

HOW TO PRODUCE ELECTRONICALLY STORED INFORMATION UNDER THE NEW RULES

by

Gregory L. Fordham, CPA, CIA, CCE, Sec+, MCP



www.knfcon.com

2550 Northwinds Parkway, Suite 275
Alpharetta, GA 30004
800-335-1188

HOW TO PRODUCE ELECTRONICALLY STORED INFORMATION UNDER THE NEW RULES

by

Gregory L. Fordham, CPA, CIA, CCE, Sec+, MCP

The use of computerized evidence in the courtroom has a long history. Its acceptance was first memorialized over thirty years ago in the 1970 amendments to Rule 34 of the Federal Rules of Civil Procedure. Those changes made it clear that data compilations were subject to request for production.¹

Although initially the concept of computerized evidence was one of paper printouts, computer savvy practitioners were quick to recognize the benefits of digital evidence and formed their request to ask for computerized data in native form. Although there was resistance, the Courts recognized both the relevance and promise of digital evidence. Consequently, it was subject to discovery and presentation as evidence after a proper foundation was established.²

PRODUCING ELECTRONICALLY STORED INFORMATION

Despite its acceptance by the judiciary, electronic discovery remained an art form practiced by a small portion of the Bar. It was probably not until the late 1990s and the revelations of incriminating digital evidence presented by the Government at the *Microsoft* trial that electronic discovery gained widespread interest. By then plaintiffs had already noticed a reduction in paper based evidence and were forced to consider a more modern approach.

As electronic discovery attracted more interest, it produced more disputes and decisions. While some retrod old ground and argued against the requirement to produce electronic data, others sought safe harbor in other sections of the Federal Rules and erected barriers with claims that discovery of digital evidence was too costly and overly burdensome. They then found vendors and experts who would prove the validity of such claims with the prices they quoted for performing the work.

With the likes of *Rowe Entertainment*,³ and *Murphy Oil*,⁴ defendants seemed to have blunted the attack. Then decisions granting sanctions in *Residential Funding*⁵ and *Metropolitan Opera*,⁶ along with a more reasoned analysis in *Zubulake*⁷ rekindled the interest. At the same time, the question of whether to use electronic discovery was elevated from one of best practice to potentially malpractice, according to Julie K. Hannaford, Co-Chair of the American Bar Association's, Computer and Internet Litigation Committee .⁸

PRODUCING ELECTRONICALLY STORED INFORMATION

Set in the notion that electronic discovery was different than paper discovery and concerned with how to secure the just, swift and speedy determination of every action, various groups began a study of electronic discovery and the rules of civil procedure. In the end they were able to articulate what they had already concluded—electronic data is different from paper and the differences are several. More specifically, electronic data is found in larger volume than paper documents; has greater persistence; is more dynamic; is more complex; and a greater dispersion than paper documents.

According to these groups, the volume of electronic documents is significantly larger than the volume of paper documents. This increased volume is the result of how easy it is to create electronic documents. For example, the e-mail has replaced many verbal communications—things that used to be handled by telephone or discussed at the water cooler.

Besides their increased volume, electronic documents are also more persistent than paper documents. For example, once a paper document is thrown away or shredded it is considered unretrievable. Electronic documents, however, are still retrievable even though they may have been deleted. The process of deletion does not erase the electronic data, rather it simply removes the pointers to where that information is stored on the electronic media. The data, itself remains there until overwritten.

PRODUCING ELECTRONICALLY STORED INFORMATION

Electronic documents are more complex than paper documents. Since the electronic documents are part of a computerized system that uses various attributes about the document to control its handling of that document, an electronic document has more data elements than simply its content. Indeed, there are various time and date stamps, there is data hidden within the document that might only be used by the system or offered by the system as a feature to the user to facilitate management of the documents. The document might also have many parts such as a spreadsheet that has many worksheets or a database table that has many rows. By itself, the worksheet or database rows may not have any discernable meaning when separated from these other parts. Similarly, the content of the worksheets or database rows may have no meaning without the column headers or field names that identify the contents of the cells.

Electronic documents are more dependent on the systems that created them than paper documents. In order to create an electronic document the user would have required certain software and hardware. As technology changes over time, it is possible that the software and hardware required to manage an electronic document are no longer used by the litigating party. For example, the organization could have moved to a different kind of tape format for creating backup tapes for disaster recovery purposes. If sufficient time has elapsed since that change was made then the tape reader could have been disposed of or lost. In such a case, it might make recovery of data on the tapes considerably more difficult if not impossible.

PRODUCING ELECTRONICALLY STORED INFORMATION

Electronic data is also more dynamic than paper documents since electronic documents can be more easily changed than paper documents. The changes can occur when the document content is changed by the user as well as when any of its other related attributes are changed by the system. For example, its last accessed date can change when the file is opened even though no changes were made to the contents of the document.

Finally, electronic documents are different from paper documents in that they can have much wider dispersion throughout the organization. In other words they could reside on centralized servers as well as at numerous individual workstations. Certainly paper documents also were subject to having numerous formal and informal storage locations—the formal filing system as well as an employee’s personal files. However, the distribution list feature of e-mails has increased the dispersion of potentially relevant electronic documents throughout the organization.

While there is truth to the above examples there is also truth in that there are more US dollars than Moroccan Dirham. The increased number of US dollars does not make them more prolific or buying and selling more difficult nor does their volume encumber those that choose US dollars as their exchange medium.

Undoubtedly many proclaimed the unfair burdens of paper discovery after the birth and widespread use of the copy machine, the fax machine and the post-it note. Indeed, many of the

PRODUCING ELECTRONICALLY STORED INFORMATION

of the attributes listed above are what make digital evidence so superior to paper documents both in terms of its evidentiary value as well as the efficiency at which it can be used to prove or disprove a claim.

Despite all the other pontificators, Judge Scheindlin got it right in *Zubulake*.

“Whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production). In the world of paper documents, for example, a document is accessible if it is readily available in a usable format and reasonably indexed. Examples of inaccessible paper documents could include (a) documents in storage in a difficult to reach place; (b) documents converted to microfiche and not easily readable; or (c) documents kept haphazardly, with no indexing system, in quantities that make page-by-page searches impracticable. But in the world of electronic data, thanks to search engines, any data that is retained in a machine readable format is typically accessible.”

In essence, Judge Scheindlin recognized that it is not volume, nor persistence, nor any of the previously mentioned attributes. Rather, it is simply a matter of accessibility. After all, once the data is accessible, the computer itself can render all other objections irrelevant.

PRODUCING ELECTRONICALLY STORED INFORMATION

What is needed, therefore, are experts who do not simply stand at the shore and proclaim the earth to be flat or watch the sun rise in the East and set in the West and deduce that the Sun revolves around them. Rather, the challenge is to find experts who understand what the data holds, how it is managed and can devise methods for leveraging the unique properties of this information with economy and efficiency.

The new rules enable the benefits of digital discovery. But while paper was uniform, digital evidence is diverse. While paper fit all communications, digital data has been engineered with greater specificity in order to maximize the advantages of its particular application. In other words, digital data is more specialized. The rule changes recognize this fact and provide greater flexibility to the parties in order to understand their data. This is accomplished through four general changes to the rules. First, a new category of data called Electronically Stored Information (ESI) is used to refer to digital evidence rather than try and interpret the term documents to include digital evidence. The second is the distinction between accessible and inaccessible data. The third is a staged approach to conducting discovery. The fourth is an increased need for planning and management of the entire discovery process from preservation through production by directing the parties to identify discovery objectives early and begin to resolve the particulars of the production. Each are discussed in the sections that follow.

PRODUCING ELECTRONICALLY STORED INFORMATION

Electronically Stored Information (ESI)

Electronically Stored Information (ESI) is the term now given to digital evidence. Although the term documents had previously been interpreted to include digital evidence, the new term was developed to make the interpretation of the rules closely match the plain meaning of their words. The comments to Rule 34 state that,

“Rule 34(a) is amended to confirm the discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium form which it can be retrieved and examined. At the same time, a Rule 34 request for production of ‘documents’ should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and “documents”.

The new rule changes do not try to more precisely define digital evidence or ESI. Rather, the lesson of the last thirty years is that technology changes rapidly and is difficult to predict. So, rather than develop an artificial boundary that might function more like a trap the concept of ESI is rather broad. In fact the comments to Rule34 state that,

PRODUCING ELECTRONICALLY STORED INFORMATION

“The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically . A common example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically—information “stored in any medium,” to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments’

Accessible versus Inaccessible ESI

The new rule changes distinguish between accessible and inaccessible ESI. In keeping with the objective that the rules are designed to promote swift, economical and just resolution, a party is generally not required to produce ESI that is not reasonably accessible.⁹ There is no predetermined list of accessible versus inaccessible data. Rather, whether or not ESI is reasonably accessible is a factual determination that considers a number of factors. Those factors are whether the data is:

- Unreasonably cumulative or duplicative;

PRODUCING ELECTRONICALLY STORED INFORMATION

- Obtainable from some other source that is more convenient, less burdensome or less expensive;
- The requesting party has had ample time to obtain the info; and
- The burden and expense of discovery outweighs its likely benefit.¹⁰

Principle 6 of the Sedona Principles suggests that the responding parties are best situated to determine the appropriate technologies for preserving and producing ESI.¹¹ Although the new rule changes allow the responding party to determine what is not reasonably accessible, that decision is subject to review under a motion to compel. In addition, any data that the responding party deems is inaccessible, the responding party should provide enough detail to allow the requesting party to evaluate the burdens and costs of discovery and finding responsive information.¹²

Even in the case of *Zubulake*, where backup tapes and deleted files and file fragments were identified as examples of inaccessible data, such a determination only triggers further cost shifting analysis.¹³ Even then the cost shifting analysis may not confirm that the data is reasonably inaccessible if the various factors for cost shifting are not satisfied.

While intuitively it make sense that the responding party is best situated to determine what ESI is reasonably accessible versus not reasonably accessible, cases like *Rowe Entertainment* and *Murphy Oil* indicate otherwise. Indeed, those cases demonstrate how respondents will support

PRODUCING ELECTRONICALLY STORED INFORMATION

their requests for protective orders with vendors suggesting inefficient production methods and charging big fees. In order to avoid having data erroneously categorized as inaccessible, requesters should stay active during the planning stages and curious about the respondent's data and management systems.

Discovery Done in Stages

The new rule changes also recognize that once preserved the discovery of ESI can be done in stages. Essentially, since the volume of data could be large there is no requirement that it be done at once. Rather, prioritize the data such that the discovery and production begins with the more easily accessible data that is more likely to bear fruit. Then progress iteratively through the data.¹⁴

A likely progression would consider on-line active data first. Then progress to near-line data. Then to off-line data such as backup tapes and then to erased, fragments or damaged data.

Increased Planning of the Discovery

PRODUCING ELECTRONICALLY STORED INFORMATION

The new changes to Rule 26(f) directs the parties to meet and discuss their discovery plan for ESI including the preservation of ESI, any issues relating to the disclosure or discovery of ESI including the form in which it will be produced, and any claims regarding privilege. According to the Committee notes the changes were implemented to encourage discussion at the outset in order to avoid subsequent disputes. To accomplish meaningful discussions it may be necessary for counsel to become familiar with the various compute systems used by the parties or to consult with individuals having special knowledge of the parties' computer systems.

While the rules contemplate discussions and advanced planning at the scheduling conference, the effort actually should begin much earlier; with the preservation notice. It should then proceed through the initial disclosures and conclude at the scheduling conference. What is more, the discovery plan should incorporate other efforts and understanding the systems through interrogatories, depositions and inspections.

Preservation Notices

Discovery planning begins with the preservation notice. It is the first chance to consider the people, places and issues related to the case. Once identified the next step is to start developing the conceptual model about the related ESI. This model should include development about the types of data that likely exists as well as the types of systems used to manage that data. Once the

PRODUCING ELECTRONICALLY STORED INFORMATION

likely systems are identified begin to consider the best ways to extract the responsive data and to examine it.

Initial Disclosures

The next phase in discovery planning occurs with initial disclosures. Under Rule 26(a)(1),

“[A] party must without awaiting a discovery request provide to other parties:

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of or a description by category and location of all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;”

PRODUCING ELECTRONICALLY STORED INFORMATION

Although this is information that the disclosing party plans to use in its case, it can contain valuable information that can be used to continue developing the conceptual model. For example:

How does the list of people compare and contrast to the preservation notice?

How does the list of ESI compare and contrast to the preservation notice?

Discovery Planning Conference

The next step in discovery planning occurs at the discovery planning conference. The discovery planning conference is held at least 21 days before a scheduling conference is held or a scheduling order is due. In addition to discussing the nature and basis of claims and defenses and the possibilities for settlement, the parties are also to discuss various issues relating to preserving electronic information, the form in which ESI should be produced, and issues relating to privilege or of protection of trial-preparation materials.

Preservation

PRODUCING ELECTRONICALLY STORED INFORMATION

One of the items to be discussed as the planning conference are issues relating to preserving discoverable information.¹⁵ If a preservation notice has already been sent then the conference would be a good time to inquire about the data that was preserved in accordance with the preservation notice. If a notice has not been sent then the conference would be a good time to discuss a list of ESI that should be preserved. At the same time, particulars about the kind of ESI and locations would be helpful as would the types of systems used to manage the data.

Another subject suitable for the preservation discussion is the method used to preserve the data. For example, were forensic images created or was the data simply collected and stored. Certainly the preferred method would be for forensic images to have been made.

Production Format

The precise form in which electronic data is to be produced has been an issue argued among the litigants. Generally, however, it has been held for some time that production in electronic form is permitted.¹⁶ Even so, there can be plenty to discuss regarding the specific electronic form. For example, should e-mails be produced as a mailbox collection in a .PST file (Microsoft Outlook file format) or should they be produced as individual messages in .MSG format (Microsoft Outlook message format).

As legal professionals have learned the wealth of information contained within the electronic data, that cannot be discerned when those same documents are produced in paper form, they have insisted on production in electronic form. In fact, in current times it is even more widely recognized that documents produced in paper form lack the important metadata contained within electronic documents. As a result, when the requesting party has asked that electronic documents be produced in native format and the form that they are maintained in the ordinary course of business they have been successful.

Under the new rules the production format is one issue that the parties are to decide the form that the production of data is to be made. Rule 16(f)(3) says that, “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.”

Both requesters and respondents should want to produce their data in electronic form. It is simpler for the respondent and richer for the requester. Although paper as a medium was generally universal, electronic data is much more specific and comes in a variety of formats. One of the issues that the requester needs to determine is whether it can handle the producer’s electronic data in its native format. If not, then the requester needs to determine whether there is a common standard form to which the producer’s data can be converted.

For example, a number of the litigation support software tools support the Microsoft Outlook format but do not support the IBM, Lotus Notes format or even the Microsoft Exchange format.

PRODUCING ELECTRONICALLY STORED INFORMATION

So, what the requester and producer will have to decide is what format the data naturally resides and whether or not it needs to be converted into some other format.

De-duplication

Since it is well recognized that the volume of electronic data will be significantly large one of the key tools that the litigants will require to conduct efficient discovery is a means to identify and remove the duplicates. Removal of duplicates should not be performed based on file name or subject matter or other visible characteristics of the data. Rather, the best method for identifying duplicates is through the use of digital signature or digital fingerprint algorithms.

The MD5 message digest was developed in 1994. It is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint" or "message digest". The MD5 algorithm is intended for digital signature applications. At 128 bits the number of potential outcomes of the MD5 message digest is 2^{128} which is larger than 3.40282×10^{38} or the number 340282 followed by 33 zeros, which is larger than a trillion, trillion, trillion. It is believed that this number of unique outcomes is so large that it is highly remote that two different messages would have the same MD5 message digest.

In the event that the MD5 algorithm does not provide a low enough probability that two documents would produce the same message digest then there is also a SHA-256. This algorithm is 2^{256} or 1.157×10^{77} or the number 1157 followed by 74 zeros which is about twice the number of possible outcomes as the MD5.

Thus, either the MD5 or SHA-256 algorithms can be used to determine a signature of all electronic documents comprising the population of those that are discoverable. From that population, the unique documents can be identified based on their message digest values.

Furthermore, the fingerprint is "non-reversible". In other words, it is computationally infeasible to determine the contents of the input file based on an MD5 hash value.

When performing the deduplication process there are two elements that requesters and producers will want to determine. The first is the granularity at which the deduplication will be performed with compound documents. For example, e-mails have both a message and they have attachments; hence a compound document. When developing a deduplication plan should they

PRODUCING ELECTRONICALLY STORED INFORMATION

be deduplicated at the entire e-mail level (message and attachments) or at each element (message and each attachment separately). Usually it is better to use the most granularity possible.

The second is producing a file list with location path and hash value of all the items considered. Knowing where they came from could help later in evaluating the migration of data or identifying lost data. The list could be provided in a database form that could be queried since it is likely that the number of items in the list would be quite large.

Signature Analysis

Generally, people identify the file type by its extension. However, in a Windows environment the extension is not as reliable as in other systems. Consequently, one method of validating a file extension is through signature analysis.

In addition to be identified by their extensions, many types of files have a certain combination of bytes in the first few bytes of the file. As an example, the following signatures are found in the first bytes of the indicated file types.

SIGNATURE	FILE TYPE
PK	Zip file
ÿWPC	Word Perfect

PRODUCING ELECTRONICALLY STORED INFORMATION

MZ	Executable program file
ĐĬ	Microsoft Office file

When attempting to hide data, evil doers often change the extension to a file and then mingle it in with other similar file types. For example, a Word document could have its extension changed from .DOC to .EXE and then the file moved to the Windows system directory where it will blend with other executable program files.

Signature analysis, therefore, is a means to review all the files on a media and identify those of a certain type that are believed to contain relevant data. So, when developing a discovery plan, the requester may want to specify that if all the files of a certain type are requested that the producer employs some kind of signature analysis process in order to accurately identify that all of the files of a certain type were provided.

Hash Analysis

In addition to de-duplication, digital signature such as MD-5 hash or SHA-256 can be used to accept or reject the files that are to be considered. In other words, if a particular file is sought, such as a trade secret, then search parameters could be constructed to look only for files with that hash value.

PRODUCING ELECTRONICALLY STORED INFORMATION

The hash value is not affected by a change in file name, since the file name is not part of the file itself but resides in the filing system. Thus, if the file name was changed as a means to hide its nature, the hash analysis would still detect it.

Hash analysis can also be used to reject or exclude certain files. For example, there are lists produced containing all the known hashes for commercial software packages. These would include the sample files that would be included if one were to ask for all of the Word or Excel files found on a person's computer. Thus, if these lists were included in the respondents production process then such files could be omitted from production.

Similarly, the lists of known hashes can be used to exclude files from subsequent searches or analysis. If these lists were included in the respondents search process then searches could be performed faster in addition to having them produce smaller result sets.

Data Carving

Data carving is another way to use the signature analysis discussed previously to locate and recover deleted files of interest. If the deleted files may no longer exist in the file system, then they would not be recoverable by trying to rebuild the file system and cross reference to the file

PRODUCING ELECTRONICALLY STORED INFORMATION

storage locations. So, signature analysis provides the ability to search the free space on a drive and find instances of files having the requisite starting byte signatures and ending trailers. The data carving technique then takes everything in the middle and reconstructs the file.

If the recovered file was actually fragmented then its various components are not stored in contiguous storage locations. As a result, when all of the data between the starting signature and ending trailer are recovered and the file reconstructed, it likely will not function. In fact, when one views the file through a Word or Excel viewer, for example, the person is likely to only see a large volume of non-sensical special characters.

What needs to be done to facilitate the review process is that after the carved data is reconstructed that it be subjected to some kind of automated scoring process that evaluates the readability of the reconstructed documents. Those that receive a high enough score are passed for normal production. Those whose scores are not high enough can be produced in a separate batch for analysis using lower level review tools.

File Fragments

File fragments are only portions of a complete file or communication. Typically, one thinks of file fragments as being that portion of a deleted file that remains after it has been partially overwritten by another file. File fragments can also exist in those portions of memory that are

PRODUCING ELECTRONICALLY STORED INFORMATION

stored on the hard drive such as Windows Swap file. In that case, the fragments are not what is left of an entire file but only the portion of the file or screen or whatever that was mapped to the hard drive.

Typically file fragments are found during low level searching of the electronic storage media. In other words, searching of the data storage areas and not necessarily the files occupying those storage area. Most likely this kind of analysis would be considered inaccessible data, although the tools for performing this kind of analysis are improving so much that it might well evolve into something more routine and, thus, reasonably accessible.

This kind of search technique is something that should be considered and discussed at the planning conference. If the parties agree to the use of a third party expert it would certainly be something that they could perform as part of the normal search and production process.

Metadata

There has become an increased interest in metadata. According to Wikipedia, metadata (Greek meta "after", "about", "beyond" and Latin data "information") are data that describe other data. Generally, a set of metadata describes a single set of data, called a resource. Meta is a common English prefix, used to indicate a concept which is an abstraction from another concept, used to

PRODUCING ELECTRONICALLY STORED INFORMATION

analyze the latter. For example "metaphysics" refers to things beyond physics, and "meta language" refers to a type of language or system which describes language. Metadata are of special interest in various fields of computer science and are used in features such as database, information warehousing, imaging, computer files systems, etc.

Practitioners have learned that there are many things about system use and document management that can be gleaned from the metadata. In the case of *Williams v Sprint/United Management Company* it was held that metadata is discoverable.¹⁷

Metadata can involve data within the document files themselves as well as data within other system resources. For example, the filing system would contain various date stamps that would be of interest. With respect to backup tapes, the tape catalog, which is the tape's file system, would contain similar information.

There are still other resources that could contain important and relevant metadata. For example, the registry, event logs and link files are other sources of metadata that can have important and relevant metadata.

Since the preservation effort will likely, or should have, involved the creation of forensic images, the software tools usually used to examine those images and to produce data are also capable of

PRODUCING ELECTRONICALLY STORED INFORMATION

providing various file system metadata as well as these other system resources like the registry, event logs and link files.

Privilege Issues

Privilege is always a thorny issue for electronic discovery. It appears in two separate contexts. The first is how to actually produce data that has been determined to be or contain privileged information. Clearly the problem with the production is the effort that can be required to evaluate the contents of an electronic document for privilege data. After all, one must examine both the naturally visible as well as the portions that are not naturally visible and can only be viewed with low level tools like a hex editor.

Perhaps the simplest method is to provide a privilege log. This protects the information while providing the parties with a list that they can use to evaluate whether further discussion of the privilege claims are warranted.

The next option is to provide redacted copies of the documents but provide them in a form such as tagged image format (TIF) or portable document format (PDF). Neither of these formats retain the hidden metadata. Thus, what you see is what you get.

PRODUCING ELECTRONICALLY STORED INFORMATION

The final option would be to provide a redacted electronic copy but this is likely impractical, although metadata scrubbing software could be used to remove the hidden metadata and normal redaction processes could be used to replace the normally visible text.

The second option involves the review of the media itself. When a tape or hard drive is imaged, it simply is not practical to redact the media for irrelevant and privileged data. So, the next best step would likely be to use experts working under protocols to which the parties have agreed.

Essentially, these protocols would have the experts collect the data and then search and review the data for the parameters that both sides have agreed are suitable criteria for selecting relevant electronic data. The results of the searches and selections performed by the expert are then provided to the responding party for privilege review prior to production to the other side.

Both the *Rowe Entertainment* and *Murphy Oil* cases exemplify this kind of arrangement.

Although both cases are best known for their opinions involving cost shifting, they also contain descriptions of the protocols adopted by the parties to handle privilege issues. In each of those cases, experts were allowed to image, extract and analyze the respondent's data in order to find items of interest to the issues in the case. Interestingly both protocols allowed the privilege review to be either before or after experts were used to sift through the data but the most economical was where the privilege review was performed after the experts had extracted and search the data for items of interest.

PRODUCING ELECTRONICALLY STORED INFORMATION

Although there are different trade-offs and considerations for privilege review, a sensible approach is to have the expert, in many cases the requester's expert under a protocol and confidentiality agreement, extract and search through the respondents data and produce items of interest to the respondent for privilege review. Allowing the requester's expert to perform the searches removes a lot of the mystery about what was considered, the techniques that were employed and whether they were proper and sufficient. This approach also will likely result in fewer documents being subjected to privilege review as long as the protocols incorporate deduplication of the population. As a result, it is less likely that mistakes would be made regarding inadvertent disclosures and the need for utilizing any claw back agreements.

interrogatory,

Another tools that can help the requesting party to understand the respondent's population of ESI and to develop the most appropriate means for extracting the data is the use of an interrogatory question to identify all of the systems used to manage digital evidence by the respondent. The answer to this question can help identify the various types of system being used to manage ESI and facilitate the research necessary to develop an efficient plan of extraction, analysis and production. The following is a suggested interrogatory question.

PRODUCING ELECTRONICALLY STORED INFORMATION

For each type of computer software, including but not limited to operating systems, networking systems, database management systems, backup systems, archival systems and application software, used to create, manage, interpret, manipulate, backup or archive any documents or electronic data that either was used or is being used to support this action identify the name of the software, version number, manufacturer or author, the specific piece of computer hardware used and the configuration of that system including serial number, owner/user, current location, processor, memory, storage, operating system and network system, if applicable.

Inspection

Rule 34 has been modified to allow a requesting party to inspect ESI. Specifically Rule 34(a) states,

“Any party may serve on any other party a request to produce and permit the party making the request, or someone acting on the requester’s behalf, to inspect, to copy, test or sample any designated documents or electronically stored information . . . “

PRODUCING ELECTRONICALLY STORED INFORMATION

While historically the inspection was likely directed at examining content, in the age of digital evidence, the focus of the inspection could be to examine the structure and storage systems of the respondents ESI management system. For example if data contained in databases is requested, the inspection could be used to examine the database structures and the types of data maintained in those structure in order to narrow the breadth of the production request both in terms of the various tables and other objects that could reside within the database as well as a means to filter the database contents to only those records having relevance to the case.

Conclusion

In conclusion the rules have been modified to remove disputes about a requesting party's entitlement to digital evidence and to the wealth of information that it contains. In addition, the rule changes recognize that users of ESI have disparate systems and configurations.

Consequently, careful planning is required to evaluate the respondents holdings and determine the best production plan considering the issues in the case and the objectives of the parties.

In planning their discovery, requesters need to be vigilant and proactive during the planning process. Requesters should not rely on the respondents to accurately recognize which of their ESI is reasonably accessible or not reasonably accessible. Requesters that are not willing to be

PRODUCING ELECTRONICALLY STORED INFORMATION

vigilant or proactive are likely to find themselves without the data they need or paying a higher price to obtain it.

Finally, requesters should realize that ESI is simply another arrow in the quiver. Digital evidence is available in, metaphorically, all shapes and sizes. The practitioner's challenge is to understand the burdens of its case and to properly match its sources of data with the objectives of its case.

1. *Federal Rules of Civil Procedure*, Rule 34(a)(1), “. . . and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.” The 1970 Advisory Committee Notes explained:

The inclusive description of “documents” is revised to accord changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent’s devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data.

2. *Bills v Kennecott Corp.*, 108 F.R.D. 459, 461 (D. Utah 1985), “It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the rules. . .” *See also, U.S. v Croft*, 750 F.2d 1354 (C.A.Wis. 1984), “It is well settled that computer compilations may constitute business records for purposes of Fed.R.Evid 803(6) and may be admitted at trial if a proper foundation is established.” *See also, U.S. v Scholle*, 553 F.2d 1109, (8th Cir. 1977), “Even where the procedure and motive for keeping business records provide a check on their trustworthiness (United States v. Fendley, [522 F.2d 181, (5th Cir. 1975)], the complex nature of computer storage calls for a more comprehensive foundation. Assuming properly functioning equipment is used, there must be not only a showing that the requirements of the Business Record Act have been satisfied, but in addition the original source of the computer program must be delineated, and the procedures for input control including tests used to assure accuracy and reliability must be presented. (Citing *U.S. v Russo*, 480 F.2d 1228 (6th Cir. 1973))”

PRODUCING ELECTRONICALLY STORED INFORMATION

3. *Rowe Entertainment, Inc. v The William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002)
4. *Murphy Oil, USA v Fluor Daniel, Inc.*, 2002 WL 246439 (E.D.La.), No 99-3564, 52 Fed.R.Serv.3d 168
5. *Residential Funding Corp. v DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002)
6. *Metropolitan Opera Association, Inc. v Local 100, Hotel Employees & Restaurant Employees International*, 212 F.R.D. 178 (S.D.N.Y. 2003)
7. *Zubulake v UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003)
8. Beckman, Joseph P., “*Virtual Discovery Costing Real Cash, Who Pays to Search E-Mail Archives?*”, Litigation News, July 2002, Vol. 27, No 5, American Bar Association, p 9
9. Rule 26(b)(2)(B), A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.”
10. Rule 26(b)(2)(C), “The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determined that (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some othersource that is more convenient, less burdensome, or less expensive, (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.”
11. Principle 6, Sedona Principles, “Responding parties are best situated to evaluate the procedures, methodologies and technologies appropriate for preserving and producing their own electronic data.”
12. Comments to Rule 26(b)(2), “The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.”
13. *Zubulake v UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003), “Of these, the first three categories [active on-line data, near-line data, offline storage/archives] are typically identified as accessible, and the latter two [backup tapes, erased fragmented or damaged data] as inaccessible.
14. Comments to Rule 26(b)(2), “A party may have a large amount of information on sources or in forms that may be responsive to discovery requests, but would require recovery, restoration, or translation before it could be located, retrieved, reviewed, or produced. At the same time, more easily accessed sources—whether computer-based, paper or human—may yield all the information that is reasonably useful for the action. Lawyers sophisticated in these problems are developing a two-tier practice in which they first sort through the information that can be provided from easily accessed sources and then determine whether it is necessary to search the difficult-to-access sources.”

PRODUCING ELECTRONICALLY STORED INFORMATION

15. Rule 26(f), “. . . [C]onfer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for disclosures required by Rule 26(a)(1), to discuss any issues related to preserving discoverable information . . .”

16. *Adams v. Dan River Mills, Inc.*, 54 F.R.D. 220, WD Va., (1972), “Because of the accuracy and inexpensiveness of producing the requested documents in the case at bar, this court sees no reason why defendant should not be required to produce the computer cards or tapes and the W-2 print-outs to the plaintiffs.” See also, *United States v. Davy*, 543 F.2d 996, (1976), “We also recognize that if the subject matter of requested records is not otherwise relevant, convenience will make it so. . . Here, inspection of the requested tapes could reasonably be expected to do so, and would incidentally insure greater accuracy and a substantial saving in auditing time by enabling the IRS, through use of the taxpayer’s own record medium, to trace transactions from the original documents to the tax return.” See also, *National Union Electric Corporation v Matsushita Electronic Industrial Co., Ltd.*, 494 F.Supp. 1257, ED Pa., (1980), “It may well be that Judge Charles E. Clark and the framers of the Federal Rules of Civil Procedure could not foresee the computer age. However, we know we live in an era when much of the data which our society desires to retain is stored in computer discs. . . . To interpret the Federal Rules which, after all, are to be construed to ‘secure the just, speedy, and inexpensive determination of every action.’ F.R. Civ. P. 1, in a manner which would preclude the production of material such as is requested here, would eventually defeat their purpose.” (emphasis in original) See also *In re Air Crash Disaster at Detroit Metropolitan Airport on August 16, 1987*, 130 F.R.D. 634 (ED Mich 1989), “By producing the computer-readable nine-track tape, MDC can reduce the unnecessary costs and delays that would accrue if Northwest were required to manually load the program and accompanying data.”

17. *Williams, et al. v Sprint/United Management Company*, 230 F.R.D. 640, 62 Fed.R.Serv.3d 1052, 96 Fair Empl.Prac.Cas. (BNA) 1775, “When party is ordered to disclose electronic documents as they are maintained in ordinary course of business, i.e. as “active file” or in “native format,” producing party should produce electronic documents with their metadata intact, unless that party timely objects to production of metadata, parties agree that metadata should not be produced, or producing party requests protective order.”