Electronic Discovery Action Plan

The best electronic discovery response plan requires work well in advance of litigation. Corporate clients need to preserve necessary documents and ensure ready access to them, while avoiding accumulation of information that need not be retained for legal or business purposes. Litigation counsel needs to identify, gather, review, and produce responsive information when a document request is issued. In the process, all involved want to avoid claims of spoliation and minimize business interruptions.

Today's litigators face an uphill battle should they fail to assist clients in implementing a comprehensive electronic discovery action plan prior to litigation. On the other hand, they can offer great value to clients by raising these issues outside the context of a particular lawsuit, enabling the client to put its best foot forward in any electronic discovery scenario.

An electronic discovery action plan should be reviewed on a case-by-case basis and tailored for individual clients' needs, but the following general guidelines can be applied in nearly any situation.

Preventative Maintenance

- **Educate your client about electronic discovery.**
  - Conduct an electronic discovery training session for in-house counsel and senior managers. Invite your electronic discovery service provider to discuss the technical issues, while you focus on the legal obligations.
  - Provide your client with jurisdiction-specific and business-specific counseling. The obligations imposed by case law vary greatly, and a number of courts have implemented local rules for the management of electronic discovery.
- **Partner with the company's IT department.**
  - Identify IT personnel who will be involved in electronic discovery when the situation arises. Help them understand the importance of their participation in the legal process.
  - Educate key IT personnel about relevant legal issues, including document retention obligations and standards for spoliation. Do not assume that the IT department understands the company's legal obligations, or even the meaning of "discovery."
  - Inform the IT department of the need to quickly gather certain technical information when an electronic document request is issued (you should discuss: backup schedules, adherence to document retention and destruction protocols, identification of types and locations of data stored on networks and email servers, mapping of other data storage locations, etc.).
- **Assist your client with employee outreach.**
  - Educate managers about key legal issues, including document retention and spoliation. Design a plan for consistent communication from managers to employees.
  - Aid the client in establishing a company culture that encourages prudent document management, and assist the client in consistently auditing and reinforcing these practices.
  - Assist the client in training employees to use email for business purposes only. Offer examples from published opinions to demonstrate the potential hazards of careless or improper email communication.
  - Help your client's employees understand the unique characteristics of electronic documents (e.g. the ability to view meta data revealing blind carbon copies on email or to view the dates a document was created or modified).
  - Plan a legally defensible employee notification procedure to trigger an immediate halt to destruction of potentially relevant documents when litigation is pending or imminent. Review with your client case law supporting the imposition of severe spoliation sanctions, even when document destruction is merely negligent.
- **Encourage your client to create an electronic data management plan.**
  - Educate your client about the risks of failing to include electronic documents in its records management policy, and

advise its management team about the precedent for sanctions when a company fails to do so. Involve designated IT personnel and records managers in the conversation.
  - Evaluate your client's document retention and destruction practices, backup protocols, tape rotation and recycling schedules, and any other company practices related to electronic data management.
  - Encourage in-house counsel to evaluate compliance on a regular basis and to schedule audits to ensure practices comply with the plan.

- **Help your client anticipate the duty to produce electronic data.**
  - Create a cross-functional team with representatives from the law department, IT department, outside litigation counsel, and the electronic discovery service provider. An open dialogue among these parties will put your client in the best position to respond to electronic discovery requests when the need arises.
  - Encourage your client to make informed decisions about whether to store information in electronic or paper format. This can have a profound impact on costs and the ability to meet production deadlines in litigation.
  - Consider conducting a "fire drill" to test the company's ability to respond to an electronic document request.

When Litigation is Pending or Imminent

- **Prepare key employees to carry out their electronic discovery obligations.**
  - Notify the necessary IT and records management personnel both orally and in writing of document preservation obligations (e.g. halting of backup tape rotation and recycling, if necessary).
  - Advise company management both orally and in writing of the time to issue a data preservation notice to employees. Include information about the consequences of failing to carry out preservation obligations effectively.
  - Select and train an IT or records management liaison to serve as the company's 30(b)(6) witness.

- **Send a preservation letter to opposing counsel if you intend to request electronic data in discovery.**
  - Describe the kind of information you intend to pursue.
  - If the law requires preservation of the kind of information you are seeking, then state the specific statute, rule, or other legal authority supporting your request.
  - Be as specific as you can without unnecessarily limiting the kind of data requested for preservation. Courts favor tailored document requests, and the preservation letter is a good place to start.

- **If you decide to issue a preservation letter, you must expect to receive one in return.**
  - Be prepared to object in writing, if necessary. Information previously gathered about your client's computer systems will put you in a good position to respond quickly.
  - Put opposing counsel on notice of your client's plan for document preservation.
  - Begin documenting details of the costs and efforts associated with preservation, in the event you want to seek a cost-sharing or cost-shifting arrangement.

- **Consider whether the case will require specialized electronic discovery expertise.**
  - If the case will involve large volumes of electronic data or will otherwise include electronic discovery issues that may become complex, you may wish to retain an electronic discovery service provider that offers legal consulting to assist you in analyzing your client's electronic discovery obligations and the appropriate actions that must be taken. A consultant can also assist in drafting electronic discovery requests to opposing parties.
  - If collecting electronic data from your client will be a complicated undertaking (e.g. if the client has complex IT systems or geographically dispersed business operations), consider whether you will want to engage a technical expert to aid in the data collection process. This will ensure that the chain of custody is preserved and that the data is not unintentionally altered.

After Litigation is Commenced

- **Consider whether electronic discovery issues should be raised at the Rule 16(c) pretrial conference.**
  - Review Rule 16, which sets forth a number of topics that may be considered at the pretrial conference. While electronic discovery is not specifically listed, Rule 16(c)(6) calls for a discussion about the control and scheduling of discovery, including orders affecting disclosures and discovery pursuant to Rules 26 through 37.
  - Weigh the pros and cons of raising the issue of electronic discovery at this early conference if opposing counsel has not already done so. With electronic discovery becoming commonplace in nearly every case, it is unlikely that silence on the issue will present any strategic advantage, but you will benefit from considering your strategy early in the case.

- **Prepare to make Rule 26(a) initial disclosures about your client's electronic data.**
  - Advise your client about the requirements set forth in Rule 26(a)(1)(B). At the commencement of litigation, and before receiving any formal discovery request, a party must disclose to opposing parties certain information, including a description by category and location of documents and data compilations. This requirement means that a party must search available electronic systems for relevant information.
  - Beware of making a "handshake agreement" to waive or limit Rule 26 initial disclosure requirements. Some courts have stated their disapproval of such agreements, and you may later be compelled to carry out the duty to investigate in a severely reduced timeframe.

- **Plan to discuss key electronic discovery issues at the Rule 26(f) conference.**
  - Some courts have modified their local rules to require attorneys to discuss specific electronic discovery issues early in the case. Even in jurisdictions without modified rules, the mandatory Rule 26(f) conference requires parties to confer to develop a proposed discovery plan. Today, electronic discovery should be an important component of the discussion in nearly every case.
  - The conference should include discussion about the following: preservation and production of digital information; procedures for dealing with inadvertent disclosure of digital information; the necessity of restoration of deleted digital information; the scope of discovery and whether it covers backup or other historical or legacy data; the media, format and procedures for producing digital information; and the assignment of the cost of preservation, production, and restoration (if necessary) of any electronic discovery.

- **Consider whether you wish to propound electronic discovery requests to the opposing party.**
  - Schedule a 30(b)(6) deposition early to learn about the opposing party's IT systems, infrastructure, and procedures. This will guide you in identifying the locations of potentially relevant information. Topics should include hardware configurations, operating software, storage locations, backup protocols, home computer use, remote access, etc.
  - Draft tailored document requests to include production of electronic data. Courts do not favor broad requests for "any and all" email or other electronic documents. A narrow request that focuses on specific document custodians, time periods, and key issues in the case will stand up in court.
  - Consider whether you want to receive document production from the opposing party in paper or electronic format, and set this out specifically in your document request.

- **Consider whether your client will want to seek a protective order.**
  - Assess the need for advance protection for the possible inadvertent production of privileged information.
  - Consider whether a "quick peek" or "clawback" agreement will be appropriate in the case.

After Receipt of Document Request

- **Carefully analyze the document request.**
  - Outline the names of document custodians who will be involved in the production. Use the client's organizational chart as a guide to identify all potential document custodians and key witnesses.
  - Map the locations of potentially responsive information. Engage all members of the cross-functional team previously established to assist in this inventory.
  - Consider the time periods relevant to the case and ensure the document requests are not overly broad or unduly burdensome.
  - Frame your objections carefully. As courts give more credence to narrowly tailored document requests, they are also more accepting of objections that are grounded in specific facts and carefully crafted to align with the particularities of the case.
  - Review your client's document preservation efforts at this juncture to ensure they are consistent with the needs of the case.

- **Prepare to gather necessary electronic data in an efficient, legally defensible manner.**
  - Identify the custodians of interest based on: specific document requests, involvement in specific activities, geography or office location, department or job function, dates of employment, or other variables relevant to the document request.
  - Define the scope of the data-gathering project. If the amount of electronic data at issue is great, or if your client has complicated systems or lacks internal IT expertise, you should consider enlisting professional data-gathering assistance. This will ensure that data is copied correctly and not inadvertently altered during the collection process. Data-gathering experts can also assist you in tracking chain of custody and implementing other necessary precautions to avoid later claims of spoliation or challenges to the authenticity of the evidence.

- Prepare a data-gathering plan that includes: a diagram of the data to be gathered; a project plan for all physical locations; a summary of the anticipated impact on operations, and plan for minimizing business disruptions; a summary of any anticipated complications; identification of all members of the data-gathering team; identification of any outside data-gathering consultants involved in the project; identification of points of contact for each physical location; an inventory of the hardware and software tools to be used; an outline of the specific collection procedures that will be used; detailed work product checklists for technical staff completing the collection work; chain of custody instructions for all involved parties; arrangements for shipment of the media containing the data gathered.
- Consider whether backup data is within the scope of the document request. If it is, your data-gathering plan will need to consider the following: an assessment of backup schedules (e.g. the availability of weekly, monthly, or yearly snapshots); identification of tapes containing potentially relevant documents; procedures for backup tape restoration; and any effect on ongoing backup procedures

• Process the electronic data for efficient, cost-effective review.

- Once the potentially relevant data has been gathered, the electronic discovery service provider prepares the data for attorney review. When gathered, electronic data is commonly copied to media such as CD-ROMs, tapes, or removable hard drives. 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 process many different kinds of file types rapidly and accurately.
- Discuss any special circumstances in the case in advance of data processing. For example, unique or uncommon file types may require special attention, or they may not be relevant to the case at all.
- Work with your electronic discovery service provider to prepare realistic cost and time estimates to provide to your client. Establish open lines of communication and a procedure for quickly communicating updates. Because electronic discovery processing is frequently a "know as you go" undertaking, many characteristics of an electronic document population are discovered once the processing begins.
- Agree on turnaround times and discuss the possibility of a "rolling production" or other options that will aid in efficient review.

• Review the electronic documents for relevance and privilege.

- Establish a review protocol at the outset. Assign a technical lead and a legal lead, and conduct early team meetings to agree on the review methodology, checklists for identifying relevant and privileged documents, identification of key words or terms for searching, and other details of the legal team's review process.
- Include your electronic discovery service provider in early planning sessions. Your project manager should be able to suggest shortcuts and best practices for use of the online review application.

• Produce relevant documents to opposing counsel.

- Discuss options for form of production. 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, as some require production of electronic data in electronic format.
- Consider proposing options for a rolling production to opposing counsel, if the volume of data is significant and this could ease review burdens.

Discovery 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.

All information provided in this document is general in nature and is provided for educational purposes only. It should not be construed as legal or professional advice. Applied Discovery encourages you to conduct thorough research on the subject of electronic discovery.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.
Applied Discovery is a registered trademark of Applied Discovery, Inc. © 2004 Applied Discovery, Inc. All rights reserved.
Last Updated September 2004. AD00017-0 0804