04-CV-052
Request To Testify
1/28 Dallas

RECEIVED
12/15/04

"Sloan, Peter"
<psloan@Blackwellsanders.com>

12/14/2004 05:59 PM

To <Peter_McCabe@ao.uscourts.gov>

cc

Subject January 28, 2005 Civil Rules Hearing in Dallas, Texas

Mr. McCabe, I send you this e-mail to request an opportunity to testify at the January 28, 2005 Civil Rules Hearing in Dallas, Texas, regarding the proposed amendments to the Federal Rules of Civil Procedure that address digital evidence preservation and discovery .

I am a lawyer in private practice, a partner with the law firm Blackwell Sanders Peper Martin, LLP. My sole client practice is working with companies on their records retention scheduling, records management compliance, and legal hold protocols. As the digital evidence discovery case law has developed over the last several years, I have wrestled with the contradictions and unanswered questions that currently exist regarding the preservation duty and its application to digital media and information, whether accessible (active and archived data) or inaccessible (such as data in disaster recovery backup media).

I 'd like to testify because I find myself encountering the issues addressed by the proposed amendments on a daily basis in my practice.

If you need additional information from me at this point, please let me know. Thank you very much.

Peter B. Sloan
Blackwell Sanders Peper Martin LLP
2300 Main Street, Suite 1000
Kansas City, Missouri 64108
Phone: (816) 983-8150
Fax: (816) 983-8090
E-mail: psloan@blackwellsanders.com
www.blackwellsanders.com

LAW FIRM

BLACKWELL SANDERS PEPER MARTIN
LLP

4801 MAIN STREET SUITE 1000 KANSAS CITY, MO 64112
P.O. BOX 419777 KANSAS CITY, MO 64141-6777
TEL: (816) 983-8000 FAX: (816) 983-8080
WEBSITE: www.blackwellsanders.com

04-CV-052
Testimony

Peter B. Sloan
Partner
DIRECT: (816) 983-8150

DIRECT FAX: (816) 983-9150
E-MAIL: psloan@blackwellsanders.com

February 15, 2005

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

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

Dear Mr. McCabe:

Thank you for the opportunity to provide testimony to the Civil Rules Advisory Committee at its January 28th hearing in Dallas, Texas. In this letter I provide my written comments, which contain six points on proposed Rules 26(b)(2) and 37(f), including the Committee's alternative language for the Safe Harbor.

As I indicated to the Committee, I am a partner in the law firm of Blackwell Sanders Peper Martin LLP. My sole client law practice is to counsel companies on how best to manage their records. This involves records retention scheduling and records management compliance practices for paper and digital records in the ordinary course of business, and also legal hold protocols applied to satisfy a company's preservation duty in the face of pending or impending litigation.

I therefore work with records management professionals, IT professionals, and in-house counsel as they grapple with records management issues – and in particular, with how to compliantly manage digital records and information. In my experience, these professionals work diligently and in good faith to meet both legal requirements and business needs, which together define compliance in the records management field.

The sticking point for these professionals, and also for me when counseling them, is the frustrating exercise of identifying exactly what the company must do to meet the preservation duty regarding digital information. Specifically, once a company has instituted a legal hold and expended reasonable effort to locate, identify, and preserve active digital information that is "reasonably accessible," what if anything else needs to be done to satisfy the preservation duty?

For example:

- With thousands of employees who each send and receive scores of e-mails every day, the company has instituted a routine e-mail management system in which record-quality e-mail is moved out of the e-mail application and into records management. E-mail that is not of record-quality is then deleted, either manually by the individual employees or through an automatic deletion feature of the e-mail application. This routine process is necessary to manage the extraordinary volume of non-record e-mail that would otherwise accumulate. Once the company moves from the ordinary course of business to a legal hold, individual employees move e-mails subject to the legal hold to a destination outside of the e-mail application and the automatic delete function. Is that good enough, or must all automatic e-mail delete processes be turned off across the entire company to satisfy the preservation duty?

  As confirmed to the Committee through testimony and written comments, shutting down such routine processes can be logistically impracticable, prohibitively expensive, and an extraordinary burden. But the current Federal Rules and case law do not give adequate guidance on this point.

- In the ordinary course of business, the company runs a disaster recovery backup system for its e-mail network storage devices. It maintains the backup media for the minimum period of time needed for disaster recovery, which the IT professionals at the company have established as ten days. Once the company moves from the ordinary course of business to a legal hold, must the legal hold result in the stopping of backup media recycling? It is unclear at that early point just who the "key players" in the litigation will be, their e-mail is spread throughout the company, and therefore their e-mail is duplicated in numerous backup media. If the company has done a good faith, diligent, and reasonable job of preserving relevant e-mail on the active, "reasonably accessible" side of things, must it nevertheless also interrupt its routine rotation of disaster recovery backup media?

  As illustrated in testimony and written comments to the Committee, the suspension of routine disaster recovery rotations is highly problematic and expensive. But again, the current Federal Rules and case law provide inadequate guidance on how to proceed.

- The company, like many companies, finds itself in litigation with some regularity. If, for even a limited period of time, it goes beyond its good faith and customary legal hold practices and interrupts its routine rotation of disaster recovery backup media for even a subset of such media based upon a "key player" analysis, it encounters the "**serial preservation**" dilemma. Serial preservation problems commonly arise when digital information that is not reasonably accessible (such as backup media), is set aside in a particular lawsuit. The only reason the company retains this data is out of an abundance of caution to meet its initial, vaguely defined preservation duty at the outset of the lawsuit. Yet long before that preservation duty expires, or its parameters can be set under existing law, another lawsuit commences with its own preservation duty that arguably may cross the same backup data preserved in the first lawsuit. A third lawsuit follows the second, a fourth the third, and so on, with the result that the disaster recovery backup media are preserved in perpetuity – and with exponential growth in volume.

  Serial preservation creates an intractable problem for litigant companies, with no clarity offered by the current Federal Rules or case law.

Preservation conundrums such as the above are the most perplexing issues in this field, and current law simply does not provide adequate guidance, particularly for medium to large companies with operations in various United States jurisdictions.

I know there are limits to what the Federal Rules of Civil Procedure can properly address, and I acknowledge the reluctance of the Committee to comprehensively define the preservation duty, particularly as it is applied at or prior to the commencement of a lawsuit. But I respectfully suggest that the success of these amendments will be measured in large part by how much clarity they provide to the confoundingly uncertain state of the law on preservation.

With that background, I offer the following comments on the proposed amendments.

1. The Rule 26(b)(2) two-tiered approach, hinging upon whether the information is "reasonably accessible," is an excellent addition to the Rules.

Digital information simply does not behave like its paper analog. For example, it is physically impracticable to preserve and subsequently produce digital data being processed in electronic memory. The data simply never becomes static in a way that will allow preservation and production. Other forms of digital data would require extraordinary cost and effort to preserve and produce in every case, such as metadata, embedded data, data in disaster recovery backup media, fragments of data in slack space, and cached data. These latter types of data have

something else in common – while some are merely residual and others serve some purpose in the internal functioning of the computer system, none of this data is directly used in the ordinary course of business by the company's employees.

Thus, due to the peculiarities of how digital information is created, replicates, and spreads in a computer network, we have a class of data that is not reasonably accessible, which is not used or relied upon by the company's employees in the ordinary course of business, and which is both perplexing and prohibitively expensive to preserve and produce.

The two-tiered approach of the proposed Rule 26(b)(2) recognizes this reality. It also has a safety valve that allows a court in the rare case to make an exception and require preservation and production of such data when the circumstances warrant.

The Committee Note on this point, found in the first paragraph regarding 26(b)(2), contains a good description of some types of digital data that are not reasonably accessible. But the Note could provide even greater clarity with the addition of other categories of digital data commonly understood to be not reasonably accessible, such as "metadata, embedded data, cached data, and data fragments."

2. The Rule 26(b)(2) identification notion is reasonable, but the Rule and Note should clarify that this requirement does not call for the specificity of a privilege log.

It is understandable that there should be some way for a requesting party to learn that there are categories of data not being produced because they are not reasonably accessible. I have a concern, however, that the current language of proposed Rule 26(b)(2) could create a new and pernicious "identification" process, requiring an unnecessarily specific designation akin to a privilege log. It is unreasonably onerous to require litigants to locate and specifically identify digital data that by their very nature are not reasonably accessible.

One alternative would be to change the language of the Rule to read "a party need not provide discovery of electronically stored information that is not reasonably accessible if it objects on that basis," with a corresponding retailoring of the Note on that point.

Another alternative is to leave the proposed Rule's language the same, but to add language to the Note to clarify that "identification" does not require the specificity of a privilege log. For example, the pertinent sentence in the Note could be changed to read, "The degree of specificity the responding party must use in generally identifying such electronically stored information, or classes of such information, will vary with the circumstances of the case."

3. The proposed Rule 26(b)(2) does not, in and of itself, clearly resolve the preservation issue for data that is not "reasonably accessible."

A reading of proposed Rules 26(b)(2) and 37(f) reveals the care with which the Committee seeks to address and remedy the dilemma of the preservation duty for digital data that is not reasonably accessible. Under proposed Rule 26(b)(2), digital data that is not reasonably accessible is properly outside the scope of discovery, unless the particular circumstances of the case warrant a court order to the contrary. But the proposed Rule 26(b)(2) and its Note do not directly speak to preservation. It is instead the Rule 37(f) Safe Harbor that explicitly addresses the preservation of digital information that is not reasonably accessible, indicating that as a general rule such preservation is not required.

I address the proposed Safe Harbor rule below, but here I note the importance of these two proposed Rules acting in concert. If proposed Rule 26(b)(2) is adopted, but the Rule 37(f) Safe Harbor is not adopted, little clarity will have been accomplished. Rule 26(b)(2) will establish that disaster recovery backup media, which are not reasonably accessible, are outside the scope of discovery – unless such media are later put back into the scope of discovery by court order. But litigants must make preservation decisions at the outset of the litigation, and they will still face the same preservation dilemma and uncertainty they experience today. Many litigants out of an abundance of caution will unnecessarily interrupt routine processes and rotations, for fear that a judge could months or years later rule that the backup media or other data not reasonably accessible should nevertheless have been preserved and produced.

Thus, if the goal is to provide clarity for litigants who sincerely wish to be compliant and must discharge the preservation duty at the outset of litigation, the Rule 26(b)(2) two-tiered "reasonably accessible" mechanism must be buttressed with a Safe Harbor such as that proposed in Rule 37(f). Otherwise, litigants will simply not have the guidance they need at the outset of litigation to make reasonable, compliant decisions regarding legal holds and disaster recovery backup media.

4. Proposed Rule 26(b)(2) would be more successful in providing clarity and guidance to litigants if its Note explicitly dovetailed with the Safe Harbor of Rule 37(f).

As discussed above, proposed Rule 26(b)(2) provides that, in all but rare cases, data that is not reasonably accessible need not be produced. But the proposed Rule does not directly address preservation. The Rule would provide greater clarity for litigants if its Note stated that "electronically stored information that is not reasonably accessible ordinarily does not need to be preserved, unless the parties agree otherwise or the court orders preservation of that specific information."

5. The proposed Rule 37(f) Safe Harbor is a sound and necessary clarification of the law.

The reality of how digital information is managed in today's world simply requires that there be routine processes that result in the disposal of data. It is entirely proper in the ordinary course of business, for example, for a company's e-mail system to be configured so that record-quality e-mail is moved out of the e-mail application into a records management structure, and for an automated deletion process to dispose of the remaining e-mail, which is not of record quality, after a certain period of time or a certain account data volume is reached. Also, it is appropriate for disaster recovery data to be kept only as long as is necessary for its purpose – disaster recovery – and for the backup media holding the compressed disaster recovery data to be regularly recycled. These automatic processes in the routine operation of a company's computer information systems are critically important to manage the data and to avoid the unnecessary and unwarranted costs of accumulating extraordinary volumes of unneeded data.

If a litigant establishes and follows a reasonable legal hold process to satisfy its preservation duty and does not violate a court order that specifically requires preservation of particular digital information, it should not be sanctioned for the loss of data resulting from the routine operation of its computer information systems.

The current rules and law are not clear on this point. The result is confusion and frustration for litigants as they make preservation decisions at the outset of litigation. The proposed Rule 37(f) Safe Harbor will add some much needed clarity, and it should be adopted.

6. The "reasonable steps" Safe Harbor is preferable to the "intentionally or recklessly" alternative.

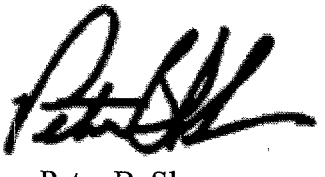
The Committee has offered two alternative Safe Harbor Rules. Each has its merits. On balance, however, and based on my experience in this field, I prefer the first alternative, which includes the requirement that "the party took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action." I favor this approach because, I respectfully suggest, a litigant <u>can</u> reasonably and appropriately make an intentional decision when executing a compliant legal hold process to <u>not</u> interrupt the routine operation of its computer information systems, such as its disaster recovery backup rotation. Instead, the litigant company will execute its legal hold by reasonably and diligently locating, securing, and preserving the relevant, reasonably accessible data on the active side of its network systems. This is an intentional decision that obviously may result in the loss of data in the backup media that continues to be recycled. Thus, even though the company's legal hold is a reasonable strategy that captures the relevant, active data that is reasonably accessible, this approach could fall outside the ambit of the second Safe Harbor alternative.

However, in this commonplace scenario, the litigant company has worked hard and done a good, reasonable job in executing its legal hold, and it should be entitled to the benefit of a Safe Harbor. Under the second alternative Rule 37(f) language, the company might forfeit its Safe Harbor protection because it made an intentional (yet reasonable) decision not to interrupt its routine backup rotation. Under the first alternative Safe Harbor, however, the issue is framed as it should be – did the litigant company take reasonable steps in its legal hold process regarding the data? If it did so, it should fall within the Safe Harbor.

The first alternative Safe Harbor will demand a focused debate on exactly what constitutes "reasonable steps to preserve" digital information, particularly digital information that is not reasonably accessible. Few judges (with the notable exception of some Committee members!) have been inclined thus far to directly address this issue in their opinions. This debate is overdue, and the first alternative Safe Harbor will require it to take place.

Mr. McCabe, thank you again for the opportunity to provide written comments regarding the proposed Civil Rules Amendments. The Committee has worked long and hard in this process, and their efforts are much appreciated.

Best regards,



Peter B. Sloan

PBS/mm