

Preparing For E-Discovery 101

Article By:

Mark Ludolph

It's 3:58 p.m. on a Friday. You have just been served with a Summons and Complaint in which your biggest customer is suing you for breach of contract. And the Complaint discusses all kinds of electronic documents – emails, texts, your website – what do you do?

You've been sued, so your first call should probably be to an attorney. But because laptops, smartphones, social media, and 24/7 connectivity have dramatically changed the nature of litigation, you are going to need proven e-Discovery expertise to get you through this.

E-Discovery is the process by which relevant electronic documents are preserved, collected and exchanged during litigation. This may include pdfs of key files, but also Microsoft Word documents, Excel spreadsheets, PowerPoint slides, emails, instant messages, website captures, photographs, audio or video files, phone records, and social media posts. However, the complexity of e-Discovery lies in the fact that electronic documents possess “metadata” – hidden information not visible on the face of a document. And, without the right skills and experience, it is very easy to alter or write-over a document's metadata, potentially destroying valuable evidence in your case. Examples of highly probative metadata include authorship, date created, date modified, and even GPS coordinates.

If this all sounds too high-tech for your business consider this: the requirement to produce electronically stored information (“ESI”) was codified at the federal level in 2006¹ and in Illinois in 2014.² Currently, there are over 3,000 case opinions involving ESI and ESI-related issues nationwide. In terms of facing the need to produce electronic information in your next lawsuit...the future is now!

So what can you do to prepare for your first (or fourth, or fortieth) lawsuit involving ESI?

Draft your Data-Map

To best prepare for modern litigation, every organization should create a Data-Map. Simply put, a Data-Map lists all sources of potentially relevant ESI held by your organization. Think: email server, laptops, phones, hard copy storage, surveillance camera systems, the company's Facebook account, cloud storage, etc. Your Data-Map should include version information, who has access to each ESI source, and a point person who manages each source – even if you outsource such management. The Data-Map should be written, dated and it should be reviewed and updated regularly.

Understand and Review your Retention Schedules

A necessary companion to the Data-Map is your Retention Schedule (also known as Retention Guidelines or File Destruction Policies). Retention Schedules outline how long all data/documents will be kept by an organization, vary widely by industry, and may even vary by source (e.g., hard copy files will be kept for five years, but surveillance camera footage will be kept for one year). While the drafting of the best schedule for your organization is a topic for another day, please note that the advent of e-Discovery does NOT necessitate that ALL documents be kept for ALL time. Industry regulations, tax laws and business necessity are key considerations.

Implement a Litigation Hold Procedure

Which brings us to the topic of Litigation Holds. While Retention Schedules dictate the regular and normal schedule by which an organization's documents will be destroyed, a Litigation Hold suspends the Retention Schedule. More specifically, the Litigation Hold outlines the litigation at issue, identifies the type of documents, including ESI, that are relevant to the case, and clearly states that such documents must be preserved and protected from destruction or alteration in any way. Further, Litigation Holds stay in effect until the completion of the lawsuit.

E-Discovery – What to Expect

So back to that late Friday afternoon Complaint. What legal assistance can you expect?

An experienced lawyer can help you:

1. Draft a Hold Letter outlining how to best preserve ESI relevant to your case.
2. Collect ESI in a manner that is cost-effective, evidentiarily sound, and non-disruptive.
3. Strategize about ESI you may need from plaintiff or a third party to prove your case.
4. Move for a Protective Order if the relevant ESI contains sensitive or proprietary information (customer lists, trade secrets, HIPAA materials).
5. Draft and respond to written discovery requests with a keen eye toward the ESI that is necessary to advance/defend your case.

[1] See the 2006 Amendments to the Federal Rules of Civil Procedure 16, 26, 33, 34, 37, and 45, and subsequent Amendments.

[2] See the 2014 Amendments to Illinois Supreme Court Rules 201, 214, and 218.