize costs and exposures.

DIY Step 3: Create and Enforce Data Retention Policies

Data preservation is a critical legal requirement in anticipation of litigation. In most jurisdictions, including the United States and United Kingdom, whenever litigation is reasonably anticipated, the company has a legal duty to preserve all potentially relevant information and ensure that the data is not destroyed. With this requirement, companies often over–preserve and defer decisions on the appropriate retention periods or data removal. However, just as important as preserving the data is destroying the data you no longer need in a timely manner, provided that there are no pending preservation requirements. Even if the legal required retention periods have expired, any data you have at the recognition of anticipated litigation is subject to data preservation and discovery. Sometimes referred to as "skeletons in the closet," data unnecessarily kept beyond compliance requirements or business needs may expose content detrimental to your case. Destroying data as soon as it is no longer needed will reduce storage, maintenance and legal expenses, and minimize future costs associated with discovery and review.

Companies often have official data retention policies, but they are not enforced or followed. Plan ahead in close collaboration with the IT department and be ready to quickly implement litigation holds as required. Sometimes, certain data groups will need to have multiple holds placed on them for different cases. This is often overlooked by organizations, and lifting one preservation requirement triggers deletion of the data, when it should continue to be preserved for other pending matters. Make sure all litigation hold requirements are properly tracked and managed for each case. Maintain documentation of which data is available and which is not to effectively manage discovery requirements.

**Conclusion**

Electronic discovery has undoubtedly been a hot topic in litigation and has, historically, been a reactive measure. The process typically commences after the onset of a preservation obligation. However, given the changing landscape of regulations and laws, taking a proactive approach to litigation readiness can minimize significant risks and costs. It is important to establish a litigation response program and perform periodic reviews to modify your programs according to changing business, technology and legal requirements. If you reassess your current litigation readiness now, you can avoid having your data dictate your case strategy.

**Footnotes**

1According to Royal Pingdom, a web–monitoring service.
2Based upon the study, "Extracting Value from Chaos," conducted by IDC Digital Universe Study and sponsored by EMC Corp. 1.8 zettabytes of data are expected to created and replicated in 2011.

**Source URL:** https://www.alvarezandmarsal.com/insights/ediscovery-path-litigation-readiness

## Links

[1] https://www.alvarezandmarsal.com/insights/ediscovery-path-litigation-readiness

## Authors:

Steven Lee, slee@alvarezandmarsal.com, +1 212 328 8716