



04-CV-036  
Request to Testify  
1/28 Dallas

RECEIVED  
12/9/04

LITIGATION

ANALYSIS

MANAGEMENT

December 8, 2004

Peter G. McCabe  
Secretary  
Committee on Rules of Practice and Procedure  
Administrative Office of the United States Courts  
Thurgood Marshall Federal Judicial Building  
Washington, D.C. 20544

Re: Testimony on Proposed Amendments to the Federal Rules of Civil Procedure  
Regarding Electronic Discovery

Dear Mr. McCabe:

This correspondence via email will serve as my formal request to testify on proposed e-discovery rules in Dallas, Texas on January 28, 2005. I appreciate the opportunity to be part of this process.

If you require additional information from me regarding the above, please contact me via e-mail at [Anne@AKershaw.com](mailto:Anne@AKershaw.com).

Very truly yours,

Anne Kershaw, Esq.

**AK** A. Kershaw PC  
Attorneys & Consultants

RECEIVED  
1/21/05

LITIGATION

ANALYSIS

MANAGEMENT

**04-CV-036**  
*Written Statement  
for 1/28 Dallas hearing  
will arrive before 2/15.*

January 19, 2005

Peter G. McCabe  
Committee on Rules of Practice and Procedure  
Administrative Office of the United States Courts  
Thurgood Marshall Federal Judicial Building  
Washington, D.C. 20544

Re: Dallas Hearings: Proposed E-Discovery FRCP Amendments

Dear Mr. McCabe:

I am scheduled to testify at the hearings in Dallas on January 28, 2005. This letter responds to your request for a written submission in advance of the hearing.

In early December it became clear that it would be beneficial to the rules amendment process to provide to the Advisory Committee specific information regarding the issues imposed by electronic discovery on large data producers. Attempting to respond to that realization, we embarked on a campaign to recruit large data producers to testify and submit comments on these issues. Our campaign was confronted with serious confidentiality concerns, primarily because these large data producers are also large targets in litigation, and expressed concern that public testimony as to electronic discovery issues would quickly become issues in litigation.

In an effort to compromise concerns, we are endeavoring to solicit this critical information from large data producers by way of a small, informal, confidential survey which we are conducting primarily through telephone interviews. Our hope is to provide the Advisory Committee through my testimony the preliminary results of this survey. We would then follow up with a full written report before the February 15, 2005 close of the comment period. Regrettably, we simply are not far along enough in our survey to provide a full submission at this time. Respectfully, I request that the Advisory Committee nonetheless allow me to proceed with my testimony of January 28, 2005.

Respectfully submitted, \_\_\_\_\_

*Anne Kershaw*

Anne Kershaw, Esq.

**Via Electronic Mail**

February 15, 2005

Peter G. McCabe, Secretary  
Committee on Rules of Practice and Procedure  
Judicial Conference of the United States  
Thurgood Marshall Federal Judiciary Building  
Washington, D.C. 20544

Re: Proposed Amendments to the Federal Rules of Civil Procedure  
Concerning Discovery of Electronically Stored Information

To The Civil Rules Advisory Committee:

The laudable goal of the Civil Rules Advisory Committee to address the complex demands of electronic discovery is clearly a challenging one, and I thank the Committee for its hard work in bringing the proposed amendments to public comment. Marshall McLuhan's pronouncement that "the medium is the message"<sup>1</sup> could not ring more true than it does in the context of complex litigation in the 21<sup>st</sup> century. As the Committee clearly recognizes, there is most certainly a difference, both in form and content, from pre-electronic discovery days and there are new and serious challenges to current and future litigants. As promised in my testimony at the hearings in Dallas, I herein provide my written submission, detailing the results of my firm's ongoing research concerning the challenges faced by large data producers in responding to electronic discovery demands.

I am a former litigator and trial lawyer, as well as the founder and principal of A. Kershaw PC, Attorneys & Consultants, a litigation management consulting firm based in New York. I have been involved with discovery management in large document cases for more than fifteen years, and have personally witnessed the growing challenges that organizations face when potential litigation is a part of their daily landscape. My firm works primarily with in-house counsel, and I have watched corporate concern rapidly giving way to alarm as the very fine line between sensible business behavior and responsible preservation practices becomes invisible. Much of our work this past year has focused on designing and implementing information preservation and response plans. Absent guidelines, designing such processes is challenging, and the efficacies of the results are uncertain. Yet solid information preservation and litigation response plans provide the best insurance against the loss of potentially relevant data, so clearly the effort is in everyone's best interests.

<sup>1</sup> Marshall McLuhan, *Understanding Media: The Extensions of Man* (Cambridge: The MIT Press, 1994), page 61

While responding to a client request for information about the Proposed Rule Amendments, we learned that the Advisory Committee is interested in obtaining specific information concerning the challenges presented with electronic discovery. With the support of a client, we embarked on an effort to encourage knowledgeable participants to testify and submit comments on these issues. However, as I mentioned at Dallas, *most in-house counsel are unwilling to publicly discuss their issues out of concern that undue advantage will be taken of their comments.* This in itself is a strong indication of a very large problem.

To address these concerns, we determined that a confidential survey, conducted primarily through telephone interviews, would allow us to provide blinded and composite information of use to the Committee. What follows is a summary of our findings. We are pleased to report that these findings, including anecdotal information elicited in the conversations, firmly dispel the notion that organizations will use the proposed amendments to hide or delete information, or that the amendments will inhibit or discourage the use of technologies that will allow more effective discovery. The findings also support the following conclusions:

1. The amount of available data is huge and a presumptive limitation on production of inaccessible information is unlikely to result in the loss of relevant information;
2. Blanket preservation orders are costly and crippling and should be discouraged in the Committee Notes;
3. Considerations of cost, business use and interruption, burden, technological feasibility, and the fundamental fairness of the conclusion should be included in the assessment of inaccessible information;
4. Electronic data should be produced in a "reasonably usable form," and to require otherwise would undermine meaningful Rule 26 conferences;
5. Discovery requests continue to be overly broad. Narrow, targeted requests should be encouraged in the Committee Notes; and
6. A mere negligence standard for the imposition of sanctions is unfair and unwarranted, given the vast amount of information available for production and the complexities of information systems.

### Survey Methodology

Questionnaires were distributed to the Chief Litigation Counsel of 40 companies that, from my firm's experience, had demonstrated an interest in electronic discovery issues. We followed up with telephone calls and the majority of responses were personally obtained through telephone conversations. The questionnaire dealt with four general categories:

1. Information technology environment (hardware);
2. Data volume;

3. Document retention policies; and
4. Experience with e-discovery.

The respondents were encouraged to solicit information from appropriate departments in their companies (i.e., information technology, legal, records management, etc.) As of this submission, 12 companies (30%) have provided the information provided below.

### **Survey Analysis: Quantitative Information**

#### **Systems Generally**

The responding companies are, for the most part, large organizations, with employees numbering from 30,000 to 260,000. One respondent has just 1200 employees, yet has a number of cases in federal court comparable to one of the larger organizations. The respondents include manufacturing, pharmaceuticals, banks, petroleum, and computer products companies, and for the most part, have offices in both the US and worldwide. All respondents have in excess of 100 cases pending in Federal Court — one currently has 2,400 cases, another has more than 3,000.

Consistent with the testimony the Advisory Committee has already heard, the information management systems of large companies are large and complex. These companies were certainly no exception.<sup>2</sup> In nearly every company, office employees utilize a desktop computer with an associated network access to email and the internet as well as telephone and voicemail (which may or may not be digital). Highly “wired” individuals may have both a desktop and laptop computer, a PDA (Personal Digital Assistant, such as a Palm Pilot), a cell phone, pager, and one or more removable storage devices such as a thumb or zip drive or iPod. All of these devices can store data and most can create it—some without the company’s knowledge or oversight—and most communicate with other devices.

The data volume created and stored in the electronic environment described above is— not surprisingly—staggering. Total data on hand by these companies is estimated to exceed 800

---

<sup>2</sup> Companies reported having:

- a. 3,000 - 7,000 servers worldwide;
- b. 65,000 – 90,000 desktops;
- c. 30,000 – 60,000 laptops;
- d. As many as 5,000 distinct databases;
- e. 1,000 to 2,000 networks, including local area networks;
- f. 20,000 Blackberries or PDA’s owned or used by employees;

Thumb drives (small removable data storage devices that plug directly into a computer) for one company number in the 100,000 range.

terabytes<sup>3</sup> with 5.2 million emails exchanged daily. One company estimated that they are now in pedabyte territory.<sup>4</sup>

Interestingly, email volume did not correlate necessarily to the size of the organization – one company with 177,000 employees reported 2.8 million emails per day, whereas a company with 30,000 employees said its traffic is 2.5 million per day. These numbers are consistent with Microsoft's reporting of large companies generating between 60 and 90 emails million per month. However, the range of this estimate may be affected by differing approaches to measure email traffic, as well as how emails are counted: if one email is sent to 100 employees, does that count as one email or 100? All companies noted that email volume is increasing exponentially with no deterrent to future growth in sight.

All companies surveyed reported the use of sophisticated and formidable back-up systems and procedures, with different combinations of procedures for business back-up as distinct from those used to allow disaster recovery. The longest recycle time reported was 30 days, the shortest only 2 weeks. The costs to restore are difficult to calculate, since there are different methods of restoration. One company with 3,000 servers in the United States (due to a blanket preservation order) reported that it takes between 1 and 2 days to restore one server. In other words, it would take between 8 and 16 years to restore them one by one. Another company reported that it has 6,000 servers. Whole sale restoration would, of course, also require hardware to house the restored data (more servers) and if tapes are deteriorated, or need reverse engineering, yet more time and money is involved. If information is needed for production, there is also the time and cost to cull, de-duplicate and review for such production.

All of this speaks to the need for practical and effective limitations as to what is initially discoverable and further, given the vast amount of active data available, supports an observation that it is highly unlikely that relevant information would be lost as a result of such limitations. The presumptive limitation on production of inaccessible information as proposed by the Committee is clearly necessary to accomplish this end.

### **E-Discovery Generally**

Turning now to electronic discovery, the respondents reported a noticeable and critical increase in e-discovery and a correspondingly and dramatic resulting increase in litigation costs. In one company, the increase was more than 300 percent in the last five years. Electronic discovery is increasingly the most expensive part of corporate litigation. In the companies we interviewed, virtually all cases now include some element of e-discovery. Approximately one-third of the respondents acknowledged that they had prematurely settled cases because of e-discovery cost issues. Twenty percent indicated that electronic discovery is the most expensive part of their litigation.

---

<sup>3</sup> 1 terabyte is equivalent to 50 million pages—20,000 boxes of documents. As a point of reference, if digitized, the 19 million books and other print collections in the Library of Congress would contain about 10 terabytes of information. See Mary Mack, Esq. and Matt Deniston, *A Process of Illumination: The Practical Guide to Electronic Discovery* (Discovery Center of Excellence, 2004) p.64

<sup>4</sup> A pedabyte is 1,000 terabytes.

Companies surveyed were experienced with blanket pre-discovery preservation orders. Two companies characterized them as routine. One respondent cited a preservation order issued by a federal judge, *sua sponte*, in a case with very broad claims, which stated:

*"Each party shall preserve all documents and other records containing information potentially relevant to the subject matter of this litigation."*

The organization subject to this blanket order promptly issued a litigation hold but was nonetheless seriously sanctioned for employee error, even though none of the errors were willful, negligent, or even had a substantively significant impact. This company has since suspended system email deletions and now has 56 servers housing all of its Microsoft Exchange email, 40 of which have been classified by Microsoft as "un-maintainable," meaning they cannot be reliably backed-up. The same company estimates that compliance with this preservation order has cost more than \$10 million since 2002. That company is not alone—another company reported that it spends \$2 million per month in tape and people costs alone to comply with a blanket hold. This company also has had to suspend system email deletions.

E-discovery generally, and broad preservation orders in particular, are costly issues for these companies, and blanket preservation orders can be crippling. The responses I received support the need for commentary in the Committee Notes to the effect that broad preservation orders are discouraged and should rarely be employed absent agreement of the parties.

This seems consistent with the testimony I heard at Dallas and in Washington. We heard repeatedly throughout the hearings that under the current rules, litigants rarely need to resort to back-up tapes for discoverable information given the volume of information produced from accessible data.

### **Data Accessibility – What is Inaccessible and Can it be Identified**

Survey respondents were asked to identify the types of data they would consider to be inaccessible from a list of eight possible items:

- Information found in active email accounts;
- Deleted email fragments found on hard drives;
- Email found on back-up tapes;
- Information created in formats or by software no longer in active use;
- Dynamic information resulting from the use of databases, websites, information on shared drives; or
- "Other" as described.

There was general agreement that active, unfiltered email is accessible, but beyond that consensus it was clear that opinions varied. Some believed that websites were inaccessible for these purposes, but most said "it depends" when discussing data created with retired programs.

Some said that email on back-up tapes is accessible, others disagreed. One respondent told me that she gave her IT department our list, and no one could agree.

This suggests, and I feel this is critical, that the distinction between accessible and inaccessible sources of data should *not* be solely based on mere technical concepts or definitions of inaccessibility. Given that a group of individuals who routinely handle electronic discovery could not agree on what is "inaccessible," a broader and more functional definition is warranted. Considerations of cost, business use and interruption, burden, technological feasibility, and of course, the fundamental fairness of the conclusion should be included in the assessment.

Companies clearly know and can identify what they currently *use* in the day-to-day conduct of their business. Throughout the years of upgrades, advancements, and acquisitions, however, the companies surveyed generally have not maintained comprehensive records of what is retired and where it is located. Because businesses are not primarily organized or operated in order to provide document retrieval for litigation, they generally do not maintain lists or indices of all of potential, retired data sources. Survey participants said that they are concerned that old data stores exist about which they have no information and cannot identify. One company told us about 72 CD's that showed up the night before a case went to the jury—and this company has a very rigorous collection process. Another told us of old back-up tapes discovered 3 years into a case. Electronic documents can be stored literally anywhere and individuals can create, save and delete information without anyone—often even themselves—knowing about it.

This is not to imply that businesses are not concerned about information that may be on back-up tapes, in storage, on floppies, in drawers. Two respondents are presently undertaking separate projects to identify all possible sources of accessible and inaccessible information, as per their definition of "inaccessible." At one company, this endeavor includes a dedicated team of 20 staff employees, plus outside consultants. The success of these projects remains uncertain and the data landscape is ever-changing. Another company told me to check back with them... in 2012.

To the extent the proposed amendments seek to remove the "gotchas" from the discovery process, the identification requirement in proposed Rule 26(b)(2) appears to be inconsistent with that goal. There is no such requirement in the paper world, and there should not be one in the electronic world. Relevant information is being located and produced, without a requirement for the identification of inaccessible electronic data or paper. As has always been the case, everyone in the litigation will continually look for, and inquire at depositions, sources of additional relevant information and seek to produce it as soon as it is discovered.

### **Form of Production**

Survey participants expressed concern about the proposed form of production language in Rule 34(a). With just one exception, respondents indicated there are difficulties in producing information "as ordinarily maintained." They also told me that the "electronically searchable form" option is too limiting in light of the many reasonable methods of production now available, especially when there is likely to be more such acceptable methods forthcoming.



As an example, one respondent indicated he would like to produce his company documents on a website, creating a single document database for all parties—and the court—that would track document usage through depositions, exhibit lists and rulings at trial. His proposal has been resisted by adversaries and passed over by judges. Selling ideas such as this, he noted, would become even more difficult if the rule specifies a default form of production. Thus, “reasonably usable” might be a better phrase to use in Rule 34(a).

Another problem—apart from our survey and speaking from my personal litigation experience—is that a default form of production in the rule could undermine meaningful Rule 26 conferences. The goal on the other side of the table, more often than not, is to make production more difficult and more expensive—not easier and less costly. Thus, if a litigant seeks agreement to produce in a way that is easier than that set forth in the rule, his or her adversary likely will insist that production be made in the form set forth in the rule. A general requirement that the production be reasonably usable may allow for more productive meet and confer conversations.

#### **Survey Results: Anecdotal Information**

The survey also generated some interesting anecdotal information, all of which dispels the notion that organizations will avoid technologies that allow for more comprehensive discovery, or that the amendments will be used to hide or delete information:

1. First, improved technologies are being used to better ensure the preservation of information. For current employees, organizations are quickly able to identify individuals subject to litigation holds, isolate and suspend email accounts, distribute notices, and follow-up. Litigation holds on documents and email are increasingly efficient and comprehensive as a result.
2. In addition, companies subject to a high volume of repetitive litigation are beginning to recognize the merits of a proactive approach to document and email collection—that is, collecting material generally sought in lawsuits on an ongoing basis, as it is created. For example, one company uses a pop-up box that requires the author of an email to identify if the email is subject to a litigation hold. Another idea, if there is a document management program, is to check a box on the document information sheet. In either case, a copy of the document is saved to a separate server for collection.
3. In the spirit of “an ounce of prevention,” one respondent indicated that his company is working to link its litigation response plan to its consumer response center and human resources department so as to detect potential problems and suspend documents at the earliest possible opportunity. He maintains that this approach will save money and facilitate collection.
4. Another observation is that electronic document storage, and its ever-expanding capacity, appears to aid and abet the human instinct to hoard or save everything. One respondent told me that 90% of the material created on her company’s systems was never looked at again—not even for deletion. As a matter of personal experience, most of us never return to old

work product and delete it. Although organizations have document retention programs that allow for the destruction of documents after the expiration of their retention period, rarely are steps taken to later find and delete these documents. In addition, there are thousands of databases, all of which are specifically intended to save information. This information is not cleared out by the back-up system. It is all available for production.

A major theme of the comments we received is that discovery requests are simply too broad. Respondents felt that perhaps the most effective way to bring the electronic discovery process to manageable proportions is to require specific, targeted requests. Search technologies are effective in finding the one or few things among many. The burdens pile up when large data producers are asked to produce huge collections – all marketing or research documents, for example. Accordingly, the use of narrow, targeted discovery requests should be encouraged in the notes to the rules.

### **A Word About Sanctions**

In my experience, a solid document management and retention program and a litigation response plan are key to effective preservation and collection and should be encouraged by the Committee. For example, the Committee Notes should mention that the existence of a demonstrably enforced document management and retention program will weigh against the imposition of sanctions, even when potentially relevant information was lost despite such a program.

The electronic discovery world is producing 100 fold the amount of information that was available in the paper world. Considering this glut of information, no one can ensure that *every* potentially relevant document from *every* data source has been adequately maintained in case of litigation, just as no one can ensure this in the paper world. There are many, many ways that someone can inadvertently lose information in this complex e-discovery world, and the knowledge gaps between the user, the technologist, the programmer, and the developer, are vast. These knowledge gaps do not exist in the paper world.

This naturally leads to the question as to whether a standard of care requiring reasonable conduct in preserving and producing can or should be deemed to be breached by mere negligent conduct in the electronic discovery world. I think not. Given the complexities and other issues discussed above, I believe the imposition of sanctions should require proof of a culpability standard of willfulness or recklessness, and particularly so for “case killer” sanctions such as adverse inference rulings or the striking of a pleading.

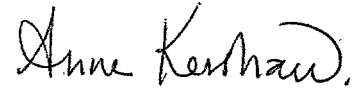
### **Conclusion**

Coping with electronic discovery has become an uphill battle for large data producers who are constantly in the throes of litigation or anticipated litigation. They are drowning in electronic documents, fearing that disposal or deletion will be interpreted as malicious or negligent document destruction—a fear that has been supported by the “sanctionable” behavior of others. The people that I spoke with told me in effect that they feel that litigation, in some ways, owns the company. The enactment of the amendments proposed will be a meaningful

Peter G. McCabe, Secretary  
February 15, 2005  
Page 9

step towards resolving these problems and bringing the discovery arena back to the mandate of  
FRCP 1.

Very truly yours,



---

Anne Kershaw