

Is Your e-Discovery Provider Asking The Right Questions?

Here Are 12 Queries To Help You Decide

Part One of Two

By D. Douglas Austin

As most attorneys practicing in these days of high-tech tools and media-savvy clients know, electronic discovery can be a complex process, even for the experienced practitioner — an undertaking fraught with variables, each of which singly, and certainly in legion, could change demands and expectations. Those changes, when they occur — and it's invariably a matter of *when*, not *if* — can confound parties to the e-discovery process, particularly when important information is *missing*.

In fact, the e-discovery process has become so complex that litigators often rely heavily on their e-discovery provider to add to hands-on legal expertise and to ensure that discovery is performed with diligence, ease and effectiveness.

One keystone in this process of building a strong and winning e-discovery process is good communication between a client and service provider,

D. Douglas Austin is a technical consultant with IE Discovery Inc. of Houston. He has two decades of experience in providing information-technology and discovery-management consulting services. Reach him at daustin@iediscovery.com or 713-851 1546. Visit IE Discovery at www.iediscovery.com.

which acts as the cement that holds working relationships together. It is the first basic requirement in ensuring a partnership of discovery success.

WHAT PROVIDERS CAN DO

As is often the case, the best way to understand the importance of a component in a process, whether the process or its elements are simple or complex, is to consider the consequences of that component's absence. In the case of e-discovery, miscommunication that might occur between an e-discovery provider and client can cause problems ranging from additional expense to collect and process electronic files properly to sanctions for failing to produce all relevant materials. In a worst-case scenario, counsel and others could face criminal penalties for spoliation of evidence that a court determines was caused by avoidable delays and poor communication among parties.

With so much at stake, there's no likely way to overstate the importance of e-discovery providers seizing initiative to determine client needs by taking on the role of litigator and asking questions. Qualified e-discovery providers are the best experts to help counsel determine a winning course of action for complete and accurate electronic production that meets litigation goals. Indeed, just as a doctor knows the

questions to ask a patient to make a proper diagnosis, an e-discovery provider who is doing his or her job knows which questions to ask to ensure that the discovery process involving electronic files is handled properly.

THE COURSE OF CRITICAL INQUIRY: DO IT CORRECTLY

Questions a provider might ask can vary considerably, depending on case requirements and characteristics of the electronic collection. However, there are some typical characteristics of any e-discovery situation. The following questions cover issues to address in e-discovery, and can serve as a guide to counsel in working with e-discovery service providers. In those instances when a provider doesn't ask some of these questions, counsel can pose them — or other salient queries — to ensure discovery of common ground, and to start off together on the path to successful litigation.

1. What criteria are being used to determine which electronic documents to collect?

Whether or not the e-discovery provider is responsible for document collection, it's important for the provider to understand the collection criteria. For instance, does the scope of production include documents stored on back-up tapes or other archival

media? If so, then it will likely affect the number of files the provider must process. Also, because backups are often incremental, and so include many of the same files in each backup, deduplication of files (*ie*, removal of duplicate files) will likely be required to avoid producing numerous copies of the same file. It is important, too, that the e-discovery provider understand the collection criteria up front to reduce the need for costly repetition of work later.

And it's important for the e-discovery provider to understand whether there is a document-retention policy in place that includes electronic files. If properly enforced, such a policy can provide considerable guidance for satisfying production requests. Electronic files outside the retention-policy time frame, for instance, will generally no longer exist to be produced. Destruction of electronic files outside the retention policy generally does not constitute destruction of evidence in the eyes of the court.

But it's also important for the provider to understand whether any steps have been taken to alter document-retention procedures upon notification or knowledge of impending legal action to preserve potentially relevant information — so don't destroy electronic files that may be relevant to the legal action at hand or that will soon be at hand. Keep in mind that a major issue during the Enron investigation was the shredding of hard-copy documents, which created controversy over contentions that the shredding was being performed in accordance with retention policies. Shredding hard-copy documents to comply with retention policies could lead opposing counsel to level spoliation claims. The same applies to electronic file deletion — if it could be assumed that the producing party *should have* known these files

were potentially relevant. Failure to take steps to preserve electronic data in the face of pending legal action can expose litigators to sanctions later on.

The e-discovery provider should also be able to identify and address issues associated with document collection, and not merely with converting documents received. e-Discovery providers should know the relevant issues involved and steps to take that will help ensure appropriate documents are included in discovery. This knowledge includes understanding data-collection criteria and how those criteria pertain to preservation and production.

2. What time frames, organizations and people are to be included in production?

Regardless of whether the provider is responsible for collection, the provider's personnel must understand production scope and the filtering criteria used for processing data. Not understanding production scope could cause inadvertent production of irrelevant information, or withholding of relevant information, which could have dire consequences. Identifying the time frames involved, and individuals whose files should be included in production, will often set the extent of the collection process. For example, a requirement to include terminated employees' files in the collection process will often require collection from backup media, because those files are generally no longer available on active media.

3. Has electronic document collection begun?

The e-discovery provider should ask about e-file collection status and requirements for documenting file chain of custody. The provider must know where the information is coming from in order to preserve and manage documentation for the chain of custody from that point. Also, taking affidavits from the source individuals who provide electronic documents can support the validity of the custody chain and help avoid

spoliation claims. To help ensure a smooth process then, the e-discovery provider should have a standard policy to preserve file chain of custody, or be able to support an existing policy.

4. In which format (*ie*, native files, TIFF/PDF or paper) will files be used for production?

Providers should be able to provide guidance regarding benefits and issues associated with producing documents in each format. Some format guidance follows.

Native Files

Points to consider regarding native files include:

- How should the files be Bates labeled? Applying Bates labels to a variety of e-file formats (some of which don't easily render pages of information) is difficult. An alternative numbering method (at the file level) might be necessary.
- Native files can contain viruses, but removal of viruses can be interpreted as spoliation — so be careful; there are no standards concerning what to do about viruses.
- Removal or redaction of privileged information can be more difficult for native files, and changes the file properties, such as *modified* date, which could be interpreted as spoliation.

TIFF/PDF or Paper

Considerations for these formats are:

- How should files that don't provide useful printouts be handled? Executable files, system files and databases are examples of these.
- Spreadsheets are often not formatted for printing and can be time-consuming and costly to produce.
- Excluding hidden text or metadata — or both — when converting to image could be considered spoliation.
- Production to paper includes all of these issues, plus additional time and expense compared to delivering

images on CD.

- Sometimes, a combined approach that includes native- and image-file formats is appropriate. Converting files to image that are naturally formatted for printing (eg, e-mails, word-processing files) makes Bates labeling and redacting those files easier. Producing spreadsheets and databases in their native format can eliminate significant costs associated with converting those files, but maintain responsiveness to production requests.

5. What are the criteria that define a duplicate?

Interpretations of what a duplicate is can vary widely, depending on discovery requirements. Sometimes, duplicates are identified solely on the physical content of a file, but they also can be identified based on the file source (just like hard-copy documents).

Several different data elements can be used to determine which files are duplicates, including: industry standard file *fingerprints* (including the MD5HASH value, which is a unique number generated by an algorithm applied to file content); global unique identifier (GUID) for Microsoft Office files; or a combination of fields (eg, date received or sent — or both — and subject, author or other fields, if desired etc.).

Versatility is also important for supporting deduplication requirements. Not only should an e-discovery provider be able to support multiple alternatives for eliminating or otherwise excluding duplicate files, but the provider should also be able to provide an audit trail of the files that were eliminated during deduplication.

6. How should e-mails and attachments be handled for discovery purposes?

A litigation-support system is generally used to review documents for relevancy and privilege. Because e-mail

systems facilitate everyday business correspondence and collaboration, many of the electronic file collections requiring review are e-mail based.

e-Mails can contain one or more attachments; indeed, several e-mails can be contained in a single e-mail, each with its own attachments. Because e-mails often refer to their attachments within the body of the e-mail, opposing counsel could raise issues if the e-mail is produced without one or more of its corresponding attachments. As a result, it may be necessary to produce the e-mail and its attachments if any one of those documents is relevant.

A provider should be able to furnish appropriate guidance on supporting e-mail relevancy review, including marking an entire e-mail as relevant when any of its components is relevant. The provider should also be able to recommend a litigation-support system for relevancy review that will be able to support this function.

(For more on litigation response as an element of business process, see “The Litigation Balancing Act — Measuring Soft And Hard Costs, And Meeting Demands In the Digital Age” in the May edition of *e-Discovery Law & Strategy*, or go to ljonline.com/alm?edisc.)

7. Should relevancy review or automated filtering of documents — or both — be performed before conversion of documents to image or paper?

Yes, because native-file relevancy review can often save significant time and conversion costs. Typically, a small percentage of electronic files (especially in e-mail collections) is relevant to a case — often 20% or less. Initial review enables a litigator to eliminate costs of converting the large number of files that are not relevant. But it can be more difficult to manage review of diverse file types than to manage a converted collection of TIFF or PDF files. Also, if the

electronic file collection pertains to multiple cases with different issues, then it might be advantageous to convert most or all files to support all of the cases.

On the other hand, automated filtering by using search terms to identify relevant files can present problems. Some of the problems that can occur include:

- Search-term lists can miss abbreviations or misspellings of the terms.
- Text searches are not always complete, because TIFFs and image-only PDFs contain no searchable text and require optical character recognition (OCR) to generate searchable text. Other file formats often contain embedded graphics (such as charts with text) that are also not fully searchable. Locating these documents to perform OCR can be difficult and consume significant blocs of time.
- Search-term collections that are overly broad can result in retrieval of a large number of documents that require review, many of which turn out to be nonresponsive.

Consider this: When using search-term lists for automated filtering, a list negotiated with opposing counsel is the safest bet. Sometimes, a combination approach is best — use a narrowly defined list of terms to identify initial documents for conversion, and then manually review the rest for relevancy. The e-discovery provider should be able to address the pros and cons of each approach, recommend the best approach, and support review and automated filtering prior to conversion.

Is Your e-Discovery Provider Asking The Right Questions? *Here Are Some Queries To Help You Decide*

Part 2 of 2

By D. Douglas Austin

As is often the case, the best way to understand the importance of a component in a process, whether the process or its elements are simple or complex, is to consider the consequences of that component's absence. In the case of e-discovery, miscommunication that might occur between an e-discovery provider and client can cause problems ranging from additional expense to collect and process electronic files properly to sanctions for failing to produce all relevant materials.

In a worst-case scenario, counsel and others could face criminal penalties for spoliation of evidence that a court determines was caused by avoidable delays and poor communication among parties.

With so much at stake, there's no likely way to overstress the importance of e-discovery providers seiz-

D. Douglas Austin is a technical consultant with IE Discovery Inc. of Houston. He has two decades of experience in providing information-technology and discovery-management consulting services. Reach him at daustin@iediscovery.com or 713-851-1546. Visit IE Discovery at www.iediscovery.com.

ing initiative to determine client needs by taking on the role of litigator and asking questions. Qualified e-discovery providers are the best experts to help counsel determine a winning course of action for complete and accurate electronic production that meets litigation goals. Indeed, just as a doctor knows the questions to ask a patient to make a proper diagnosis, an e-discovery provider who is doing his or her job knows which questions to ask to ensure that the discovery process involving electronic files is handled properly.

THE COURSE OF CRITICAL INQUIRY: DO IT CORRECTLY

Questions a provider might ask can vary considerably, depending on case requirements and characteristics of the electronic collection. However, there are some typical characteristics of any e-discovery situation. The following questions cover issues to address in e-discovery, and can serve as a guide to counsel in working with e-discovery service providers. In those instances when a provider doesn't ask some of these questions, counsel can

pose them — or other salient queries — to ensure discovery of common ground, and to start off together on the path to successful litigation.

For questions 1 through 7, and more e-discovery information, go to our Web site, at www.ljnonline.com/alm?edisc.

8. What file types need to be converted?

Most providers can handle standard formats, including Microsoft Office (Word, Excel, PowerPoint), Acrobat PDF, and Outlook PST or MSG format, among others. Less popular formats (eg, PaperPort MAX images, WordStar, etc.) may be more complicated to process and often require manual effort, costing more time and money.

Providers should also be able to produce a list of standard supported formats that have been tested and approved as a standard part of conversion. It's important to know which formats are supported up front to avoid processing delays and extra costs.

9. How should hidden information be handled on files con-

verted to image or paper?

Many providers assume that electronic files should be converted as they would normally be printed, but that's not always a safe assumption. Some examples of why this isn't always a safe assumption follow:

- PowerPoint files can include hidden slides.
- Excel workbooks can include hidden columns, rows or sheets.
- Word documents can include hidden text, or tracked changes, or a combination of these features.
- Excluding this information can be interpreted as not meeting production requests or as spoliation, and not asking for this information during production could result in missing the smoking gun. The e-discovery provider must be prepared to address the issue of hidden information, and be able to support inclusion or exclusion of this information when processing files.

10. How should corrupted, encrypted or password-protected files be handled?

Repairing or decrypting files can drag out the discovery process and break budgets, and there's no guarantee that these files can be made usable. Use of error logs to identify files that could not be produced to opposing counsel because of corruption or encryption issues will at least disclose the existence of these files and why they could not be produced. The e-discovery provider should be prepared to address how these files will be handled and noted for production purposes.

11. What metadata date should be considered the docu-

ment date?

Determining the appropriate date to use within a litigation-support system is a particularly important and complicated aspect of managing metadata, especially when also using file dates to determine whether the file is included within a relevant time frame. Different dates may be appropriate to use for different file types. Examples:

- e-Mails generally use the date sent or date received.
- Calendar items generally use date scheduled or meeting date.
- General office files typically use the create date or last modification date.

It should also be noted that operating-system file dates are often not reliable. Copying a file to CD or to disk for processing can update the operating-system date. A number of applications (such as Word and Excel) now track their own internal creation and modification dates, separately from the operating-system dates. A complication in the handling of dates is that old versions of these files use the operating-system dates to identify create and last-update dates because the application-specific dates didn't exist in earlier versions of those products.

The electronic-discovery provider should be aware of these issues associated with electronic file dates, and know how to use that information to ensure that each file type is properly handled.

12. What litigation-support system will be used to review the converted files?

Format for output from the e-discovery conversion process is partially determined by the litigation-

support system used. For example, if a particular system supports page synchronization between image and text (where text can be searched, but users then must find the same image page with the reference), then it may be better to generate single-page text files so that those files can be used to insert page breaks between files. This allows tracking of pages within document text.

The e-discovery provider should be prepared to identify issues associated with management of electronic documents within the litigation-support system chosen and be able to suggest the most appropriate solution to support the goals of the production team.

CONCLUSION

While a good provider should take proper responsibility for the success of counsels' e-discovery efforts, attorneys and clients will be the ones who suffer the consequences of failure. One way to prevent this is to make sure that the selected provider is asking the right questions at the beginning of the discovery process.

Awareness of these questions also enables the litigator to negotiate terms with opposing counsel to ensure that production needs are met cost-effectively.

Addressing these questions will promote smooth, cost-effective and successful discovery.

This article is reprinted with permission from the August 2004 edition of the LJN'S E-DISCOVERY LAW & STRATEGY. © 2004 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact American Lawyer Media, Reprint Department at 800-888-8300 x6111. #055/081-07-04-0006

Who is IE Discovery?

IE Discovery is the first legal services provider offering comprehensive Discovery Management and other litigation support services to corporate law departments, outside counsel, and government agencies. Comprised of legal professionals, technologists, and document specialists, the IE Discovery staff creates solutions for a wide range of complex, information-intensive litigation.

What is Discovery Management?

Discovery Management is a sophisticated methodology for collecting and transforming disparate documents and data - both in electronic and paper forms - into a unified system that enables attorneys to quickly analyze relevant information for more effective advocacy. Encompassing the complete discovery cycle, from collection to production, IE Discovery's robust services rely on the InfoDox™ platform, a secure, Web-based system for searching, organizing, and producing discovery documents.

IE Discovery offers solutions for all areas of Discovery Management:

- Planning - Legal and technical consultants assist clients to devise a Discovery Management strategy, for ongoing litigation and future cases.
- Collection - Identification and acquisition of discovery data and documents, both electronic and paper, from multiple sources.
- Processing - Staffed with experienced document professionals, the processing service follows rigorous quality assurance guidelines.
- Review - Legal professionals, using platform tools, perform reviews for relevancy, privilege, and issue coding, as required.
- Production - The identification, organization, and output of production documents to opposing counsel.

discovery
ie discovery, inc.
800.656.8444
www.iediscovery.com

TEXAS
9101 Burnet Road
Suite 202
Austin, Texas 78758
512.833.5588 voice
512.832.0302 fax

WASHINGTON D.C.
1101 Wilson Boulevard
Suite 1450
Arlington, Virginia 22209
703.527.2700 voice
703.527.2785 fax