



Implementing an Effective Electronic Discovery Response Plan

Introduction

A successful electronic discovery response plan is built on the same foundation as traditional discovery response. From an analysis of the document request through gathering and processing electronic data, to attorney review, and eventual production to a requesting party, the process for responding to electronic discovery is much the same as traditional discovery. The key differentiator—and the aspect of electronic discovery that causes attorneys the most anxiety—is the fact that some technical expertise is required to manage electronic discovery efficiently and effectively.

With the establishment of a collaborative relationship on both legal and technical fronts—between in-house attorneys and outside counsel, and between the company's IT department and their electronic discovery service provider—corporations and their outside counsel can map out a straightforward plan for electronic discovery response.

Step 1: Analyze the Scope of Electronic Discovery

The first step in analyzing the scope of electronic discovery or a particular electronic document request is to answer two “Who?” questions: 1) Who are the document custodians or likely key witnesses? and 2) Who is knowledgeable about how and where their electronic documents are created and stored? The answers to these “who” questions will help you formulate your overall electronic discovery strategy. In the same way you identified key players and likely witnesses early in traditional discovery, so must you pinpoint specific electronic document custodians or specific computer users in electronic discovery. You should work closely with your client to prepare an outline—even a partial organizational chart—of all people who may have created, received, or shared potentially relevant information on their computers.

The need for early analysis stems from two key legal obligations: the duty to investigate and disclose potentially responsive electronic information, and the duty to affirmatively preserve electronic information that may be subject to production in the case.

Duty to Investigate and Disclose

At the commencement of litigation, even before receiving any formal discovery request, a party must conduct an appropriate analysis to disclose to opposing parties information including a description by category and location of electronically stored information. FRCP 26(a)(1)(B); *Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 U.S. Dist. Lexis 32211, p. 16-17 (S.D.N.Y. 2006) (Duty to communicate with clients to ensure “all sources of relevant information are discovered.” Duty arises prior to formal discovery and is likely triggered by demand letter, complaint or answer).

Multiple copies of responsive electronic information may be stored on hard drives, networks, backup tapes, laptops, floppy disks, employees' home computers, and wireless email devices or PDAs. The question facing both in-house and outside counsel is this: How far does the duty to uncover information extend?

The court in *Phoenix Four* examined the duty to investigate the existence of relevant electronic information. In response to plaintiff's request for documents, defendants advised their counsel that there were no computers to search for responsive information. Therefore, defendants' lawyers reviewed and produced hard copy materials and subsequently produced those documents. Nearly one year later, a freelance computer technician hired by one of the defendants found 25 gigabytes of data—as much as 25 boxes—stored in a dormant, partitioned section of defendants' server. The court chastised counsel for failing to do more than a cursory search for sources of information:

It appears [defendants' counsel] never undertook the more methodical survey of the [defendants'] sources of information ... [Counsel's] obligation under *Zubulake V* extends to an inquiry as to whether information was stored on that server ... I emphasize that the duty in such cases is not to retrieve information from a difficult-to-access source, such as the server here, but rather to ascertain whether any information is stored there.

Id. at 18-19 (citing *Zubulake v UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (“*Zubulake V*”). The court awarded monetary sanctions against defendants and defendants' counsel for costs, including attorneys' fees associated with bringing the motion, converting recently discovered documents into a searchable format, and for re-deposing certain witnesses. The key message in the *Phoenix Four* case was that courts expect counsel to take affirmative steps to ascertain whether their clients have relevant information. It is not good enough to accept a client's blanket assertion that no such information exists.

In another case, the court reasoned that Rule 26 requires a party to disclose not just the existence of computer-based information, but also the fact that such information exists in electronic form. *In re Bristol-Myers Squibb Securities Litig.*, 205 F.R.D. 437 (D.N.J. 2002). In issuing the discovery ruling, the court emphasized that counsel would be wise to avoid unnecessary expense and disputes by using the Rule 26 conference to discuss issues associated with electronic discovery.

As the eve of electronic case filing (ECF) is upon us, in this and most other Districts, the production of electronic information should be at the forefront of any discussion of issues involving discovery and trial, including the fair and economical allocation of costs.

Id. at 444.

In addition to preparing initial mandatory disclosures and planning for subsequent responses to specific discovery requests, inside and outside counsel must work together to anticipate and plan for a Rule 30(b)(6) deposition of a designated IT person. Such depositions are now commonly utilized to seek substantive information about corporate IT systems and document management protocols and to shape further discovery. FRCP 30(b)(6); see, e.g., *Turner v. Resort Condos, Int'l.*, 2006 U.S. Dist. LEXIS 58561 (S.D. Ind.); *Alexander v. FBI*, 188 F.R.D. 111 (D.D.C. 1998)(court permitted deposition to learn about email systems and system for acquisition, location, and disposition of computers to guide substantive discovery).

Duty to Preserve Electronic Data for Production

In analyzing the scope of electronic discovery in a particular case, you must also consider how this impacts the duty to preserve evidence. Preservation duties arise or increase when your client reasonably anticipates litigation; receives pre-litigation correspondence; or receives service of a complaint, answer, or discovery request. Electronic information is subject to these standard preservation duties. See, e.g., *Wiginton v. CB Richard Ellis*, 2003 U.S. Dist. LEXIS 19128, *12-13 (N.D. Ill.). The extent of the measures your client must take to meet the obligations depends on several factors, including: the jurisdiction in which the case is filed; the facts of the case (e.g., whether relevant evidence is centered on a particular period in the past); and the specificity of document requests. See, e.g., *Wiginton, supra* (failing to halt routine document retention and destruction policy may constitute bad faith).

In one of the most extreme cases published to date, a default judgment was granted against a defendant when the court found a pattern of “stonewalling” along with discovery abuses that included lack of preservation and defendant improperly certifying to the court that it had produced everything. *Coleman (Parent) Holdings v. Morgan Stanley*, 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005). The trial ended in a \$1.4 billion verdict for Coleman. The appellate court which did not consider the defendant’s discovery abuses reversed and remanded the case for entry of judgement in favor of Morgan Stanley. *Morgan Stanley v. Coleman (Parent) Holdings*, 2007 Fla. App. LEXIS 4167 (Fla. Ct. App., March 21, 2007).

Requests for orders requiring preservation of computer information are on the rise. At least one court has allowed injunctive relief requiring “freezing” of a party’s computer systems, even before a discovery request was issued. *Dodge, Warren & Peters Ins. Svcs., Inc. v. Riley*, 105 Cal. App. 4th 1414 (2003). Other courts have noted the increased frequency of use of affirmative orders to preserve electronic data in complex litigation. See, e.g., *Pueblo of Laguna v. United States*, 2004 U.S. Claims LEXIS 49, *5 (Fed. Cir.). In contrast, some courts have rejected the need for such relief in the absence of any showing that the company or its attorneys are likely to “flaunt their obligation under the federal rules” in the absence of an affirmative order. *Madden v. Wyeth*, 2003 U.S. Dist. LEXIS 6427, *3 (N.D. Tex.).

The extent of a party’s duty to locate, preserve, and produce electronic information is now commonly the subject of a great deal of discussion between in-house and outside counsel. As with many other discovery matters, the jurisdiction in which the case is filed can have a significant impact on how the duty must be carried out. Decisions such as *Phoenix Four*, and the now famous *Zubulake* line of cases provide some guidance for how inside and outside counsel ought to work together to analyze an electronic discovery request. See *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 18771 (S.D.N.Y.) and its progeny. Ultimately, these situations are highly fact-specific and the circumstances of each case will dictate the appropriate course of action. Most important is the ability to demonstrate to the court a reasonable, legally defensible plan for managing electronic discovery that has been coordinated between in-house and outside counsel and the necessary technical personnel.

Step 2: Gather Potentially Responsive Data

Once you have assessed the scope of electronic discovery and conducted a thorough analysis of the request for electronic data, the legal and technical teams must work together to prepare a plan for efficient data gathering. Finding information in response to electronic document requests can initially appear to be an enormous undertaking, and a disorganized or untimely response can have disastrous consequences. However, with preparation and the right mix of legal and technical expertise, the process can be easier and more efficient than procedures used in the “paper world.”

Identifying the custodians of responsive electronic information in answer to the “Who” questions in Step 1 above will aid the technical team in mapping out the physical location of potentially responsive electronic documents. Next, you must think about what kinds of electronic documents were created by the key players, as not all computer users create information in the same way. Company executives and members of upper management typically use standard office software, including email and word processing programs, or presentation software such as Microsoft® PowerPoint®. Employees in finance and accounting departments tend to create large numbers of spreadsheets and other numbers-based data, and may use database systems.

Engineers or computer programmers often use computer-aided drawing programs or other specialized technical software. The best way to gather electronic data can depend greatly on the identity of document custodians and the kind of data at issue.

As you prepare your data-gathering plan, you also need to think about where the electronic data resides. Where is backup data stored? Where are documents saved on the network? Where are email messages kept? What are the options for local storage on hard drives and removable media? Gathering this information early is necessary to guide an effective discovery process; failure to develop a reasonable data-gathering plan may subject your client to later expense and delay. *See, e.g., In re Livent, Inc. Noteholders Sec. Litig.*, 2002 U.S. Dist. LEXIS 26446 (S.D.N.Y.) (defendant ordered to provide written explanation of all steps taken to locate responsive email messages).

The following list is an example of additional specific questions that should be addressed and discussed among the legal and technical teams before data gathering begins:

- Who are the custodians of interest?
 - Based on specific document requests?
 - Based on involvement in specific activities?
 - Based on geography?
 - Based on department or job function?
 - Based on dates of employment?
- What are the dates of interest?
- Must deleted files be recovered and produced?
- Are backup tapes within the scope of the request?
 - If so, what is the time period for which tapes must be restored?
 - If so, are monthly, quarterly, or yearly snapshots acceptable?
- In what form must the data be produced (and how does that impact data collection)?
- Can current in-house IT staff handle the workload, or does it make sense to contract data-gathering consultants to help?

With answers to the questions above, and guidance from in-house and outside counsel, the technical teams can then carry out the data-gathering work. In many cases, the client's IT department can handle the heavy lifting involved in onsite data collection. An electronic discovery service provider can be of great assistance in many cases, providing an approved protocol for protecting the authenticity of evidence (e.g., ensuring that original document creation dates are not accidentally overwritten or erased) and preserving the chain of custody.

Step 3: Process Electronic Data for Attorney Review

The greatest challenge of electronic discovery in most cases is the volume of electronic data that must be considered for potential production. While many attorneys assume that this volume necessarily translates to increased costs, there are many opportunities to save on expenses in the data processing stage.

Once the data gathering in Step 2 is complete, the legal team turns the documents over to the technical team to prepare the data for attorney review. When gathered, electronic data is commonly copied to media such as CD-ROMs, tapes, or removable hard drives. Care must be taken, however, to preserve metadata in the copying process. The data can then be quickly transferred from the client site for processing. Electronic data processing typically occurs at a service provider's facility where technical personnel have the expertise to rapidly and accurately process many different kinds of file types.

In paper discovery, documents are “processed” by making working copies, stamping Bates numbers, storing boxes of documents in a central repository and, in some cases, scanning and coding the documents so images of the paper can be stored in a database. Electronic discovery enables electronic documents to be processed to achieve the same results—organization and identification of the documents in preparation for attorney review. The difference lies in the automation of technology that enables uploading of electronic documents directly from their original electronic format. With all documents electronically uploaded and rendered to a common file format (most commonly TIFF or PDF), unique identification numbers can be seamlessly assigned and documents can be automatically sorted by custodian, creation date, file type, or other identifiable characteristics. With electronic processing, the full text of all documents can also be saved, stored, and made available for searching—no OCR'ing or coding of key information is required. The “parent-child” relationships between email messages and their attachments are also preserved during processing, providing the review team with an accurate picture of not only the text on the face of particular documents, but also the context of how electronic documents are related to one another.

There are opportunities for significant cost savings during the data processing stage. Duplicate documents can be eliminated, avoiding the need for repetitive review. Keyword searches and other “culling” mechanisms can also be employed at this stage to reduce the original set of documents to a more manageable size.

Despite the increased volume of electronic documents versus their paper counterparts, comparisons have shown that electronic document processing is far cheaper than paper processing.

Step 4: Review Electronic Data for Privilege and Responsiveness

Once electronic data has been gathered and processed, the technical team turns the process back to the legal team to access the documents for review. Web-based repositories for electronic documents are now commonly utilized to provide the review team with access to the entire document collection from any computer with an Internet connection. Full-text searching enables attorneys to find critical documents quickly. The ability to redact privileged information or apply annotations to critical documents, all from one shared interface, also makes the review team more productive.

In order to get the most out of electronic review, it is important to establish a review protocol early in the case. Defining parameters for privilege assessment, allocating particular custodians to individual members of the review team, and establishing a pre-approved set of search words or terms can all contribute to efficient, effective document review.

Managing documents electronically also enables the team to track the process electronically. Using mouse clicks to move documents from one collection to another eliminates the physical labor associated with managing document review, and removes the cost of bringing teams of people to one physical site for review.

Keyword searches and electronic reports enable the case manager to perform high-level quality control measures, ensuring no documents are overlooked or inadvertently produced.

In-house counsel can also be empowered by Web-based electronic review with the ability to check on the status of a case, quickly view documents that have been designated as “hot” or “privileged,” and to more effectively collaborate with outside counsel on strategy decisions without the need to ship documents back and forth between locations.

Step 5: Produce Responsive Data in an Efficient, Cost-Effective Manner

Once document review is complete, the legal and technical teams must come together again to carry out production of responsive documents. As a practical matter, electronic documents can be produced in numerous formats—printed to paper, sent electronically via an FTP site, or copied to media such as CD-ROMs, tapes, or removable hard drives. In designing the production part of an electronic discovery response plan, however, careful attention must be paid to the legal requirements of various jurisdictions.

Under Rule 34, a responding party is generally required to produce information in only one format. However, a court may order a party to produce hard copies of electronically stored information or make hard copies available to a requesting party. The appropriate form of production in a given case is another fact-specific matter that must be discussed early in litigation.

Coordinating an Electronic Discovery Response Plan Between Legal and Technical Teams

Electronic discovery best practices are based on a union of legal and technical expertise. Outside counsel can assist the corporate client in all five steps outlined above by providing ongoing advice about the law of electronic discovery and what to expect in the process. Experience with prior cases and an established working relationship with a skilled electronic discovery service provider will streamline the process and enable you to respond quickly and effectively when litigation is pending or imminent. In-house counsel can have a significant impact on the success of electronic discovery by acting as a conduit for early and effective communications with others in the corporation. Both outside and in-house counsel will benefit from a good working relationship with the technical teams.

The following tips provide an overview of how inside and outside legal and technical teams should work together to prepare an effective electronic discovery response plan.

Inside and Outside Legal Teams

- Work together to assess the company’s document retention policy, if one exists. Ensure that the policy addresses electronic information, and that IT staff understands the purpose of the policy and the legal importance of compliance. If no policy is in place, be sure the company’s senior management team understands the pros and cons of this decision as related to litigation issues.
- Assist the company in making litigation preparedness a part of employees’ daily work. Increase company-wide awareness of the types of information that must be disclosed in litigation. Educate all employees about the pitfalls of carelessly destroying or retaining information. Most employees operate with their employer’s best interests in mind, and

they will respond well to the notion that the company has entrusted them with aiding in carrying out its legal obligations.

- Outside counsel can assist in facilitating an ongoing working relationship between in-house legal and IT personnel. Too often, this relationship is formed only when a litigation crisis is looming. IT staff can provide the facts about how the company creates and stores data. Outside counsel can provide guidance to IT personnel about good practices for electronic document retention and destruction. Make IT employees aware of the most common electronic data problems: retaining unnecessary information for too long, or failing to retain information that the company has an obligation to keep. Striking the right balance here is critical to avoiding problems in court.
- Outside the context of any particular litigation, inside and outside counsel should discuss the scope of the obligation to preserve electronic data. With a map of the company's IT systems in hand, the legal team should prepare an action plan for immediately halting document destruction if the need arises. The legal team should also outline the extent of efforts that may be required to identify and search different systems and storage media for the data of "key players" in a case.
- Work together to designate and train an IT representative to act as the company's 30(b)(6) deposition witness when electronic data storage is at issue. Having a witness trained in advance will greatly reduce the company's anxiety level and will ensure there are no surprises at the deposition.

Inside and Outside Technical Teams

- Internal technical staff should organize data storage in a way that simplifies later identification, retrieval, and production of responsive information. IT personnel should talk with the legal teams and the electronic discovery service provider about the practical implications of choosing particular software, as well as the implications of changing systems. Together, the technical teams should consider capabilities that may be relevant to a discovery response: How is data stored? In what format is it stored? Is it accessible or inaccessible? Does the company want to have ready access to information from systems no longer in use?
- The company's IT department should have a specific plan outlined for the immediate suspension of usual document destruction and backup tape recycling protocols if the legal teams determine a case requires this action. An experienced electronic discovery service provider can offer suggestions for how best to accomplish this task when the need arises.
- The technical teams should maintain a focus on minimizing disruption of business operations when electronic data must be collected. A primary goal should be reducing the time individual employees must divert to examining their files for responsive information. Knowing how to leverage technology to protect employees' time and produce timely, accurate responses can save a great deal of expense. A plan for prompt and complete discovery responses will also prevent the imposition of intrusive measures, such as on-site inspections by an adversary.

- IT personnel should educate themselves about how best to carry out the data collection process. In some cases, the company's IT department will have sufficient expertise to handle this task internally. In other cases, outside assistance may be required. A predetermined protocol for collecting and copying electronic data will ensure that the chain of custody is preserved and that data is not unintentionally altered.
- The internal IT staff can provide valuable information when an electronic discovery service provider is asked to reduce the original volume of electronic data collected before the attorneys begin review. Many courts allow service providers to assist with keyword searches or other methods of pre-review data reduction. The company's IT personnel will be in the best position to provide information about how the files of various document custodians are organized. If the company's IT staff is available to provide some tactical guidance, the service provider will spend less time and money on administrative work, and can focus on substantive electronic discovery services.

Conclusion

The prevalence of electronic discovery means that all businesses must have ready access to the evidence they need to produce, while guarding against accumulating overwhelming volumes of information. Effective planning requires a new working relationship among internal and external legal and technical resources. With an effective electronic discovery action plan in place, in-house attorneys can gain control over data retrieval and review processes and costs, while outside counsel enjoy a tremendous advantage in preparing their clients' cases.

The Discovery Experts: Industry Relations

LexisNexis Discovery Services has the right consulting and technology choice for every discovery need. Top law firms, corporations and government agencies rely on the LexisNexis® products and services, Applied Discovery®, Concordance™, and Hosted FYI™, to meet their discovery obligations on time, accurately and cost-effectively. Services include records management consulting, data collection, forensics, media restoration, data filtering, data processing, review and document production in the format that each matter requires. The Industry Relations team works to educate the legal community on the continually evolving case law and technology of electronic discovery.

For more information or to contact the experts, please visit lexisnexis.com/discovery.

