

ARTICLE FOR BRIEFCASE

**DISCOVERY IN THE DIGITAL AGE: THE E-DISCOVERY
AMENDMENTS TO THE FEDERAL RULES**

By Eric S. Eissenstat

*“The line it is drawn
The curse it is cast
The slow one now
Will later be fast
As the present now
Will later be past
The order is
Rapidly fadin’.
And the first one now
Will later be last
For the times they are a-changin’.”¹*

Years ago, the digital age was the stuff of science fiction. Consider the views of the following “experts”: “I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won’t last out the year”² ... “I think there is a world market for maybe five computers”³ ... and “There is no reason anyone would want a computer in their home.”⁴ Truly, the times are a-changin’.

Technological advances have dramatically impacted the way we communicate, work and live — for good and bad. Cell phones and voice-over internet protocol (VOIP) are rapidly replacing telephones. Information is now gathered from the internet instead of books and newspapers. Human interaction is being replaced by text messaging and e-mails. Gadgets such as iPods and GPS systems are the norm. And as the times change, the rules for electronic discovery must change also.

For the past ten years, experts from the bench, Bar and academia have been analyzing possible changes to the Federal Rules of Civil Procedure regarding electronic discovery. In 1999, the Committee’s mission included “mechanisms for providing full disclosure in a context where potential access to information is virtually unlimited and in which full discovery could involve burdens far beyond anything justified by the interests of the parties to the litigation.”⁵ A full-blown analysis of possible changes took place in 2000, amendments were proposed in 2004, and three public hearings were held in 2005 involving over 74 witnesses and 180 written comments. The consensus: discovery of electronically stored information (“ESI”) has important differences from information recorded on paper and these differences are causing problems that amendments to the Rules can address. By the time you read this article, the e-discovery amendments will have taken effect on December 1, 2006. The new amendments are designed to address issues surrounding

discovery of the vast amount of data available from a wide variety of sources. The following is a brief overview of the Amendments and their possible impact.

I. The Pros and Cons of Electronic Discovery (or *“A computer lets you make more mistakes faster than any invention in human history, with the possible exception of handguns and tequila.”*⁶)

Electronic discovery is a fact of life presenting both opportunities and problems. Corporate America has embraced the digital age to a point where nearly all critical business records are stored electronically. Recent studies show that 92% of new information is stored on magnetic media, primarily hard disks⁷ and over 70% of those documents are never printed or put into hard copy.⁸ Employees now exchange over 3 billion e-mails every day. So the question becomes: how to discover this data.

Many experts suggest that the exchange of computer data — as opposed to paper — reduces costs and delay. The cost of photocopying and transport can be reduced dramatically or limited altogether. The time involved in reviewing and organizing evidence can be reduced by use of key words, sorting, grouping and other tools. The use of mathematical model software, such as Topic Review, can analyze the associations among words and documents and then group the data into themes. Such technology can be used to identify key people, terms, dates, prioritize and assign folders, manage work flow and test theories. The cost of using litigation support systems is reduced dramatically if the documents are in electronic form from the start. Electronic discovery leads logically to electronic evidence. It stands to reason that many of the media conversion costs associated with electronic courtroom presentations may be reduced or eliminated if documents are in electronic form from the start.

There are substantive advantages as well to electronic evidence. Evidence that would have been impossible or extremely difficult to obtain now routinely is part of our truth-seeking process. Drafts of documents that may have been lost or destroyed in the conventional paper-based world are now retrievable. Nearly all of the modern panoply of computer/media communications ranging from e-mail messages to digital telephony to virtual conferences are recorded and saved as digital “documents.” Vast amounts of data that would have been impossible to collect and manipulate in the conventional paper-based world can be assembled, transmitted, manipulated and analyzed by computers.

However, the vast amount of data available also creates problems. In the paper discovery process, document sources are, for most intents and purposes, physically stable. Conversely, information stored in electronic form is easily changed, overwritten or obliterated through the routine use of computers. The simple act of booting a computer, opening a file, adding new data on a hard disk, or running a routine maintenance system on a network can alter or destroy existing data without the user’s knowledge. Satellite litigation has spawned over preservation issues which one could not imagine in the days where 8-tracks were the hot technology and students, like this author, took computer classes using mag-cards. Data location and the costs associated with production can be overwhelming and, frankly, outrageous. In our new digital age, employees have desktop computers

plus disks or other removable data storage media, laptop computers, home computers, handheld personal organizers, portable music devices, etc. — all containing potentially relevant data. Businesses have network servers connecting and storing data from many PCs plus backup and archival data storage. Offsite data storage facilities, internet service providers and other third parties also hold data subject to discovery. Relevant documents stored according to computer logic — as opposed to “business record logic” — can be difficult to locate and untangle from irrelevant and privileged documents. Electronic mail does not have a coherent filing system because e-mail systems are seldom designed for file management and retrieval. Relevant business-related e-mail messages will be found side-by-side with irrelevant and often very private/personal e-mail messages. The existence of data on backup tapes or disks provide special problems concerning retrieval and access. In the end, one might conclude that as a result of electronic discovery, “we are nowhere and it’s now.”⁹

II. The New ESI Rules (or “Computers make it easier to do a lot of things, but most of the things they make it easier to do don’t need to be done.”¹⁰)

The new Federal Amendments establish a new term — “electronically stored information” or ESI. ESI is “any type of information that can be stored electronically.”¹¹ ESI was defined broadly to be dynamic. It includes not only the electronic information available today but also that which will exist in the future. Certain fundamental truths appear clear as a result of the new Amendments. First, ESI is not only discoverable, it’s on equal footing with the discovery of paper documents. Second, clients and lawyers must come to grips with the preservation and production of ESI. Third, lawyers must understand how to request, review, produce and respond to ESI. And last, but not least, judges are provided a variety of mechanisms to remedy e-discovery abuse.

III. The Meet & Confer Amendments (or “The secret to getting ahead is getting started.”¹²)

Get ready. Amendments to Rules 16 and 26 and Form 35 require parties and lawyers to deal with electronic discovery at the start of a case. For example, parties must now (a) make voluntary disclosures of the categories and locations of all ESI that may be used to support claims or defenses; and (b) confer prior to scheduling conferences on issues relating to the (i) preservation of discoverable information; (ii) the disclosure or discovery of ESI (including the form or forms in which it should be produced; (iii) issues relating to claims or privilege or protection as trial preparation material, including procedures on the assertion of such claims after production; and (iv) whether to ask the court to incorporate their agreement in the scheduling/case management orders.¹³

Of course, the obligations to preserve and disclose presupposes the notion that one can promptly locate, identify, review and analyze the ESI — skills that few of us possess but now must all obtain. The Rule 26(f) discovery conference must now involve discussions on the form of producing ESI, which is a distinct and recurring problem due to the fact that it exists and may be produced in many different forms. Preservation must be on the agenda because ESI is dynamic and

easily changed. Privilege issues should be addressed now, rather than later, as the Rules allow parties to agree on a procedure for asserting privilege after inadvertent production, in recognition that the volume and forms in which ESI is stored make privilege review and determination increasingly difficult, burdensome and expensive. The Amendments to Rules 16 and 26 are also intended to encourage agreements on protocols relating to privilege claims to attempt to facilitate discovery that is faster and less costly. Ultimately, we must now learn much more about our clients, including who to contact to get information about ESI, its location, form, backups, legacy data and retention practices. We will need to understand our client's technology or find someone who does.

IV. I Can't Find It (or "*If you don't know where you're going, any road will take you there.*"¹⁴)

In order to comply with the new Amendments, litigants and their lawyers must not only know their own systems but have a discovery plan. This is because the Amendment to Fed. R. Civ. P. 26(b)(2)(B) states that a party need not provide discovery of ESI from sources that the party identifies as not reasonably accessible because of undue burden or cost.¹⁵

In order to take advantage of this Amendment, a party must identify the sources of potentially responsive information not searched or provided due to the cost and burdens of accessing that information. The responding or disclosing party bears the burden to show that the information is not reasonably accessible. The opposing party can then ask the court to order production for "good cause." Courts will have discretion to require discovery upon a determination that "good cause" outweighs the burden considering the limitation of Rule 26(b)(2)(C), and the court may impose appropriate terms and conditions on the production.

Amended Rule 26(b) requires that information identified as not "reasonably accessible" must be difficult to access by the providing party for all purposes, and not just litigation purposes. Further, it appears clear that a party that makes information difficult to access because it may be discovered in litigation is subject to sanctions. Courts will likely expect litigants to tell them precisely why ESI is difficult to access or unduly expensive. Conversely, they should also expect lawyers to tell them what it is they are seeking, why they need it, and to be creative in proposing test cases, sampling filters and the like at the outset. The parties should also be expected to tell the court who should pay for gathering and producing such information and why.

The relationship between the Amendment to Rule 26(b) and preservation issues are specifically addressed in the Committee Notes. They note that the Rule is not intended to undermine or reduce common law or statutory preservation obligations. In other words, parties may still be obligated to preserve data on a source that is identified as not "accessible" as a party's preservation duties arise from independent sources. Further, while parties may have a common law duty to preserve documents (and now ESI) that are potentially discoverable in foreseeable litigation, *see, e.g., Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 434 (W.D. Pa. 2004), the parties may still seek, and courts may issue, "preservation orders." *See, e.g., Pueblo of Laguna v. United States*, 60 Fed. Cl. 133 (Mar. 19, 2004). If a preservation order is sought and/or entered, it is important to craft it to be specific and clear and address topics such as the scope of the data subject to the order, what databases, software, computers or other devices are required to be

preserved, and how and what may be destroyed. And any preservation order should also address that all persistent question: who pays? Rule 26(f) contemplates that among the issues to be discussed at the outset of the case is the preservation of relevant data, recognizing that the parties' discussion should aim towards specific provisions, balancing the need to preserve relevant evidence with the need to continue routine activities critical to ongoing businesses.

V. It Is Too Expensive — You Pay For It

(or "*Money, so they say
Is the root of all evil today.
But . . . its no surprise that they're
Giving none away.*"¹⁶)

At the heart of any discussion about electronic discovery is who foots the bill. Prior to the advent of electronic data, courts were not generally receptive to claims by poor record keeping organizations that their inefficiencies made discovery too expensive and time-consuming. *See Baine v. General Motors Corp.*, 141 F.R.D. 328, 331 (M.D. Ala. 1991). While cost-shifting in electronic discovery may deter shotgun and abusive discovery, it may also preclude meritorious claims against corporations with poorly managed records. Cost-shifting may also have the ironic effect of slowing down and making discovery more expensive — expressly contrary to the express purpose of the Federal Rules to "secure the just, speedy and inexpensive determination of every action."¹⁷

Under current jurisprudence, the presumption is that the responding party must bear the expense of complying with discovery requests. A party may seek exercise of the court's discretion to grant an order protecting it from undue burden or expense, including conditioning discovery on the requesting party's payment of the costs. In the electronic discovery world, courts have taken several approaches on this issue. *Compare Zubulake v. UBS Warburg, L.L.C.*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake IV*") with *Thompson v. U.S. Dept. of Housing & Urban Dev.*, 219 F.R.D. 93, 98 (D. Md. 2003) and *McPeck v. Ashcroft*, 212 F.R.D. 33 (D.D.C. 2003). The ABA Civil Discovery Standards identify sixteen (16) factors courts may consider in deciding whether to allow a requesting party's discovery and how to allocate the cost of that discovery. *See American Bar Association, Amendments to Civil Discovery Standard* § 8(29). Under the Amendments, the balancing of the equities on this important issue will continue to be left for the courts to sort out.

VI. I Did Not Mean to Give This to You (or

*"Give it back.
You need to give it back.*"¹⁸)

Amendments to Rule 26(b)(5)(B) now give a party the right to demand the return of information that was produced inadvertently without having asserted privilege or trial preparation protection. This has led to terms, such as "quick peak" or "clawback agreements," which are designed to allow a party to produce information without a prior privilege review, with the requesting party reviewing the information for responsiveness before a privilege review is conducted. Clawback agreements often have a third party technology expert performing an initial responsiveness review, which has the added benefit for the producing party of preventing the requesting party from seeing possibly inadvertently produced privileged or sensitive documents.

The procedure to get your documents back is as follows. First, if a party learns it inadvertently produced privileged or work product information in discovery, that party may notify the receiving party and state the basis of the claim. Next, the receiving party must then return, sequester or destroy the information and may not disclose it to third parties until the privilege claim is resolved. Further, if already disclosed, the receiving party must then take reasonable steps to retrieve the information. Finally, either the producing party or the receiving party can promptly present the materials to the court, under seal, for determination regarding the privilege.

To retrieve privileged information and maintain the privilege, notification must be timely. One cannot delay notification of inadvertently produced privileged information once it has been learned that it was inadvertently disclosed. Further, the Rule only addresses the procedure for asserting privilege claims after production. It does not change the substantive law of privilege. Waiver issues will likely continue to hinge on the effort to protect the material and whether the notification was truly timely. Privilege log issues also remain unanswered. While the ESI must be logged just like other privileged materials, the Rule does not address how detailed the privilege description must be. Must it be on an item-by-item basis or can it be described more broadly in light of the vast amount of volume of data at issue? Many of these issues can be addressed in the court's Rule 16 scheduling order, which allows a party to request preservation and clawback agreements be included in the scheduling order.

VI. Meta-what?! (or “Can’t you see this a land of confusion?”¹⁹)

All electronic files including websites, e-mail messages, spreadsheets and word-processing documents contain metadata. “Meta” simply means about, or behind, or beyond while “data” equals things or information. Metadata generally contains information describing the history, tracking or management of an electronic document, and can include its authors, editors and dates of creation, modification and printing. Metadata can be revealed in various ways including using the “properties” and “track changes” functions or reading the document with commercially available software to learn about the metadata. As a result, documents which may appear to be worthless because they are unreadable when printed in hard copy can be very valuable when one goes behind and sees the metadata behind such document.

While the Committee Notes to Rule 26(f) discuss metadata, the issues regarding discoverability of metadata remain unclear. Will the courts make clear and understandable the distinctions between data and metadata? Is the removal of metadata during litigation (by producing only hard copies or converting a native file to a “.tif” or “.pdf” image) subject to a claim of spoliation? Is metadata relevant to discovery requests? What should a party do to preserve metadata at the time of the request (which typically changes through routine operations)? Can a party set its computer systems to routinely delete metadata that might be discovered in subsequent litigation? As discussed below, since the Amendment to Rule 34 allows a party to produce information in a form in which it is ordinarily maintained or in electronically searchable form and since it is only required to produce “such information in one form,” may a party convert data to a format that would eliminate metadata? Answers will only come from litigation about these issues.

VIII. What Do I Want? (or “*Programming today is a race between software engineers striving to build bigger and better idiot-proof programs and the universe trying to produce bigger and better idiots. So far, the universe is winning.*”²⁰)

Amendments to Fed. R. Civ. P. 34 coin the term “ESI” and permit requesting parties to specify the form in which ESI is to be produced. Conversely, the Rule also permits the responding party to object to that form and produce it in the form in which it is ordinarily maintained, if no form is requested. The Amendment is designed to prevent massive “dumps” of disorganized documents. It also makes clear that absent court order, one need produce ESI in only one form. The Committee Notes to amended Rule 34 state that the Rule was intended to be broad and flexible enough to embrace future developments in technology.

Litigants often request that “documents” be “produced.” Responses generally provide paper documents and electronic information typically copied to a compact disk in its native format or converted to .tif or .pdf images. While the Amendment to Rule 34(b) sets forth a multi-step process concerning the production format of ESI, unresolved issues remain. For example, what does one do regarding the production of data that requires the use of proprietary hardware or software, passwords, encryption keys or other proprietary data? It is likely that courts will require producing parties to provide some access to such tools, if needed, to obtain the information if the party’s proprietary information can be protected by a protective order, including an attorneys’ eyes only protective order. If the necessary software or hardware is owned by a third party, a producing party may assert a contractual right to preclude disclosure. Again, courts will likely craft orders requiring the disclosure of such information if necessary to access data designed to protect the proprietary nature of the software or data.

An issue which has become more and more frequent is to what extent direct access to computers and other electronic devices is permitted. Cases prior to the Amendments have held that Rule 34 does not grant unrestricted direct access to database compilations. *See In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003); *Diepenhorst v. City of Bancreek*, 2006 LEXIS 48551 (W.D. Mich. 2006); and *Advante Int’l v. Mintel Learning*, 2006 WL 1806151 (N.D. Cal. June 29, 2006). The Committee Notes to amended Rule 34 state that the Amendment is not meant to create routine right of direct access to a party’s electronic information, although such access may be justified in some circumstances. The Notes further mandate that the courts should guard against undue intrusiveness.

IX. Third Party Subpoenas (or “*I’ve got no time for you right now, don’t bother me.*”²¹)

Often third parties who have no interest in spending the time or effort to get involved in someone else’s dispute are invited to provide information. The Amendments to Fed. R. Civ. P. 45(a), (c) and (d) provide for the discovery of ESI in the possession of non-parties and provide protection for non-parties against the burdens of discovery. It conforms provisions for subpoenas

to changes in the other discovery rules relating to ESI. Of course, claims of confidentiality, burdensomeness, costs and inaccessibility of a non-party will fall with more favor on the court's ears than those of a party.

X. I Lost The Data (or *“Imagine if every Thursday your shoes exploded if you tied them the usual way. This happens to us all the time with computers and nobody thinks of complaining.”*²²)

Fed. R. Civ. P. 37(f) contains significant amendments regarding lost ESI. The Rule has been amended to provide that a court may not impose sanctions for failing to provide ESI that has been lost or becomes inaccessible as a result of routine, good faith operation of an electronic information system. The Rule attempts to address a necessary feature of computer systems, i.e., the recycling, overwriting and alteration of ESI from normal use. Thus, even when litigation is anticipated, it can be hard to interrupt or suspend routine computer operations to preserve or isolate data without creating problems.

Amended Rule 37 provides protection against sanctions if ESI has been lost or destroyed due to routine operation if the operation is in good faith. The Committee Notes recognize that many organizations routinely recycle backup tapes every few weeks and that placing a hold on such recycling is very expensive. Further, regular purging of e-mails and electronic communications may be necessary to prevent buildup of data that can overwhelm computer systems. Also, some systems are functional only if they continually revise information they manage.

“Routine operation of an electronic information system” is the various ways in which “such systems are generally designed, programmed, and implemented to meet the party’s technical and business needs.”²³ A party cannot destroy specific information or exploit routine operations to preclude discovery. It is also clear that in some circumstances, good faith may require a party to suspend or modify routine operations if it is subject to a preservation obligation. The preservation obligation depends on the substantive law of each jurisdiction and is not altered by the Amendment. Thus, substantive law or a court order may require a litigation hold.

Prior to the Amendment, case law regarding spoliation exploded. Spoliation cases focus on the sources of the duty of the preservation; when the duty arose; the degree of intention or culpability required for liabilities; and the remedies of the breach of the duty. Lawyers should now be aware of are the client’s system and document retention policies, how data is created, managed, destroyed and preserved within a client’s system; what impact a “litigation hold” may have on the system and the expense of such hold; what may be done to preserve possible responsive data; and how to maintain good record keeping on preservation and disclosure and production efforts. Cases addressing these preservation and spoliation issues are wide and varied and include, among others, *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, 2005 WL 679071 (Fla. Cir. Ct., 15th Cir. Mar. 1, 2005); *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 434 (W.D. Pa. 2004); *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133 (Mar. 19, 2004).

XI. What Should I Do Now? (or “*To err is human — and to blame it on a computer is even more so.*”²⁴)

Practicing law in the digital age is hard work. Whether the new Rules will make it easier or harder remains unclear. What is clear is that those who are aware, prepared and proactive under the new Rules will likely fair better than those who aren't. To best assure success, lawyers must (a) work with their clients as a team to ensure compliance with the Rules and substantive law, and (b) make use of the vast untapped sources of information available from opponents. And if you find yourself frustrated regarding all of this electronic discovery, remember that “the most overlooked advantage of owning a computer is that if they foul up, there's no law against whacking them around a little bit.”²⁵

ESE/cw:383044.3

-
1. Bob Dylan, *The Times They Are A-Changin'* (1964).
 2. The Editor in Charge of Business Books for Prentice Hall (1957).
 3. Thomas Lawson, Chairman of IBM (1943).
 4. Ken Olson, President, Chairman & Founder of Digital Equipment Corp. (1977).
 5. 1999 Report by Judge Niemeyer to the Standing Committee recommending adoption of the 2000 amendments.
 6. Mitch Ratcliffe, *Technology Review* (1992).
 7. Peter Lyman and Hal R. Varian, *How Much Information 2003?*, at <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/>.
 8. Julian Gillespie, Patrick Fair, Adrian Lawrence, David Vaile, *Coping when everything is digital: Digital Documents and Issues in Document Retention*, Baker & McKenzie Cyberspace Law and Policy Centre, Sydney, 2004.
 9. Bright Eyes (2005).
 10. Andy Rooney.

- 11.Fed. R. Civ. P. 34.
- 12.Sally Burger.
- 13.Fed. R. Civ. P. 16(b), 26(f), 26(f)(3) and 26(f)(4), and Form 35.
- 14.Lewis Carroll, *Alice in Wonderland*.
- 15.Fed. R. Civ. P. 26(b)(2)(B).
- 16.Pink Floyd, *Money* (1973).
- 17.Fed. R. Civ. P. 1.
- 18.Hoobastank, *Give It Back* (2001).
- 19.Disturbed, *Land of Confusion* (2005).
- 20.Rich Cook.
- 21.The Beatles, *Don't Bother Me* (1963).
- 22.Jeff Raskin interviewed in [Dr. Dobb's Journal](#).
- 23.Advisory Committee Note to Amendment to Fed. R. Civ. P. 37(f).
- 24.Robert Orben.
- 25.Eric Porterfield.