

Tackling e-Discovery

Obtaining & Using Electronic Evidence

Thomas J. Henderson

This article was originally published in "connect. explore. energize," NELA's 2007 Eighteenth Annual Convention Manual on CD-ROM. All rights reserved. For this and more NELA publications, please visit the NELA Bookstore on our web site at: www.nela.org or turn to page 205 for our Law Publications Order Form, and fax it to: (415) 677.9445 or mail to: National Employment Lawyers Association, 44 Montgomery Street, Suite 2080, San Francisco, CA 94104.

Two years ago, like many lawyers, I knew next to nothing about electronic discovery. Although I had discovered computerized data for analysis in some cases, I had no idea how even to think about discovering documents from word processing and other software programs, or e-mail, and didn't have much of a concept of what else might be included within the ambit of electronic discovery.

Although I did not understand e-discovery, I knew that it was an emerging issue that was receiving a great deal of attention in the bar and from the bench. And, we were preparing to file a new case. It appeared as if the time had come for me to learn how to do e-discovery. So, I learned.

As with learning anything new in the practice of law, I identified and read materials on e-discovery and consulted those with experience. There are great sources available that provide useful and helpful explanations of electronic information, its preservation and discovery. Among the most useful are those by:

Craig Ball (www.craigball.com)

Joan Feldman (www.forensics.com)

Kenneth Withers (www.kenwithers.com)

The Federal Judicial Center (www.fjc.gov)

Vendors also have useful information and on the questions of needed capacity and resources, interviewing them was helpful, if only to understand what is involved in processing electronic information and the services they offer. In developing a plan for

e-discovery and identifying and finding answers to the important questions, consulting a computer forensics expert was essential. In a relatively short time and for relatively modest fees, I obtained answers to critical questions and developed an effective strategy to obtain the electronic information we needed in an efficient and economical way.

You also learn by doing. I sent document preservation letters, discovered document retention policies, negotiated preservation and auditing protocols for electronic information, deposed IT professionals and obtained document preservation orders. I proposed and tested search terms for automated electronic searches to be used to identify electronic documents responsive to document requests, and secured production of over 450,000 pages of e-mail and other electronic documents, electronic copies of intranet policy databases, and gigabytes of electronic employee data. I also performed my own electronic searches of the product of e-discovery to identify a company's policies and practices and evidence of discrimination in the administration of those policies. My experience should encourage others to believe that they can learn electronic discovery. Thus, I share something of how and what I learned, and continue to learn, organized around a series of basic questions.

1) Is e-discovery really necessary or can I get by without it?

Electronic discovery is a competency that every litigator needs. Today, most communications and records are created and exist as electronic information, and you need to understand how to discover them to obtain the evidence required for your case. Further, the benefits of electronic discovery are many, including the type and volume of information available, the capacity to manage huge volumes of information easily and efficiently in electronic form and the ability to search thousands of documents in minutes through automated electronic word searches.

Those who have not yet learned electronic discovery cannot put it off any longer. It is doubtful that you can adequately represent your client in many matters without discovering electronically stored information (“ESI”). If nothing else, the new amendments to the Federal Rules of Civil Procedure now make it impossible to avoid the topic of electronic discovery. You will have to address the subject with your opponent and the Court in the Rule 26(f) Report and the Rule 16 Pretrial Conference. And the point of this presentation is that, with some time and effort, you can learn how to conduct e-discovery effectively.

2) When and how should I begin to address e-discovery?

Because most records and documents now are electronically produced, communicated and stored, their existence needs to be addressed from the outset of your investigation. In interviewing your client, you will have to inquire about electronic information to identify the documents and records relevant to the claims and facts. The inquiry should encompass all of the possible sources of electronic information, including not only word processing documents and e-mail, but spreadsheets, voicemail, intranets or web pages, instant messages, video and audio recordings and the nearly infinite number of ways in which we now produce ESI.

When identifying sources of information, it is

important to consider how information is captured electronically and where it may be stored. Electronic information is truly ubiquitous. For example, e-mail may exist on a personal computer as well as the server for the e-mail system. Calendars can be stored on PDAs as well as a personal computer and the system server. And electronic information relevant to your case may be maintained and produced in ways you would not expect. For example, you would expect an automated time clock system to have information on hours employees worked. But if employees are being asked to work “off the clock,” their hours may be reflected in electronic records of who entered a building at what time or videotapes from a security system maintained at the facility or off-site.

Keep in mind that, while fragile in some ways, electronic information also has a way of persisting. Although electronic information may have been removed from a device or that device no longer exists, it may still exist elsewhere. For example, an e-mail might be found on another device, like a PDA, or in another location, like a system server or a system back up tape. And, as we have come to understand, hitting the delete button on an e-mail or deleting a word processing file does not eliminate the electronic information. The ability to recover “lost” electronic information is one factor contributing to the burgeoning field of computer forensics.

Be sure to look in all directions when investigating possible sources of electronic information, including in the mirror.

- You certainly want to interview your client carefully about all of the ways in which electronic information is created at their workplace. This would include the software and devices the employer uses in its HR functions, those made available to employees to perform their work, intranets and communication methods, and software or information that may exist for other purposes, such as expense reporting, sales records, etc.
- Consider, as well, third party sources of electronic information. Many companies use vendors to manage

or perform functions that will involve creation and storage of electronic information, such as the security services discussed above.

- Don't forget your client! Because employers normally have exclusive access to the records and documents relevant to your client's claims, it is easy for a plaintiff's employment lawyer to overlook electronic information that your client may have created or stored. But, it is vital to question your client concerning the means by which he or she may have created or stored electronic information. These could be on a home computer, cell phone or PDA, information burned to CDs, or your client's profile on myspace.com or comments in an employee chat room. And, you must give your client effective instructions to preserve any electronic information they have.

3) When and why send a preservation letter and what should it say?

The Duty to Preserve Evidence

Learning what information exists in electronic form and where it may be stored is one aspect of the common law obligation to preserve it as potential evidence. See *E*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582, 588 (D. Minn. 2005) ("The obligation to preserve evidence begins when a party knows or should have known that the evidence is relevant to future or current litigation."); accord *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). A failure to preserve evidence can result in sanctions, including the exclusion of evidence, even in the absence of bad faith. *Patton v. Newmar Corp.*, 538 N.W.2d 116, 118-19 (Minn. 1995) (affirming exclusion of expert evidence as sanction for inadvertent spoliation of evidence, resulting in summary judgment); *E*Trade Secs.*, 230 F.R.D. at 588-89 (citing *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988)).

Preserving Electronic Information Can Require Special Measures

Ensuring that your client and your adversary satisfy their obligations to preserve electronic information

as evidence requires a lawyer to have some understanding of how electronic information exists and how it can be changed. Electronic information is almost nothing like paper documents.

Electronic information is dynamic and fluid and therefore requires special care to preserve. For example, later versions of an electronic document can overwrite and destroy earlier versions of the document. But the electronic information is not just the text of the document. Even if the text remains the same, simply opening an electronic document will alter its "metadata" or the information maintained about the document, its author and its history. Other types of electronic files contain even different kinds of information. For example, e-mail may contain attachments and spreadsheets may contain embedded formulae that perform calculations across columns or rows. Further, methods of copying electronic information within a program or application or from one storage device to another will not necessarily preserve all of the information, and doing so can change the metadata.

So it is important to understand the kinds of ESI your client and your adversary have in order to determine what will be necessary to preserve that information. There is helpful information describing the characteristics of electronic information, such as Craig Ball's "Computer Forensics for Lawyers Who Can't Set the Clocks on Their VCR" (www.craigball.com/cf_vcr.pdf). But, unless you have a thorough knowledge of technical issues associated with various software applications and the storage and transfer of electronic information, it is wise to seek technical assistance in determining measures needed to preserve that information.

Instruct Your Client

Thus, while you will want to compose a preservation letter to send to your adversary at the earliest opportunity, your first obligation is to instruct your client effectively to preserve any electronic information they have created or stored. Instructions to your client can advise them of the duty to preserve, explicitly speak to electronic information and alert

them that accessing or saving the information may inadvertently alter it and to seek guidance if use or changes in information are expected. Providing the instructions in writing allows the client to study and refer back to them and offers proof that you and your client have addressed those duties at the outset.

Spell Out the Evidence for Your Adversary

The document preservation letter is a similar set of instructions for your adversary, although they need not comply. The preservation letter may trigger the duty to preserve evidence, if it represents the first notice to your adversary of the likelihood of litigation. Even if not, it serves to put your adversary on notice of the type of claims they face and the information you believe is important to your client's claims. It also should provoke an undertaking by the adversary to identify other information relevant to the claims, as the duty exists independent of any such letter or its specification of information. Perhaps most importantly, it should serve to stop the routine or inadvertent destruction of electronic evidence. At a minimum, the letter serves as unmistakable notice and a standard against which the receiving party's preservation measures, or lack thereof, can be judged.

For that reason, drafting the letter to demand reasonable measures to preserve information potentially relevant to your client's claims has the best chance of accomplishing your objectives. Because electronic information is ubiquitous, avoid using terms such as "any and all" which became common when the object of discovery was paper. It may be unreasonable and impractical to demand that your adversary preserve all sources or versions of electronic information that may contain relevant material. Instead, focus on describing the information you know or believe exists. Beyond that, appropriate categories of information relevant to the claims can be identified and then refined or limited to that associated with relevant individuals or positions, time frames or particular topics. Craig Ball's *The Perfect Preservation Letter* (www.craigball.com) is an excellent discussion of considerations that should go into a preservation letter, and also includes a model letter.

In most cases, you should send the letter as early as possible and in advance of the litigation. The primary purpose of the letter is to try to prevent the loss of evidence. Except for one willing to knowingly destroy evidence, the earlier the notice, the better the chance of preventing the loss. This is particularly true regarding organizations that routinely eliminate or destroy information in the administration of their information technology functions, by purging e-mail after a period of time, or recycling and over-writing back up tapes or devices. Here, business as usual routinely destroys evidence and acting early can result in the preservation of ESI, for example, by your adversary simply removing a backup tape from the recycling rotation or capturing a mirror image of a drive.

Ask for a Meet and Confer

Finally, the preservation letter should suggest that the parties meet to discuss the information to be preserved and the means of doing so. A discussion can promote an exchange regarding the information relevant to the claims and a focus on what should be preserved and the methods of preservation. An objective of the discussions should be an agreement on what and how information would be preserved. This can be to the advantage of the preserving party because it provides a route to a narrowed and less expensive and burdensome preservation obligation while eliminating risk of sanctions for spoliation. Such discussions also benefit the requesting party because they provide early knowledge about the existence and character of information relevant to the claims, the types of information available from the preserving party and assurance that information is being or unquestionably should be preserved.

Even if the preservation letter's invitation to meet is not accepted, the fact that the requesting party was willing to discuss and attempt to reach agreement on preservation helps to demonstrate that the preservation demands were both reasonable and practical. The preserving party would have a difficult time arguing that it did not implement measures

outlined in a letter because they were unreasonable and unduly burdensome where it refused an invitation to meet to discuss the issues and resolve any problems.

4) What issues need to be addressed at a meeting with my opponent or at a discovery conference?

Whether the meeting comes in response to a preservation letter before the litigation even commences or does not occur until the Rule 26(f) conference, you should be prepared to discuss with your adversary the issue of electronic information in a comprehensive way. While you may not have an in-depth understanding of all of the matters to be discussed, that should not deter you. Discussions with your opponent are a part of a process in which you will learn what you need to know, including those issues on which you may need technical assistance to reach your objectives. As lawyers, we learn how things work and how organizations operate as a function of the facts of each new case, and learning what and how electronic information is created and maintained is no different. And you may be surprised to find that, with some advance reading and preparation, you are better prepared and more informed than your opponent, who also will likely be learning along the way.

The amendments to the federal discovery Rules clearly are designed to encourage the parties to discuss electronic information early in the litigation and in ways that can eliminate potential problems, expedite production and balance benefits against burdens. Rule 26(a) and (b) and the accompanying Committee Notes discuss preservation of electronic information and issues associated with its production and use in discovery, including reference to the Manual for Complex Litigation, Fourth, § 40.25 (2004), which proposes a sample interim document preservation order. *Id.* at §§ 11.12, 11.442. Its primary purpose is to direct the parties to meet and confer on the terms of a final order that will preserve relevant evidence, make discovery more efficient and avoid abuse, controversy and expense. Given the need to tailor a document preservation order to best serve

those purposes while avoiding unnecessary disruption, the Manual identifies issues the parties should discuss, including issues relating to the existence and operation of computers and computer networks in the routine course of business that may alter or destroy existing data and the existence and accessibility of archival and non-archival computer system backups. *Id.* at § 11.442.¹

There are many resources that identify and discuss the topics that should be addressed in meetings between the parties. Barb Frederiksen, a gifted expert and consultant with Johnson-Laird, Inc. (www.jli.com), has provided an *Agenda for Discovery Meeting(s)* in the program materials which provides a comprehensive list that is commonsense and practically oriented to gather and organize information toward establishing a discovery strategy, from production to end-use of the information. That is the important thing to keep in mind throughout this process: you want to learn enough to be confident that all potentially relevant information is being preserved and that the right information is being produced, in a form and manner that efficiently allows you to identify and use the evidence you need, through a process that is economical, in the context of the case, and practically useful, given your capabilities and resources as an end-user.

In addition, the recent amendments to the ABA Civil Discovery Standards (August 2004) (www.abanet.org) identify a number of topics relevant to preservation and discovery of electronic information that should be discussed by the parties at an early point. Also, the Sedona Conference has developed recommended agendas for discussion and agreement between the parties (*The Sedona Principles: Best Practices & Principles for Addressing Electronic Document Production* (January 2004 Version) www.thesedonaconference.org).

All of these resources can be useful in making sure that you are addressing the necessary issues and learning what you need to know about the electronic information that is available and how it might be produced and used effectively.

I would note that obtaining the producing

party's document retention and destruction policies can be a significant and useful source of information. These policies can provide information regarding the breadth of information that is generated by the party, the means by which it is produced and maintained and the information that routinely is destroyed and the schedules by which that takes place. This is information largely necessary for a preservation order and that can point to the most effective and economical deviations from routine purging or destruction practices that will accomplish the needed objectives. Also these policies can serve as a basis by which you can check the accuracy of statements or other information provided by your opponent, or serve as the basis for demands that an uncooperative party be more forthcoming.

You also should not expect that all information will be provided and all questions will be answered in an initial meeting. Among parties and counsel with experience in electronic discovery, the process may proceed more quickly, but do not be surprised if your opponent or opposing counsel are not knowledgeable about electronic information or experienced in its discovery. Indeed, you may expect significant gaps in knowledge between your opponent and its counsel and between, for example, company representatives and its IT staff. This means that you may have to ask broad and searching questions with the understanding that opposing counsel will have to investigate to find an answer. It also means that you should not assume that the first answer you receive is accurate; it may be the result of a conversation between counsel and a company representative both of whom are relatively uninformed. You may need to be quite persistent in following up on questions and issues until you receive specific, thorough and consistent answers that comport with technical realities.

Of course, if you believe that these discussions are not yielding accurate or reliable information, or as a check on the accuracy of representations, you can take the deposition of your opponent's IT staff. The agendas and checklists described above can provide a basis to guide you in identifying the knowledge base of

the person or persons you need to request for a Rule 30(b)(6) deposition and the areas of questioning of those witnesses.

The amendments to the Rules relating to e-discovery clearly were intended to drive the parties to address electronic information in discovery and to do so early, cooperatively, economically and efficiently. However, we also may expect that some parties will not only be less informed about electronic information and its discovery, but will resist cooperation, preservation and discovery itself. In that event, you need to use the information you have obtained to pick wisely the battles you will take to the court to obtain the maximum effect. In many respects, the Rule amendments should assist you in getting the information you need.

5) How do I find out what electronic evidence my opponent has?

As discussed above, efforts to determine what ESI your opponent may have should start at the outset of your consideration of a case. The results of those efforts will help lead to identifying and obtaining that information. There are several avenues that can be used separately or in combination to determine the ESI you need from your opponent.

Meet and Confer

Rule 26(f) contemplates that the parties will meet to discuss and attempt to reach agreement on ESI. Take advantage of the opportunity. Use the checklists discussed above to determine the computer systems that your opponent has and the types of ESI they contain, such as e-mail, business documents and databases. Use the information gained from your initial investigation and your client interview to form the questions you ask and to evaluate the information provided by your opponent. Also, if you have or obtain your opponent's document retention and destruction policies, use the information they provide as the basis for questions and to measure responses. As noted, those policies should provide something of an inventory of the ESI your opponent creates, the

systems in which it is created and retained, and the schedule on which it is preserved and then destroyed.

Having independent sources of information for these discussions can be invaluable. As noted above, your opponent's counsel or representatives may be relatively uninformed. Or they may be uncooperative, or both. In any event, it is important to probe for information. If the responses seem incomplete, press to fill in the gaps. If the responses do not make sense or seem to contradict other information, insist on clarification until you receive logical, consistent information.

30(b)(6) Depositions or Interrogatories

If your opponent is unwilling or unable to cooperate in meet and confer sessions, or it appears unlikely that discussions will promptly or effectively provide information needed to understand your opponent's ESI, you can obtain the information through depositions of responsible IT employees. You may also want to pursue depositions to complement otherwise productive discussions, if questions remain unanswered. Use of a notice of deposition under Rule 30(b)(6) should allow identification of appropriate deponents by specifying the particular subject or subjects of inquiry. Make sure you indicate that you need information about the systems, format, storage devices, and the like, with respect to various kinds of ESI so your opponent identifies a person or persons with the depth and technical knowledge you need.

The checklists for meet and confer sessions also can serve as guides to the topics that should be covered in the deposition or depositions. Again, make sure to use the information gained from your investigation and any documents you have obtained to form your questioning and assess the accuracy or thoroughness of responses, and to identify additional relevant documents. Use a document request in connection with the deposition notice to obtain production of additional documents relevant to understanding the system or systems that are the subject of the deposition.

The same inquiries can be made through interrogatories, rather than depositions. The same

sources of information can be used to draft the interrogatories. However, the benefits of depositions are significant, and a strategy using document requests and interrogatories served early in a case may represent a more effective use of interrogatories.

Document Requests and Interrogatories

In order to expedite the process of learning about your opponent's ESI and actually obtaining it, document requests and interrogatories can be propounded early in the litigation. Early discovery requests serve to state the demands for information you know you will need and obligate your opponent to provide it at an early point. The discussions and any discovery that follow are then primarily focused on what is to be produced from among all that exists to respond to your requests. Further, you may have the benefit of already having important information from your opponent's responses to this discovery as discussions proceed. Having propounded discovery early, you are in a better position to demand prompt and effective responses by threatening a motion to compel.

In drafting the document requests, ask for the content of the material you need. The fact that much of the information you seek will exist in ESI is irrelevant to the subject matter of the information you will seek. However, make sure that your requests encompass the kinds of information you learned may exist in electronic form from your early investigation and interview with your client.

What distinguishes ESI from other sources of information is the unique features of its electronic format. To benefit from those features, ensure that you receive ESI rather than hard-copy versions of the information by requesting that the information you want be produced in electronic form where it exists, and in hard-copy form only where it does not exist electronically. This stated preference for information in electronic form should enable you to obtain all responsive material that is available in electronic form. Accompanied by a definition of "document" as any non-identical duplicate, should then result in the production, for example, of a document in its electronic form, including metadata, as well as prior drafts of the

document, and a hard-copy that was printed and to which were added marginal notes.

Document requests also should seek materials that describe what ESI and other sources of information exist, where and how they are stored and when and how they are retained or destroyed in the regular course of business. Request copies of document retention and destruction policies, descriptions and inventories of document and data systems and other descriptive materials regarding your opponent's IT functions. For example, information describing your opponent's capabilities in restoring information from backup tapes or archives, converting ESI from one format to another and de-duplicating data all can be important in discussions or potential litigation on issues of whether electronic information is reasonably accessible and usable regarding the form and cost of production.

Drafting interrogatories targeted at information needed for preservation and discovery of ESI should cover the topics on the checklists discussed above. They also should ask for explanations of your opponent's various capabilities in handling and managing electronic information where written descriptions may not exist. Propounding interrogatories early in a case may provide you with information you need regarding ESI at a time when you are attempting to develop a plan for electronic discovery and, at least, will require your opponent to give specific attention to the topics and issues you will first discuss in the Rule 26(f) conference, in the likely event that all issues are not resolved in that meeting.

6) Why are the “form for production” and “reasonably accessible” sources of electronically stored information important under the amended Rules?

Under the amended Rules, whether particular electronic information is reasonably accessible will determine whether you will receive ESI and perhaps whether you will have to pay some of the cost of its production. The form of production concerns whether you will receive the information in electronic or paper form and the format in which you will receive ESI.

Both are thus vital matters that deserve your early careful attention.

Form of Production

Above I suggested that document requests state that information should be produced in electronic form where it exists. That is one aspect of specifying the form of production, but not all that needs to be said on the subject. Unless you specify that you want information produced in electronic form, it is conceivable that your opponent could satisfy its obligations by providing hard-copy printouts of electronic information (although the omission of metadata and other types of information may render production only of the printout incomplete). But even if information is to be produced in electronic form, there are a variety of formats in which it could be produced and you need to consider that question carefully to ensure that you can effectively and economically use the ESI once it is produced.

The format in which ESI is produced is critical to whether you have the ability to electronically search the information or whether it needs to be converted into another format, which could result in added costs. For example, an electronic document could be produced as a TIFF image. While it would be produced as an electronic file and, when opened, you could see the text of the document, it would not be electronically searchable and would not contain associated metadata. Thus, although produced in electronic form, it would provide incomplete information and deny you the benefit and efficiencies of automated searches. Similarly, the ESI might exist in a proprietary software application and if produced in that format, could not be accessed without purchasing that application and, even then, may not be amenable to searches or appropriate information management functions. Thus, it is important to give attention to the format of the ESI and to determine those formats which will permit you the ability to search, use and manage electronic data.

Generally, the rule has been that the requesting party is entitled to specify the format in

which electronic information is to be produced and if the responding party fails to so produce the data, courts will enforce the specification. Amended Rule 34 provides a regime for specifying formats for production, objections, statements of alternative formats, and determination of the issue by the court, if necessary. Briefly, the requesting party has the opportunity to specify a form in which the ESI is to be produced, to which the responding party may object while proposing an alternative. If the requesting party fails to specify a form for production, the producing party is free to produce in the form in which it is ordinarily maintained or select a format of its choosing, so long as it is a form that is reasonably usable. Disputes will be determined by the court, which the Committee Notes suggest will not be limited to forms suggested by the parties.

Requesting ESI in its “native format,” that is, the form in which it exists in the software application in which it was created, generally is the best way to capture all of the metadata and associated information. Converting data to another format can result in the loss of some metadata. On the other hand, a native format may be proprietary or represent a difficult form or environment in which to use the data. Therefore, in propounding document requests, it may be best to request the ESI in native format and with all metadata, or in another format that retains all metadata and is searchable. This makes clear your twin intentions to obtain all included information and in a usable form.

In the end, both parties likely will want the electronic information in several formats. In order to be able to view the document or material as if it were printed (often indispensable to making sense of the material) and produce printed versions for exhibits, the information should be provided in TIFF images. To be able to perform automated searches, the material also should be produced in text files. To capture metadata, including information about attachments and other features, searchable files of metadata should be produced, separate from but able to be connected to the text and TIFF versions of the information. These three separate but associated

forms of electronic information will, in most cases, provide all of the information and capacity to use that information to identify evidence.

It is always best to resolve these issues through discussion and agreement with your opponent, where possible, and the amended Rules clearly encourage that process. The question of the form for production is an area where the parties may have mutual interests: both parties will need the data in a form that is usable, and Rule 34 sets the usability of the data as a requirement of any choice of form by the producing party. Thus, if the native format of the data would be awkward or difficult to produce or would make it difficult to work with the information, the producing party may want to convert it to another more usable form. So long as all data from the native format is included and preserved, that should serve the requesting party’s interests as well.

And the requesting party should approach discussions mindful of the opportunities for give and take across the spectrum of production and preservation issues. For example, if the producing party will assume the responsibilities of converting the ESI into a format useful to the requesting party, that party may agree to narrow the amount of ESI subject to preservation obligations. Or, where the producing party agrees to convert ESI into a different, more usable format, the requesting party might agree that less than all of the metadata need be converted or produced as an initial matter, so long as it remains available in its native format, should the need to obtain it arise. It can pay to be mindful of all of the issues that require resolution in preservation and production and to identify and find resolutions that serve the respective parties’ interests among those issues.

Reasonably Accessible

Whether electronic information is reasonably accessible has been an important consideration in determining whether the cost of producing that information would be shifted from the producing to the requesting party in pre-amendment litigation. See, e.g., *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 284 (S.D.N.Y. 2003). The amendments work a substantial

change here. Now the question is whether the responding party must produce electronic information in discovery. Under amended Rule 26(b)(2)(B), a producing party needs only to identify, not produce, ESI from sources that it contends are not reasonably accessible. The requesting party may attempt to establish good cause, in response to which the court will determine whether the information is to be produced and may specify conditions for the discovery, including limitations on the type or volume of information and allocation of the cost of production.

Technology is eliminating some arguments that ESI is not accessible. Data on backup tapes or devices now are often easily and frequently recovered for business purposes. Current technology for the conversion of data across formats and applications is increasingly available and can be found in off-the-shelf programs at very modest prices. Asking questions on these subjects in your investigation and discovery may help forestall or win litigation over whether ESI is accessible; descriptions or promotional material touting a company's IT capabilities and services can prove useful in demonstrating its capability to produce or translate electronic information, for example. However, information created in now-obsolete software applications, sometimes referred to as "legacy" data, or existing only in aging storage devices may still be difficult to recover.

Even if sources of ESI can be accessed, there is the question how to identify that material which is responsive and should be produced from among what may be huge quantities of irrelevant electronic data. Here attention can be given to identifying various types or sources of information and including or excluding categories on that basis. Sampling or testing electronic information to determine whether it contains relevant content and ways in which it can be produced or searched also can be useful. The development of search terms to identify relevant material, including through testing proposed terms and measuring the results within samples of the electronic information, is particularly useful in narrowing the universe of information to be produced. To the extent the parties can cooperate in these

enterprises, the burdens and costs of production can be reduced. In the absence of cooperation, the requesting party must press for the ability to sample or test the information itself, or for the responding party to do so in a transparent process that shows the results.

Search terms and automated searches also can serve to expedite examination and production of ESI by identifying potentially privileged and protected material and removing it for purposes of sampling or testing. Or they can be used to remove potentially privileged material from an initial production and be the subject of a separate review. This capacity, together with the amended encouragement in Rule 26(b)(5) and (f) to discuss "quick peek" or "claw back" agreements to preserve privilege and incorporate them into a court order and in Rule 16(b)(5) and (6), all can serve as ways to reduce delay and expense in production.

It is reasonable to assume that, with the prospect of excluding certain electronic information from discovery, responding parties will be tempted to declare ESI not reasonably accessible, and litigation on the issue will ensue, complete with battles of computer forensics experts. Of some concern are the suggestions in the Committee Notes that litigation over the issues of reasonably accessible information and good cause for its discovery may involve distinct discovery and extended litigation. The Notes refer to sampling of data to learn what information may exist on certain devices and its value to the case, as well as the methods, burdens and costs of accessing the information. Certainly, these methods sometimes are necessary, for example, in determining what exists on older backup tapes and how to locate and extract responsive information. These aspects of the Rule amendments should not be permitted universally to increase the cost of discovery by interposing as prerequisites, first, the cost of discovery and expert testimony needed just to establish that the information is accessible and there is good cause for its discovery and, second, the cost of identifying, recovering or converting the information to a usable condition. In time, developing standards in case law

and technological advances may combine to reduce litigation on these issues and narrow the circumstances in which data need not be produced.

7) What would I do with electronic documents if I got them, and how can I afford electronic discovery?

The question how you would make use of electronic documents also should be asked from the beginning of your investigation. Of course, as evidence, the use of ESI follows the facts you need to find and prove; whether they are empirical facts from a database, practices or standards from handbooks or intranet policies, or motive or intent reflected in e-mail or interview notes. The difference is that enormous quantities of information can be obtained, searched, identified and managed with great efficiency.

The ability to obtain, search and effectively use ESI depends on several factors: whether the data is in a format that easily can be searched and managed; the volume of the electronic files obtained; and the resources and capacity you have to devote to analyzing and managing the data.

As discussed above, unless the ESI is in a form and format that is searchable and easily managed, it will be of little value. Thus, careful attention must be given to obtaining electronic information in a format that permits automated searches and other efficiencies. Remember that the question of an appropriate format applies to each type of data — the format for e-mail may be different than spreadsheets and different than web pages. And the software to be used to search the data must match your capacity to handle that data. There is off-the-shelf software available to manage and search electronic information loaded onto your own servers. On the other hand, vendors offer access to software and other tools to search and manage remotely over the Internet electronic information stored on their system servers.

The fact that enormous quantities of information are easily available in electronic form does not mean that you should demand that it be produced. Electronic data requires some expertise and effort to manage, and space on a server where it can be stored

and searched. Obtaining too much data may exceed your capacity to manage and analyze it to identify evidence. Of course, vendors are available to load, clean and store electronic information and provide the means to perform automated searches of virtually any quantity of data, at a cost. Thus, consider the resources you have or can purchase to manage the data and plan for the production of corresponding volumes of data.

Plan for the electronic discovery that fits the needs of your case, your capacity and your budget. Start with a conversation with the person who handles your IT needs about the assets you already have and your personnel or staffing capacity. Interview vendors and assess what they have to offer and at what cost. Consult with an e-discovery expert to explore alternative approaches. Talk to your client about the need for and benefits of electronic discovery and the associated resource and capacity issues. Develop a plan that reflects your needs, capabilities and available resources. Following that plan to guide your discovery demands and the negotiation and litigation of ESI issues will result in a manageable and efficient means of identifying the evidence to prove your case. ■

Thomas J. Henderson
Sprenger & Lang PLLC
1400 Eye Street, NW
Suite 500
Washington, DC 20005
phone - (202) 772-1158
fax - (202) 332-6652
thenderson@sprengerlang.com
www.sprengerlang.com

¹The Manual's Sample Order, at § 40.25, 2. *Subjects for Consideration* provides as follows: *The parties should attempt to reach agreement on all issues regarding the preservation of documents, data, and tangible things. These issues include, but are not necessarily limited to: (a) the extent of the preservation obligation, identifying the types of material to be preserved, the subject matter, time frame, the authors and addressees, and key words to be used in identifying responsive materials; (b) the identification of persons responsible for carrying out preservation obligations on behalf of each party; (c) the form and method of providing notice of the duty to preserve to persons identified as custodians of documents, data, and tangible things; (d) mechanisms for monitoring, certifying, or auditing custodian compliance with preservation obligations; (e) whether preservation will require suspending or modifying any routine business processes or procedures, with special attention to document management programs and the recycling of computer data storage media; (f) the methods to preserve any volatile but potentially discoverable material, such as voicemail, active data in databases, or electronic messages; (g) the anticipated costs of preservation and ways to reduce or share these costs; and (h) a mechanism to review and modify the preservation obligation as discovery proceeds, eliminating or adding particular categories of documents, data, and tangible things.*