



Electronic Discovery

Everything you ever wanted to know, but were afraid to ask.

Electronic discovery (sometimes referred to as e-discovery) is not only a *product*, but also a *process*. Electronic discovery – the product – consists of computer-generated data such as email, spreadsheets, documents, and computer back-up tapes that have evidentiary value and, as a result, are considered to be discoverable. The benefit of receiving discovery in its native, electronic format is that you have access to valuable metadata. Metadata consists of embedded file properties that reveal, among other information, when a document was created, who created it, when it was modified, and where it was stored. This metadata is hidden in a paper production and lost in the imaging/OCR process.

Electronic Discovery – The Process

Obtaining useful electronic discovery involves the following steps:

- **Locating and identifying the data.** The type of data you will be looking for will either be active data or data requiring some form of forensic analysis such as replicant data, residual data, or taped backup data. This data can reside on office desktop computers or workstations, staff computers, notebook computers, PDAs (personal digital assistants) or “palm pilots,” home computers, network servers, back-up systems, taped archives, and removable (zip) drives. If you have a standard request for production of documents that you are using, be sure to update your designation of documents to include this information.
- **Preserving the data.** Electronic evidence must be collected carefully to ensure its authenticity and chain of custody for admissibility and to avoid spoliation. A reputable electronic evidence service provider can assist you in taking the necessary steps to ensure proper chain of custody including such measures as drive-imaging technology, properly restoring data from backups and archives, and utilizing industry-standard security and preservation methods.
- **Processing or “harvesting” the data.** The metadata is then processed or harvested to extract the relevant data and

convert it to a useable format. For example, the metadata is filtered to identify and eliminate duplicate documents (also known as de-duplication) or program files.

- **Analyzing and presenting the data.** Finally, once the data has been culled down to the information that is relevant, it can be converted to uniform viewable and searchable text that can be included in any of the main document management databases.

Common Terms

The following are some terms you may hear when dealing with electronic discovery:

- **Active data.** Active data has either not been deleted or may be retrievable through the “Recycle Bin” on the Windows program.
- **De-Duplicate.** The process of eliminating duplicate documents.
- **Forensic analysis.** Retrieving supposedly deleted files and other information from computers or other electronic storage media.
- **Gigabyte.** 1,000 megabytes.
- **Megabyte.** 1,000,000 bytes.
- **Metadata.** “The data about the data.”
- **PST file** – Outlook can store items (copied or moved) in a PST (Personal Store) file. The items can be an Appointment, Contact, Journal, Mail, Note, or Task item, as well as any file type.
- **Replicant data.** Replicant or cloned data files are created through the automatic backup feature on most programs.
- **Residual data.** Residual data may be sitting in forgotten clusters on a system or left in the buffer memory of printers and scanners.
- **Terabyte.** 1,000 gigabytes.

What to Look For When Evaluating an Electronic Discovery Provider

Here are some things to consider when selecting an electronic discovery service provider:

- **Experience.** What kind of experience does your provider have? How long have they been in business?
- **Client References.** Can they provide you with one or two clients to contact with regard to their satisfaction with the product and the service provider?
- **Legal Background.** To avoid any claims of spoliation or mishandling of data, it is extremely important that the provider you select have someone on board who has a legal background, specifically, an attorney who understands the rules of evidence.
- **Your expectations.** Make sure you clearly articulate your expectations to the provider. If they know what it is you are expecting to get at the end, it will go a long way towards preventing any disappointment or frustration you may have with the end product or the process itself.
- **Security.** All electronic discovery companies should have safeguards in place to protect against large-scale problems such as user verification procedures, redundant systems, off-site backup equipment, data encryption, and firewall security.
- **Ease of Use.** Look for a company that offers a user-friendly, Web-based interface that allows for searching, numbering and organizing documents. These tools should be accessible from a central screen and should allow for complex searches.
- **Billing Policies.** Ask your provider for a breakdown of all costs so you will not be surprised. For example, electronic processing versus any manual time spent working through the data.
- **Service and Support.** Look for a company that not only understands how the technology works, but how it fits into the discovery process. Inquire as to how problems are handled and as to how the company charges for its services.

Questions to Ask Your Electronic Discover Provider

Here are some questions to ask your provider about their electronic discovery process:

File extraction and identification.

- What information was extracted?
- Were program files extracted?
- How are files identified?
- How can you be sure all file types have been extracted?
- How are files that cannot be identified handled?
- Were any proprietary files extracted as well as the program used to create them?

Electronic File Conversion.

- What format is used for file conversion, TIFF, PDF, or something else?
- Will the file format be compatible with any of the main litigation support databases, such as Summation, DBText, and Concordance?
- Do you rely on all automation to convert e-discovery or is there human intervention involved to catch what the software does not process?

Email. How are email chains and email attachments handled?

De-duplication. What procedures are employed to identify duplicate documents and how can a client be assured that the documents identified as duplicates are truly duplicates?

Display of metadata. What type of metadata is provided with each image or file?

Searching and reporting capabilities. Be sure to ask about the methods of searching your data and the type of reports than can be generated from the data files.

Pricing. Typically pricing is based on processing of a gigabyte; since the data is electronic, pricing is not based on per document or per page basis.

Turn-Around Time. Ask up front about the time it will take to complete your project.

Litigation Information Management *Your support professionals.*

Please call us for more information
about our coding, imaging, repository,
and consulting services.

