Federal Bar Association

Federal Litigation Section

ALAN BLAKLEY
CHAIR
Blakley & Velk
523 South Orange Street
Missoula, MT 59801
(406) 543-0909
(406) 543-0990 (fax)
alan@blakley net

GEOFFREY ANGEL
CFO/TREASURER
Angel Law Firm
125 West Mendenhall
Bozeman, MT 59715
(406) 586-1926
(406) 585-7654 (fax)
christianangel@hotmail com

JOSEPH DATTILO
MEMBERSHIP COORDINATOR
Brouse McDowell
1001 Lakeside Avenue, Suite 1600
Cleveland, OH 44114-1151
(216) 830-6833
(216) 830-6807 (fax)
jdattilo@brouse com

N. PATRICK FLANAGAN
IMMEDIATE PAST CHAIR
Hale Lane Peek Dennison
Howard Anderson & Pearl
P O Box 3237
100 West Liberty Street, 10th Floor
Reno, NV 89505
(775) 327-3000
(775) 786-6179 (fax)
pflanagan@halelane com

WINSTON HAYTHE
PUBLICATION MANAGER
Office of Criminal Enforcement,
Forensics & Training
U S EPA (MC-2235 A)
1200 Pennsylvania Avenue, NW
Washington, D C 20460
(202) 564-6057
(202) 564-0075 (fax)
haythe winston@epa gov

KEN LAWSON
CHAPTER LIAISON
Office of the U S Attorney
400 North Tampa Street, Suite 3200
Tampa, FL 33602
(813) 274-6000
(813) 274-6178 (fax)
ken lawson@usdoj gov

KELLY MCCLOSKEY
LIAISON WITH FEDERAL JUDICIAL CENTER & ADMINISTRATIVE OFFICE OF THE U.S. COURTS
O'Rourke, McCloskey & Moody
The Chicago Title & Trust Tower
161 North Clark Street, Suite 2230
Chicago, IL 60601
(312) 849-2020
(312) 849-2021 (fax)
KMcclos823@aol com

JOHN F. (JOE) PERRY
***SIDEBAR* NEWSLETTER EDITOR/SECRETARY**
Springer Bush & Perry, PC
2 Gateway Center, 15th Floor
Pittsburgh, PA 15222
(412) 281-4900
(412) 261-1645 (fax)
joepa@springerlaw com

RECEIVED
12/13/02
02-ED-006

December 5, 2002

Peter McCabe
Secretary
Committee on Rules of Practice and Procedure
Federal Judiciary Building
Washington, D.C. 20544

Dear Mr. McCabe:

In September, we received an inquiry from Richard L. Marcus on behalf of the Discovery Subcommittee Advisory Committee on Civil Rules regarding discovery of electronic materials. That inquiry asked us if we would provide helpful advice to the subcommittee about some of the issues surrounding electronic discovery. We have prepared the enclosed comment for your use. As you will note, this comment reflects the thoughts of many members of the Federal Litigation Section of the Federal Bar Association, including myself. However, it does not constitute a public position of the Federal Bar Association nor of its Federal Litigation Section.

Thank you for including us in the process. If you have any questions, you may call me at 406-543-0909. Mr. Jacobs can be reached at 305-350-5127 and Mr. Stone at 408-453-9200.

Sincerely,
FEDERAL LITIGATION SECTION

Alan F. Blakley
Chair

AFB/sem
Enclosure

cc: Richard Marcus via fax

Comment of the Federal Litigation Section, Federal Bar Association[1] in Response to the Inquiry from the Discovery Subcommittee Advisory Committee on Civil Rules Regarding Discovery of Electronic Materials

December 9, 2002

Alan F. Blakley
Blakley Velk, Missoula, MT

Kevin Jacobs
Homer, Bonner & Delgado, P.A., Miami, FL

Clark Stone
Skjerven Morrill LLP, San Jose, CA

Summary

Electronic discovery creates unique issues for both Courts and parties in civil litigation today. The ever-increasing use of computers and electronic communication systems will result in electronic discovery's being conducted, to some degree, in most types of civil litigation in the future. However, explicit changes to the Federal Rules of Civil Procedure addressing specific electronic discovery issues may be unworkable at this time in this rapidly evolving area. Rather, the Federal Rules should require District Court local rules to address certain detailed electronic discovery issues, including document retention, recovery of deleted materials, privilege concerns, and post-litigation document return and destruction. Additionally, education of the bench and bar should be encouraged to promote a better understanding of electronic document and communications systems and the corresponding electronic discovery issues.

Background

Use of electronic mail, or email, is pervasive in most businesses today. Similarly, businesses create, circulate, and store a significant amount of their business documents, data, and related communications in electronic format.[2] Given the widespread use of email and electronic documents, even small businesses can generate hundreds to thousands of emails and other electronic documents daily. The now routine and ubiquitous use of email, computers, and other business equipment that store electronic information (e.g., fax machines that maintain lists of faxes sent and received) in both business and personal matters will only increase in the near

[1] This comment is the product of the work of several members of the Federal Litigation Section of the Federal Bar Association, including its chair, Mr. Blakley. The comment generally reflects the views of its members. It is not inconsistent with any existing position of the Association. It does not, however, constitute a public position of the Federal Bar Association nor of its Federal Litigation Section and should not be considered the public position of the Association.

[2] In a recent ruling on an electronic discovery issue, one District Court cited a University of California study finding, "93% of all information during 1999 was generated in digital form, on computers." In re Bristol-Myers Squibb Securities Litig., 205 F.R.D. 437, 440 at n.2 (D.N.J. 2002).

future. Accordingly, courts, attorneys, and clients should expect that electronic document discovery issues will become far more prevalent in almost all types of civil litigation.

Many believe that the creation and retention of electronic documents facilitates discovery of electronic materials with less cost and burden to the parties. To some degree, this is true. The ease and relatively low cost of archiving and keeping electronic documents can make a far larger volume of material more readily available to litigants in many cases, versus the previous practice of central retention of archived hard copy documents. The ability to rapidly search large amounts of emails and electronic documents using "keywords" can, in many instances, uncover relevant and responsive documents and communications with minimal time, effort, and expense.

On the other hand, the widespread use of electronic documents and emails has created, in many cases, an almost overwhelming amount of information subject to discovery. Much electronic information is retained or archived for disaster recovery, due to the relative ease of backing up and the associated low cost of electronic storage. This type of archiving does not always make collection and searching of this information easier. Rather, it often results in large amounts of uncatalogued and disorganized material which must be recreated, sometimes with long outdated software, then searched for relevance and privilege prior to production. Additionally, worldwide computer networks have replaced the central hard copy document depository, with the result being that dozens to thousands of individuals may be the custodians or recipients of discoverable materials. The ever-changing technology of computer software, networks, and data processing systems can, in many situations, make archived data and documents unrecoverable within the short period of time allowed in civil discovery due to technical obsolescence. Finally, the ability to recover "deleted" material from computer hard drives imposes additional burdens and costs on parties who want to recover intentionally or inadvertently deleted electronic materials.

The comments to the 1970 Amendment to Fed. R. Civ. P. 34 make clear that electronic data and information is included in the definition of "documents," thus requiring the parties to address electronic discovery issues in their Fed. R. Civ. P. 26(a) Initial Disclosures. Further, the Case Management Conference requirements of Rule 16 also include provisions that apply to discovery of electronic materials, without specific reference to them. Finally, the Judicial Conference's Civil Litigation Manual (2001 ed.) encourages Courts to address aspects of computer-based discovery early in the case, including data preservation, location and volume of data, recovery of "deleted" data, and cost allocation. Given these requirements, it would seem that electronic discovery issues would be addressed by the parties and the Court in due course in each case, with the parties including these issues in their Initial Disclosures and meet-and-confer, and with the Court being aware of and raising these issues in the course of case management. Some Federal Courts, through local rules, have begun to require parties to consider and to discuss some of these issues. See, e.g., D. Wyo. L.R. 26.1.

Recently published cases concerning electronic discovery indicate that parties and the Federal Courts are dealing with an increasing number of electronic discovery related issues. These issues include the high cost of electronic document production, the burdensome nature of searching and producing electronic materials, intentional and unintentional electronic spoliation, and technical issues concerning recovery of deleted and archived electronic materials. See, e.g., In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437 (D.N.J. 2002) (cost sharing issues for

electronic document production of over 3 million pages of material and the disastrous result of failing to confer); Playboy Enter. Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) (order requiring court-appointed computer expert to create "mirror image" of defendant's hard drive to attempt recovery of deleted emails); Rowe Entm't, Inc. v. The Wm. Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002) (plaintiff required to bear cost of multiple defendants' production of email discovery); Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 U.S. Dist. LEXIS 3196 (E.D. La. Feb. 19, 2002) (plaintiff to bear the estimated high cost of email production from backup tapes; however, defendant to bear the cost of privilege review and email "culling"); Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002) (plaintiff's failure to timely produce emails from backup tapes due to purported "technical problems" used by defendant as basis to request adverse inference jury instruction at trial). Given the ever-increasing use of email and electronic document systems for personal and business use, it seems clear that electronic discovery issues will arise on an increasing basis in future litigation.

Some Courts have already promulgated specific rules pertaining to electronic discovery and document management. For example, California Civil Procedure Code section 2017(e) specifically addresses the use of technology in conducting discovery and maintaining documents in "complex" cases. California's electronic discovery rules are premised on "encouraging cost-effective and efficient discovery technology," and require that the Court ordering such discovery make express findings that the proposed electronic methods are efficient and cost-effective, do not require undue expenditures of time or money, and do not impose an undue economic burden on any party.

The Need For Rules Specifically Addressing Electronic Discovery

Federal Rule of Civil Procedure 16(b) Should Be Amended to Identify Electronic Discovery as a Topic to Be Covered Specifically by Local Rules.

Given the rapidly evolving technology that enables electronic discovery, it is probably premature at this point in time to amend the Federal Rules of Civil Procedure to govern electronic discovery in any great detail. Instead, Rule 16(b) should be amended to identify electronic discovery as a topic to be covered specifically by local rules. This should spur Federal Courts to promulgate detailed local rules governing electronic discovery. The expectation is that, over time, the technology enabling electronic discovery will stabilize and the better procedures for conducting electronic discovery and dealing with electronic discovery disputes will be recognized as such. At that point in time, the Rules may be amended to ensure some uniformity and predictability across the Federal Court system regarding a party's obligations to facilitate electronic discovery, without the risk that evolving technology will quickly render an amendment to the Rules unworkable or inadequate.

Electronic Document Retention and Disclosure of Computer Systems

Local Rules Must Address the Problem of the Preservation of Electronic Documents and Provide Clear Guidance to Parties Trying to Comply with the Duty to Preserve Relevant Documents and the Technological Difficulties in Doing So.

One of the problems that occurs in an electronic document environment is that the universe of potentially responsive documents changes with each keystroke. For example, if a party is a sizeable company, there will likely be countless electronic documents that exist on the day the lawsuit is filed but which may no longer exist when the parties meet for the Rule 16 scheduling conference, the first mandated opportunity for the parties to discuss electronic discovery issues. These electronic documents that no longer exist may include emails deleted automatically, documents that resided in the unallocated space of a hard drive and were overwritten by new data, and documents that existed on backup tapes that were recycled. This continuous loss of documents is very difficult to arrest, particularly when it involves corporate parties that have local area networks (LANs), wide area networks (WANs), voicemail systems, hundreds or thousands of personal computers, laptops, digital assistants, and myriad software programs.

Today, a party must attempt to balance the duty to preserve evidence in electronic form (and avoid charges of spoliation of evidence) with the tremendous costs and technological difficulties associated with doing so. Most companies do not design their document retention policies with the view that every electronic scrap of paper is saved indefinitely on the chance that it may later be deemed relevant to a lawsuit. Many companies simply create backup tapes of data stored on servers and maintain those backup tapes for a fixed and relatively short period of time, but policies vary widely. A company's document retention policy may even vary from office to office, and individual users may configure their own computers in ways that result in greater or lesser document retention. The duty to preserve relevant documents becomes complicated and even overwhelming in this electronic environment. The alleged failure to comply with this challenging duty has resulted in a proliferation of charges of spoliation of evidence, many of which are more opportunistic then meritorious.

In view of this, it is clear that there needs to be some certainty with regard to a party's obligation to prevent the loss of relevant electronic documents and to deviate from its normal document retention practices during litigation. As stated above, this certainty should be provided, for the time being, by detailed local rules. These are some suggestions for and comments about the content of those rules as they relate to the obligations to retain and preserve documents:

- *Local rules might place the burden on the requesting party to seek detailed information about the computer systems and retention policies of the responding party.*

It can be an enormous task to obtain detailed information about a client's computer systems and retention policies. Such information should include:[3]

[3] See Kenneth J. Winters, Computer-Based Discovery in Federal Court Litigation, 2000 Fed. Cts. L. Rev. 2, at App. A (October 2002).

- Most likely locations of records relevant to the subject matter of the action
- Number, types, and locations of computers currently in use
- Number, types, and locations of computers no longer in use, but relevant to the facts of the case
- Operating systems and application software currently in use
- Operating systems and application software no longer in use, but relevant to the facts of the case
- Names and versions of network operating systems currently in use
- Names and versions of network operating systems no longer in use, but relevant to the facts of the case
- File-naming and location-saving conventions
- Disk or tape labeling conventions
- Backup and archival disk, tape, or server inventories or schedules
- Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time
- Electronic records management policies and procedures
- Corporate policies regarding employee use of company computers and data
- Identity of current and former personnel who had access to network administration, backup, archiving, or other systems operations during any relevant time
- Name of individual in charge of computer systems
- Other issues (e.g., impending upgrades) that may impact electronic discovery

This disclosure may not be necessary in all cases. Therefore, the obligation to provide such information should probably be triggered by a request from a party, and not be automatic.

- *Alternatively, local rules might provide that any party who maintains substantial electronic documents, including email, must disclose its computer systems and retention policies within a certain period after retaining counsel.*

The thought here is that parties should expect that electronic discovery will be a fact in any litigation where substantial electronic documents exist, though some thought would have to be given to what "substantial" should mean. In this event, a party should not await a request for a disclosure of the information that will enable the other party to determine whether it will need to seek an agreement or an order to ensure adequate preservation of electronic documents.

- *Local rules might provide that a party who discloses its computer systems and retention policies should be immune from spoliation charges to the extent it complies with it own policies and its effort to preserve relevant documents are not otherwise unreasonable.*

Once a responding party has provided information about its computer systems and retention policies, whether pursuant to a specific request or a local rule requirement, it should be able to rely on continued compliance with its policies without the fear that the requesting party will later claim the policies led to the spoliation of electronic evidence, assuming that the policies are not facially unreasonable (e.g., daily purging of emails). This would constitute a "safe harbor" for the responding party.

- *Local rules should provide that a requesting party who wants the responding party to deviate from its retention policies must demonstrate need and may need to pay costs.*

To the extent a requesting party wants the responding party to deviate from its retention policies, the requesting party should demonstrate need and may have to be willing to pay the costs incurred by the responding party to change its policies. The parties should endeavor to come to an agreement on these issues. Where there is disagreement, this issue will need to be submitted to the Court. To assist the Court in resolving the disagreement, a local rule may provide a cost-shifting test similar to that used in Rowe Entertainment, Inc. v. The William Morris Agency, 205 F.R.D. 421 (S.D.N.Y. 2001).[4]

Hard Drive Examinations and the Problem of "Deleted" Documents

Local Rules Should Address the Issue of When a Requesting Party Should be Entitled to Forensically Examine another Party's Computers.

A thorough search for computer-based information responsive to a discovery request would include a search for information contained in the unallocated space of a computer hard drive. Unallocated or free space is the portion of a hard drive that does not contain active files. It is where ostensibly deleted documents may be found. The imposition of any requirement that a responding party search unallocated space as a matter of course is likely to be resisted because of the expense involved. Few parties will have ability to search unallocated space with in-house assets. consequently, to search unallocated space on a single hard drive, a typical party will have to hire a computer forensic expert, who can search the hard drive using special forensic software. Aside from the costs involved,[5] there is no assurance that any information will be found or that information found will be complete enough to constitute admissible evidence. In part, this is because the search process usually requires the use of keywords. A forensic expert uses keywords to search unallocated space for "hits." These hits may include parts of a document responsive to a discovery request or they may not. Determining what keywords will be used is likely to be a contested issue. A requesting party would ordinarily seek a large number of keywords to increase the probability that responsive documents would be located. A responding party, on the other hand, would naturally be inclined to limit the number of keywords. In either case, the search will probably result in a substantial number of hits that have nothing to do with the issues in the case and may not result in the discovery of any relevant information.

This becomes more probable in view of the fact that the deleted information remaining in unallocated space often comprises only part of a document. This is explained by the fact that documents are usually stored in non-contiguous "clusters" on a hard drive. Clusters are small blocks of memory on a hard drive. Depending on the size of a document compared with the size

---

[4] The Court in Rowe examined eight factors: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of the information from other sources; (4) the purpose for which the responding party maintains the data; (5) the relative benefit to the parties of obtaining the data; (6) the total cost associated with the production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party. 205 F.R.D. at 429.

[5] Practitioners report that a cost of $2,000 to $5,000 per hard drive examination is typical. As technology evolves, this cost may be reduced substantially.

of the clusters on the hard drive, the document may be stored in multiple clusters. These clusters are not always adjacent to one another. While the document is saved or is being viewed, the computer knows which clusters comprise the document. After the document is deleted, however, the computer no longer knows how to find the specific clusters that comprise a document, and the clusters are subject to being overwritten with new data. The overwriting process is random, so that some clusters among those that formerly comprised a single document may be overwritten and some may not. A search of unallocated space may reveal individual clusters, which may contain portions of a document, but the search may not (and often does not) reveal entire documents, much less entire documents that are useful. Consequently, the utility of a forensic search of unallocated space on a computer hard drive is quite limited in most cases.

In other cases, though, a forensic examination of a hard drive and unallocated space may lead to the discovery of an important missing document (even a "smoking gun" document) or reveal critical information regarding when a document was created, modified, or viewed (i.e., so-called metadata) or whether it is genuine. For these legitimate reasons, the prospect of forensically examining the opposing party's hard drive and unallocated space can be very attractive.

It is not surprising that requests to inspect computers pursuant to Rule 34 appear to be increasing. The invasiveness of hard drive examinations and the opportunity to eliminate the other party's ability to determine unilaterally which documents are relevant can lead to abuse, however. Recognizing this, some Courts have denied requests to inspect another party's computers where no justification was found. See, e.g., Lawyers Title Insur. Corp. v. U.S. Fid. & Guar. Co., 122 F.R.D. 567, 570 (N.D. Cal. 1988) ("At minimum, counsel who seek access to opponents' information management systems should be required to show that conventional discovery methods have failed to produce information they need to litigate their case."); Stallings-Daniel v. The N. Trust Co., 2002 WL 385566 *1 (N.D. Ill. Mar. 12, 2002) ("Nothing in the documents produced justifies an intrusive and wholly speculative electronic investigation into defendant's e-mail files."); Van Westrienen v. Americontinental Collection Corp., 189 F.R.D. 440, 441 (D. Or. 1999) ("Plaintiffs are not entitled to unbridled access [sic] defendants' computer system or to canvass all of defendants' debtor files. Plaintiffs should pursue other less burdensome alternatives ...."). Consistent with these decisions, local rules should include some specific standards for determining when a computer inspection is warranted, which party should bear the costs, and whether the forensic examination should be performed by a Court-appointed expert.

Issues Pertaining to Electronic Production and Management of Documents

Local Rules Should Direct Parties to Explore the Possibility of Producing Electronic Documents in Electronic Form, Bypassing the Need to Produce Hard Copies.

Parties in a case involving emails and electronic documents should also address the issue of electronic document production and management early in the case. In addition to emails, many businesses also maintain other documents exclusively in electronic format—i.e., no hard copies of documents are maintained beyond those used for limited purposes. For example, companies with offices located in multiple worldwide locations can allow employees to access, edit, and comment on "workshare" type electronic documents via the company network and the Internet, with these edits and comments made available in real time to other offices and employees.

Additionally, most companies today maintain their detailed financial and accounting records in a format that makes printing of these documents almost impossible, unless steps are taken to gather and summarize this information into a less detailed (but more manageable) format.

The parties should explore the possibility of producing these electronic documents in electronic form, bypassing the need to print and produce hard copies of these documents. See, e.g., In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. at 437. Concerns over electronic "alteration" of source documents can be addressed by converting documents to unalterable electronic image files, such as PDF and TIFF format documents, prior to production. Steps must also be taken to electronically "Bates stamp" electronic documents for tracking purposes, and documents requiring confidentiality designation pursuant to protective orders or confidentiality agreements must also be properly marked prior to electronic production.

The parties must also address cost-sharing issues, as costs of electronic document production can be high, especially if recovery of "archived" or deleted documents is involved. If one or more parties anticipates requesting electronic documents that are not readily available to the producing party, this issue must be raised early in the litigation and agreement reached as to which party will bear the cost of production.

Privilege Issues Relating to Electronic Discovery

Local Rules Should Direct Parties to Address the Logistical Issues of Returning and/or Destroying Inadvertently Produced Privileged Electronic Material, Including the Need to Retrieve Multiple and Archived Electronic Copies.

Review of electronic documents for privileged communication should, in many cases, be easier and less costly that comparable hard copy document review. Large amounts of documents can be electronically searched prior to production for keywords relating to privileged communications, including senders, recipients, and subject matter.

However, if inadvertently produced, electronic documents containing privileged information can be more difficult to return to the producing party, as copies can reside in multiple locations in electronic storage, backup tapes, and the like. Parties must address the logistical issues of returning and/or destroying inadvertently produced privileged electronic documents, including the need to retrieve multiple and archived copies.

Post-Litigation Electronic Document Issues

Local Rules Should Direct Parties to Consider Post-Litigation Return or Destruction of Electronic Discovery Materials, Which May Include the Existence of Multiple Electronic Copies of Documents, Emails, Pleadings, Court Papers, and Other Documents that Contain Confidential Information.

Electronic document discovery and production create unique issues concerning document disposition, return, and destruction at completion of litigation, particularly when the electronic documents contain confidential information or trade secrets. Currently, parties typically agree at

the conclusion of litigation either to return to the producing party or destroy all copies of documents containing sensitive information. While tangible hard copies make this a manageable task, electronic documents present some challenges. Electronic document productions can result in multiple electronic copies residing with a party's law firm on multiple mediums (e.g., individual hard drives, diskettes, laptops), at multiple offices, with numerous individual attorneys and experts, and with outside litigation support services such as trial demonstrative consultants. Copies also exist where this material has been backed up during the course of litigation while residing in a firm's network storage. Provisions pertaining to post-litigation document return or destruction must take into account the existence of multiple electronic copies of documents, emails, pleadings, court papers, and other documents that contain confidential information.

Education

While it does not involve a Federal Rule change, we strongly urge the subcommittee to include a recommendation in its report concerning education. Most attorneys and many judges do not have an adequate understanding of the field of electronic information and discovery. For instance, many of the problems encountered in Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002) could have been avoided had the parties provided the electronic information as electronic information and not focused on printing paper versions of emails. The Federal Bar Association's Federal Litigation Section has worked with the Federal Judicial Center to produce a program entitled *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence*. This and other programs help both judges and litigators gather a better understanding of issues in electronic discovery.

Conclusion

The Federal Rules of Civil Procedure should be amended to require the District Courts to include specific provisions in their local rules pertaining to electronic discovery issues in litigation. These provisions should address the parties' responsibilities concerning preservation of electronic evidence, the need to meet-and-confer early in the case on electronic discovery issues, recovery of deleted electronic materials, management of electronic document production, privilege issues, and post-litigation electronic document return or destruction. Additionally, programs should be developed to educate the Courts and attorneys on electronic document and communications systems and their corresponding electronic discovery issues.