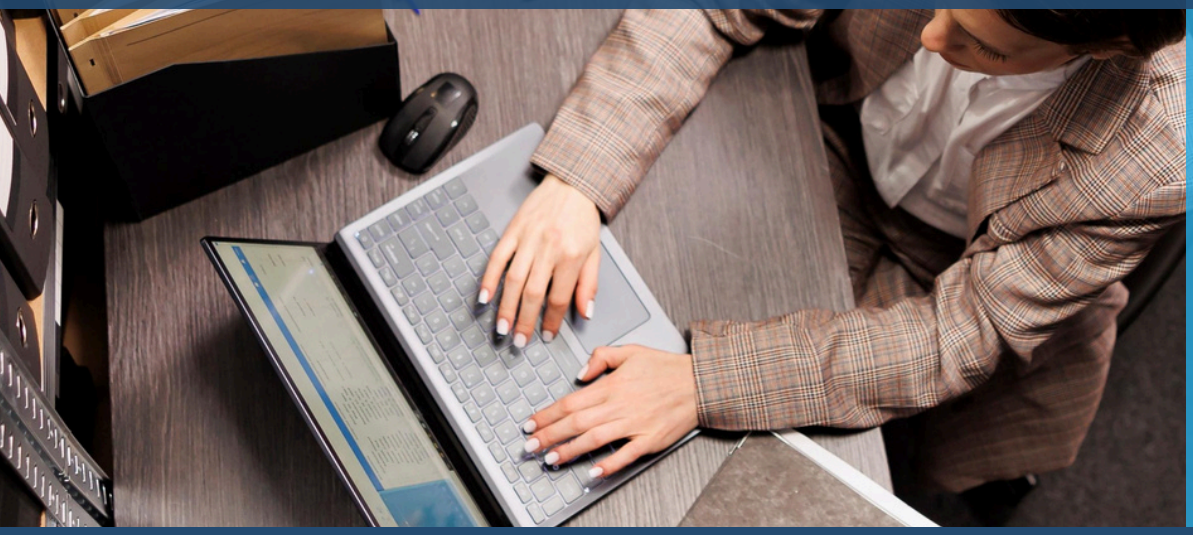
ArcherHall

The Essential Guide to E-Discovery: 10 Things Every Attorney Should Know



Overview

E-Discovery, the discovery of documents in electronic formats, is an important issue for attorneys to consider in their cases. Even though these responsibilities are often handed off to paralegals or vendors, the decisions that occur downstream after that handoff can have a variable impact on the outcome of your case. In addition to FRCP Rule 26, every attorney should take the issues in this guide into consideration when planning e-discovery efforts.

1 Volatility

How many times have you accidentally deleted a document? How many times do you open and close files each day? Digital data is fast and changeable. When you power on a computer, hundreds of events occur in the background that enable your monitor, mouse, keyboard, internet, files, and other attached items to work together. This alone can potentially overwrite log files or temporary data. User files are subject to loss from user deletion, internet sync, malware/ransomware, or retention policies set to wipe after a set time period.

It's best to preserve before litigation or immediately upon receiving a production request. Preservation is often easy to perform...if you start early. Many businesses use cloud email and storage solutions with built-in tools for enforcing litigation holds. In the case of Google Vault and Office 365, this can be as easy as clicking a few buttons. For powered-off items, like older computers and phones, you can take custody of these and leave them in a secured location where there is no risk of accidental disposal or use.

All discovery deals with volatile data—paper documents can be shredded or damaged by poor storage—but digital data has many more moving pieces that introduce risk.

2

Volume

USB flash drives, phones, and laptops are deceptively small, potentially containing MILLIONS of files. As you can imagine, reviewing millions of files would take a long time. Thankfully, you can cull this data down during the review process—but volume should factor into your review, storage, and timing decisions. More data takes more time to process and migrate; more data is also more expensive to store on a review platform. If you don't know the difference between gigabytes and terabytes, an e-discovery expert can help you translate those numbers into effective time to prepare for production.

3

Format

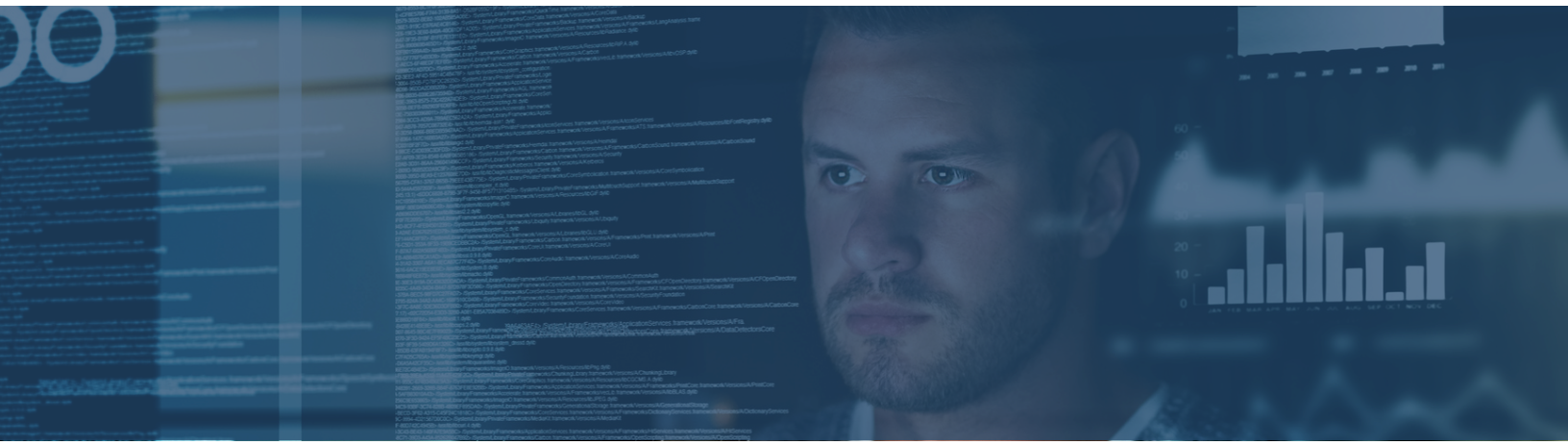
The data format may change your discovery strategy. It's important to understand which data is relevant and what data needs TLC (Time for a Little Conversion) which will be crucial to reducing discovery costs and preventing hurdles. For instance, if you are dealing with a case where the theft of source code is at issue, you may be interested in the analysis of code repositories. These files will not be viewable on a review platform and will require the assistance of an expert to interpret. If CAD diagrams or maps are in question, these will need to be converted to PDF or TIFF to view outside of a dedicated software program.

While we're talking about PDFs or TIFFs, here's a piece of advice: always ask for the format you want when asking another side to produce for you. Unless a file is originally stored in TIFF format, you might look to PDFs as your document image format of choice. PDFs are often searchable or can be made searchable more easily than TIFFs. However, if you have an e-discovery vendor assisting with your production, receiving data in native file format is even better—native files are usually smaller than either. Imaging can be handled more transparently if your side is the one performing it.

4

Metadata

Metadata is data about data. Your discovery should account for whether this is important to preserve and review. We always recommend requesting it in case it is needed later. Metadata, like timestamps, can help you narrow review efforts to relevant time periods to avoid working through decades of non-relevant items. Metadata can indicate whether data was edited after its creation. You may be able to determine whether other copies of a document exist, such as in CC email field metadata or last printed dates on Microsoft Word documents.



5

Location

Location can include a physical address, a secured or non-secured room, a particular computer, or a particular custodian, an owner of data. This will affect the processes you need to use to obtain it. The data you need may be in your client's email account, in an out-of-state branch office of a business, or at the house of an opposing party. These three scenarios all present technical and legal challenges to be considered during discovery.

We are commonly seeing more data located in "the cloud". This term simply means that data is located on someone else's server, as opposed to one physically in the possession of a data custodian. Examples of cloud data include files stored on Dropbox or posts on social media. This data must be accessed over the internet, although in some cases a cloud storage provider can mail you a physical copy of targeted data.

6

Compliance

When you collect files for e-discovery, you may be subject to handling those items in accordance with legal or best practice protocols. You may need to redact sensitive information or encrypt storage devices used to transport productions. In the case of law firms reviewing documents that include PHI (protected health information), they will need to adhere to HIPAA (Health Insurance Portability and Accountability Act) requirements. This will affect their ability to use certain vendors or e-discovery review platforms. Failure to properly handle data according to rules around compliance could cause a law firm to incur fines or legal action.

7

Authentication

As you navigate the complexities of e-discovery, the importance of authenticating electronic documents cannot be overstated. You'll need to employ stringent methods to confirm the integrity and origin of digital evidence, protecting it from tampering, hacking, or unauthorized access. Techniques such as digital signatures, metadata analysis, and maintaining a clear chain of custody are crucial. By mastering these authentication practices, you enhance the credibility of the evidence you present in court, solidifying the foundation of your case. Understanding and applying these methods is vital in safeguarding the integrity of your legal proceedings.

8

Search Terms

Searching for keywords may seem like an easy task, but that's not entirely true. Keywords must be created based on the details of the dispute. Without enough information, you could miss out on shorthand, aliases, or common misspellings of words. When it's time to look for these search terms, you may need to use specific e-discovery tools to account for variations in text extraction or encoding. Special keywords like email addresses may need to be run not just against e-discovery content but against the metadata of documents. You may also need to translate keywords when more than one language is used by one or more parties in the case.

9

Cost

It's important to get an estimate of the cost to preserve and review data before starting any e-discovery efforts. You can work with an e-discovery expert or vendor to discuss the issues in your case and where you need to focus on any future budget. You may find that even though you want to identify all relevant data, it makes more sense to preserve all data and then review only a small, relevant subset of communications. You should also consider cost during meet and confers or upon receipt of a production request. Get an expert's second opinion on how much full discovery, preservation through production, would cost so you can evaluate whether it is proportional to the dispute.

10

Visualization

If you have a large number of relevant documents that need to tell a story, you should consider how visualizations can help you in your case. Visualizations, such as graphs, videos, or side-by-side document comparisons, can be used both as evidence and as a tool during discovery to guide your strategy. For example, a graph showing what computers or phones contain the most hits on a search term—and what party uses that device—could allow you to determine the primary player in a workplace event. It could also be used to justify whether the production of a particular keyword is overbroad.