

RECEIVED  
11/24/04



adam.cohen@weil.com

11/24/2004 08:11 AM

To peter\_mccabe@ao.uscourts.gov

cc

Subject electronic discovery hearings

04-CV-045  
Request to Testify  
2/11 DC

Dear Mr. McCabe, please accept this as my request to testify at the hearings in Washington, D.C. I am a partner at Weil Gotshal & Manges LLP, a co-author of the treatise Electronic Discovery: Law and Practice, and the Chairman of the Committee on Electronic Discovery of the New York State Bar Association's Commercial and Federal Litigation Section.

If there is any further information you would like me to provide please let me know, and thank you for your consideration.

Adam I. Cohen  
Weil, Gotshal & Manges LLP  
767 Fifth Avenue  
New York, N.Y. 10153  
Tel. (212) 310-8901  
Fax (212) 310-8007  
<http://www.weil.com/weil/home.html>

< END >



# New York State Bar Association

One Elk Street, Albany, New York 12207 • 518/463-3200 • <http://www.nysba.org>

## COMMERCIAL AND FEDERAL LITIGATION SECTION

2003-2004 Officers

### LEWIS M. SMOLEY

Chair  
Davidoff & Malito LLP  
605 Third Avenue  
34<sup>th</sup> Floor  
New York, NY 10158  
646/428-3273  
FAX 212/286-1884  
lms@dmlegal.com

### LAUREN J. WACHTLER

Chair-Elect  
Montclare & Wachtler  
110 Wall Street  
New York, NY 10005  
212/509-3900  
FAX 212/509-7239  
ljwachtler@montclarewachtler.com

### STEPHEN P. YOUNGER

Vice-Chair  
Patterson, Belknap et al  
1133 Avenue of the Americas  
New York, NY 10036  
212/336-2685  
FAX 212/336-2222  
spyounger@pbwt.com

### MICHAEL B. SMITH

Secretary  
Solomon Zauderer et al  
45 Rockefeller Plaza  
7<sup>th</sup> Floor  
New York, NY 10111  
212/956-3700  
FAX 212/956-4068  
msmith@szefs.com

### LESLEY FRIEDMAN ROSENTHAL

Treasurer  
Paul, Weiss, Rifkind, Wharton  
& Garrison  
1285 Avenue of the Americas  
New York, NY 10019  
212/373-3092  
FAX 212/492-0092  
LRosenthal@paulweiss.com

### CATHI A. HESSION

Delegate to the House  
of Delegates  
Fleming Zulack & Williamson, LLP  
One Liberty Plaza  
35<sup>th</sup> Floor  
New York, NY 10006  
212/412-9506  
FAX 212/964-9200  
chession@fzw.com

### FORMER CHAIRS:

Robert L. Haig  
Michael A. Cooper  
Shira A. Scheindlin  
Harry P. Trueheart, III  
P. Kevin Castel  
Mark H. Alcott  
Gerald G. Paul  
Mark C. Zauderer  
Bernice K. Leber  
John M. Nonna  
Jack C. Auspitz  
Sharon M. Porcellio  
Jay G. Safer  
Cathi A. Hession



04-CV-045

December 20, 2004

Request to Testify  
2/11 DC

Peter G. McCabe, Esq.  
Secretary of the Committee on Rules of Practice and Procedure  
Administrative Offices of the United States Courts  
Washington, D.C. 20054

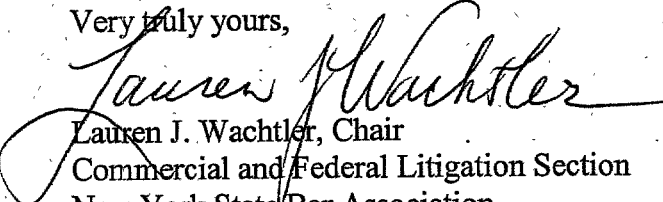
**Re: Report of the Electronic Discovery  
Committee and Federal Procedure  
Committee of the Commercial and  
Federal Litigation Section of the  
New York State Bar Association**

Dear Mr. McCabe:

Enclosed for consideration by the Advisory Committee on Civil Rules is a copy of the Report on Proposed Changes in the Federal Rules of Civil Procedure Relating to Electronically Stored Information. This report, which was prepared by our Electronic Discovery Committee and our Committee on Federal Procedure was unanimously adopted on December 15, 2004 by the New York State Bar Association Commercial and Federal Litigation Section.

It is respectfully requested that Gregory K. Arenson, the Chair of our Federal Procedure Committee, and Adam I. Cohen, the Chair of our Electronic Discovery Committee be given an opportunity to appear before the Civil Rules Advisory Committee on February 11, 2005 in Washington, D. C. to present the views set forth in this report.

Very truly yours,

  
Lauren J. Wachtler, Chair  
Commercial and Federal Litigation Section  
New York State Bar Association

LJW/zuy  
encl

cc: Adam I. Cohen, Esq.  
Gregory K. Arenson, Esq.

**REPORT ON PROPOSED CHANGES IN THE FEDERAL RULES  
OF CIVIL PROCEDURE RELATING TO ELECTRONICALLY  
STORED INFORMATION**

**New York State Bar Association  
Commercial and Federal Litigation Section**

**Dated: December 15, 2004**

## TABLE OF CONTENTS

	<u>Page</u>
TABLE OF CONTENTS.....	i
INTRODUCTION.....	1
SUMMARY.....	2
DISCUSSION.....	5
I. Adding Electronically Stored Information To The Discovery Rules.....	5
II. No Production Of “Not Reasonably Accessible” Electronically Stored Information, Except Upon A Motion With A Showing Of Good Cause.....	9
III. Early Attention To Issues Relating To Discovery Of Electronically Stored Information As Part Of Case Management.....	13
A. Current Rules.....	13
B. Proposed Amendments.....	14
C. Comments.....	15
IV. Providing Electronically Stored Information In Response To Interrogatories.....	16
V. Form Of Production.....	18
A. Proposed Amendments to Rule 34(b).....	18
B. Comments.....	19
1. Default Formats.....	20
a. Form in which ordinarily maintained.....	20
b. Electronically searchable form.....	21
2. Additional Searchability Issues Specific to Certain Types of Electronically Stored Information.....	22
a. E-mails.....	22
b. Metadata.....	22
c. Spreadsheets.....	23
d. Encryption/password protection.....	23
e. Databases.....	23
VI. Requests To Test Or Sample.....	24
VII. Preservation And Spoliation Of Discoverable Information.....	25
VIII. Protection Against Waiver Of Privilege.....	31
CONCLUSION.....	36

## INTRODUCTION

Almost four years ago, this Section stated that it was unnecessary for any changes to be made in the Federal Rules of Civil Procedure to accommodate the discovery of electronically stored information. Since then, case law about electronically stored information has grown exponentially as courts have started to face and deal with issues related to the preservation, discovery and spoliation of such information. In particular, the former chair of this Section, now a United States District Judge and a member of the Advisory Committee on Civil Rules of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (the "Advisory Committee"), Shira A. Scheindlin, has written a series of extremely thoughtful decisions on these issues providing excellent guidance for their resolution. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*"); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("*Zubulake III*"); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) ("*Zubulake IV*"); *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243 (SAS), 2004 WL 1620866 (S.D.N.Y. July 20, 2004) ("*Zubulake V*").<sup>1</sup> Nonetheless, other courts are not required to follow and have not followed the standards stated in the *Zubulake* decisions,<sup>2</sup> and some courts have adopted local rules or guidelines concerning discovery of electronically stored information.<sup>3</sup> In

---

<sup>1</sup> *Zubulake II – Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243 (SAS), 2003 WL 21087136 (S.D.N.Y. May 13, 2003) – did not concern an issue relating to electronically stored information, but the confidentiality of a deposition transcript.

<sup>2</sup> *See Multitechnology Servs., L.P. v. Verizon S.W.*, No. Civ. A. 4:02-CV-702-Y, 2004 WL 1553480, at \*1 (N.D. Tex. July 12, 2004) ("*Zubulake* is a district court opinion without binding authority"); *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2004 WL 1895122, at \*4 (N.D. Ill. Aug. 10, 2004) ("we modify the *Zubulake* rules by adding a factor").

<sup>3</sup> *See* Rule 26.1(4) of the Rules of the United States District Court for the Eastern and Western Districts of Arkansas; Civ. Rule 26.1(b)(2)(d) and (g) of the Local Civil and Criminal Rules of the United States District Court for the District of New Jersey; Rule 26.1(d)(3) of the Local Rules of the United States District Court for the District of Wyoming; the Electronic Discovery Guidelines of the United States District Court for the District of Kansas; and the Default Standard for Discovery of Electronic Documents of the United States District Court for the District of Delaware.

addition, there have been conferences discussing issues relating to electronically stored information<sup>4</sup> and a treatise authored by co-authors of this report.<sup>5</sup> With this ferment and the possibility of inconsistent approaches to the same issues, the Section finds that it is now appropriate to establish uniform rules in the federal courts concerning the discovery of electronically stored information.

On August 9, 2004, the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States published for comment Proposed Amendments to the Federal Rules of Civil Procedure (the "Amendments"). Accompanying the proposed amendments was a Report of the Civil Rules Advisory Committee, revised August 3, 2004 (the "Report"). This report contains the comments of the New York State Bar Association Commercial and Federal Litigation Section on the proposed amendments to Rules 16, 26, 33, 34, 37 and 45 and Form 35.

#### SUMMARY

The Section's position on each of the proposed changes to the Federal Rules of Civil Procedure involving discovery of electronically stored information is:

Rule 16(b)(5): The Section supports the proposed change to allow a court as part of the initial case management order to include provisions for the disclosure or discovery of electronically stored information.

Rule 16(b)(6): The Section supports the proposed change to allow a court as part of the initial case management order to include a provision embodying an agreement on inadvertent waiver of privilege.

---

<sup>4</sup> See The Sedona Conference Working Group Series, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (January 2004), available at [http://www.thesedonaconference.org/publications\\_html](http://www.thesedonaconference.org/publications_html) (the "Sedona Principles").

<sup>5</sup> See Adam I. Cohen & David J. Lender, *Electronic Discovery: Law and Practice* (Aspen 2003).

Rule 26(b)(2): The Section supports the proposed change to characterize electronically stored information as either reasonably accessible or not reasonably accessible for purposes of discovery and to require a showing of good cause by the requesting party to obtain discovery of the latter. However, we suggest that the Advisory Committee Note explicitly state that accessibility is determined by the steps that need to be taken for the electronically stored information to be usable, not merely by the medium on which the information is stored. A court should also consider the frequency with which the electronically stored information has been accessed in the past.

Rule 26(b)(5)(B): The Section supports the proposed change to provide a procedure for handling privileged information that is inadvertently disclosed. We suggest that the Rule include a statement of the obligation not to use, disclose or disseminate information once notified that it has been inadvertently produced and is privileged. We do not think that a requirement for certification of destruction or sequestration of inadvertently disclosed information is necessary. We would like to see further explanation in the Advisory Committee Note of sequestration of electronically stored information after notice of inadvertent production.

Rule 26(f): The Section supports the proposed change to require parties to discuss at their initial discovery conference the preservation of information.

Rule 26(f)(3): The Section supports the proposed change to require parties to discuss at their initial discovery conference the disclosure or discovery of electronically stored information.

Rule 26(f)(4): The Section supports the proposed change to require parties to discuss at their initial discovery conference the protection of privileged information in discovery whether as stated in the proposed Rule or as stated in the alternative in the Report.

Rule 33: The Section supports the proposed change to allow a party responding to interrogatories to provide access to electronically stored information as an answer.



Rule 34(a)(1): The Section supports the proposed changes that will separate electronically stored information from documents and permit testing or sampling of either.

Rule 34(b): The Section supports the proposed change to allow a request to specify the form in which electronically stored information is to be produced and in theory supports the proposed change to allow a responding party to produce electronically stored information in a form in which it is ordinarily maintained or in an electronically searchable form. However, the Section recommends that the Advisory Committee Note provide greater guidance regarding the production of electronically stored information in native format and in an electronically searchable form or that it use other terminology.

Rule 37(f): The Section supports the proposed change in the proposed Rule to provide a safe harbor from a spoliation sanction for electronically stored information that becomes unavailable due to the routine operation of an electronic information system when reasonable steps are taken to preserve the information and opposes the proposed change in the footnote to the proposed Rule. The Section suggests that an explanation be provided in the Advisory Committee Note of the factors to be used in determining what is the routine operation of an electronic information system.

Rule 45(a)(1)(C): The Section supports the proposed changes that allow for subpoenas to request electronically stored information and testing or sampling of any information in parallel to the changes to Rule 34(a)(1).

Rule 45(a)(1): The Section supports the proposed Rule to allow subpoenas to specify the form in which electronically stored information may be produced.

Rule 45(b)(2): The Section supports the proposed changes regarding requests for testing or sampling in a subpoena that conform to the proposed changes in Rule 45(a)(1)(C).

Rule 45(c)(2)(A): The Section supports the proposed changes regarding the response of a subpoenaed person to a request for electronically stored information or for testing or sampling that conform to the proposed changes in Rule 45(a)(1)(C).

Rule 45(c)(2)(B): The Section supports the proposed changes regarding the response of, and the form of that response by, a subpoenaed person to a request for electronically stored information or for testing or sampling that conform to the proposed changes in Rule 45(a)(1).

Rule 45(d)(1)(B): The Section supports the proposed changes to the extent it supports the parallel changes in Rule 34(b).

Rule 45(d)(1)(C): The Section supports the proposed changes, which for the most part correspond to the proposed changes in Rule 26(b)(2). However, we suggest that the proposed Rule also include the statement at the end that the court may specify terms and conditions for the discovery of electronically stored information that is not reasonably accessible.

Rule 45(d)(2)(B): The Section supports the proposed change, which corresponds to the change in proposed Rule 26(b)(5)(B).

Form 35, ¶ 3: The Section supports the proposed changes, which correspond to the changes in proposed Rules 26(f)(3) and 26(f)(4).

## DISCUSSION

### I. Adding Electronically Stored Information To The Discovery Rules

The Advisory Committee proposes to add a new term to the Rules – “electronically stored information” – to distinguish it from documents. The Report acknowledges that the “term ‘documents’ cannot be stretched to accommodate all the differences between paper and electronically stored information in all the rules.” The choice of terminology appears to be reasonably accurate and appropriately flexible. The use of the word “electronically” signals the

main area of concern that has engendered the movement to amend the rules, *i.e.*, information that is generated, received, transmitted, processed, and recorded by computers and other electronic devices. Use of the word "stored" should be similarly uncontroversial.<sup>6</sup> Obviously, if information has not been stored in some way it cannot be produced in discovery.

Proposed Rule 34(a)(1), *inter alia*, explicitly inserts "electronically stored information" within the scope of available discovery and adds references to information recorded on non-electronic media. The proposed Rule states (with changes from the existing Rule indicated):

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, and copy, test, or sample any designated *electronically stored information or any designated* documents (including writings, drawing, graphs, charts, photographs, *sound recordings, images, phonorecords, and other data or data compilations in any medium . . .*).

It should not be controversial to update Rule 34 to explicitly refer to "electronically stored information." As a practical matter, courts and litigants have been treating electronically stored information as subject to discovery under Rule 34 for decades. *See* Advisory Committee Note to Rule 34 (1970); *see also Crown Life Ins. Co. v. Craig*, 995 F.2d 1376, 1382-83 (7th Cir. 1993) ("Advisory Committee notes to the 1970 amendment of Federal Rule of Civil Procedure 34 make clear that computer data is included in Rule 34's description of documents"); *Zubulake I*, 217 F.R.D. at 316-17; *Playboy Enter. Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999). Current Rule 34(a)(1) defines the scope of document discovery as permitting "the party making the request . . . to inspect and copy[] any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, *and other data compilations from which information can be*

---

<sup>6</sup> There is *no* basis in the language of the proposed Rules or the proposed Advisory Committee Notes to suggest that use of the word "stored" as opposed to, for example, "created," is meant to impact preservation obligations, *e.g.*, by suggesting that no preservation obligation could arise with respect to information that is not normally stored. This point could be further clarified in the proposed Advisory Committee Notes explicitly if such misunderstanding emerges as a concern.

*obtained*)” (emphasis added). The Advisory Committee Note for the 1970 amendments to Rule 34 explains that the term “data compilations” was added to expand the description of “documents” in accordance with new advances and changes in technology. Many judicial opinions have interpreted the reach of Rule 34 as extending to all manner of electronic information. *See Crown Life, supra, Zubalake I, supra; Playboy Enter., supra.*

Nonetheless, the current language of Rule 34 clearly is out of step with this reality. As the proposed Advisory Committee Note states, it is a “stretch” to use the terminology of “documents,” with its origins in the paper world, to refer to sources of information such as e-mails. Amendments, at 28. Even the phrase “data compilations” seems arcane because it is not a term used in referring to the most common subjects of discovery of electronically stored information, such as e-mail or word processing files. Indeed, just how far the discoverability of electronically stored information extends has been the subject of debate.<sup>7</sup>

Given the rapid, ongoing development of technology and specifically of new ways of storing information, the Rules should strive to be as neutral and flexible as possible in describing discoverable electronically stored information in terms of media. A list of specific types of media available for discovery purposes would ensure speedy obsolescence of any rule containing or based on such a list, and the Advisory Committee has eschewed such a list. To the extent that other types of non-electronic media may be subject to discovery, these would appear to be encompassed by the proposed changes to the parenthetical to specify sound recordings, images or “other data . . . in any medium.” What information is *potentially* discoverable in the first instance should depend upon

---

<sup>7</sup> The Sedona group has suggested that, if “data can be readily compiled into viewable information, whether presented on the screen or printed on paper,” it should be classified as the equivalent of a “document.” *Sedona Principles*, at 33. It further argues that “data used by a computer system, but hidden and never revealed to the user in the ordinary course of business, should not be presumptively treated as part of the ‘document.’” *Id.*

the relationship of its subject matter to the claims and defenses involved in the lawsuit – not on whether it is stored on paper, electronically, or in some other medium.<sup>8</sup> Limitations on discovery based on burden and cost allocation considerations, where the medium and manner in which information is stored may be important factors, are dealt with elsewhere in existing Rule 26(b)(2) and proposed Rules. The Section supports the proposed changes in Rule 34(a)(1) to incorporate and distinguish electronically stored information.

The Report (at 16) seeks comment on whether Rule 34 or the Advisory Committee Note should specifically state that a party responding to a Rule 34 request should not avoid reviewing and producing electronically stored information because a production request did not separately seek it, and, if so, what should be stated. This is a situation that should not arise under the proposed modifications. First, as discussed below, the scope of discovery of electronically stored information is a subject that should have been discussed by the parties and addressed by the court during Rule 26 and 16 conferences. Accordingly, there should be no ambiguity by the time Rule 34 requests are served about whether a requesting party seeks electronically stored information in discovery, even if there remains an ambiguity regarding the precise scope of the electronic discovery sought. Moreover, given the proposed modification to Rule 34(a)(1), a requesting party need simply point out that its requests cover all information within the scope of that Rule in order to make it clear that it seeks electronically stored information. Under the circumstances envisioned by the proposed Rules, it is probably reasonable for a responding party to assume that, where a requesting party has not asked for electronically stored information in either a Rule 16 or Rule 26 conference or in a Rule 34(a)(1) request, the requesting party is not interested in such

---

<sup>8</sup> Conversely, a discovery request seeking production of a type of media without regard to the subject matter of its contents would be improper.

information. Accordingly, the Section recommends that the proposed Advisory Committee Note to Rule 34(a) not include a statement that “a Rule 34 request for production of ‘documents’ should be understood to include electronically stored information.”

## II. No Production Of “Not Reasonably Accessible” Electronically Stored Information, Except Upon A Motion With A Showing Of Good Cause

The Advisory Committee proposes to amend Rules 26(b)(2) and 45(d)(1)(C) to add a distinction between discovery of electronically stored information that is reasonably accessible and that which is not reasonably accessible. Proposed Rule 26(b)(2) states:

A party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible. On motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause and may specify terms and conditions for such discovery.<sup>9</sup>

“Reasonably accessible” is not a defined term in the proposed Rules.<sup>10</sup> As a means of distinguishing “reasonably accessible” electronically stored information from that which is “not

---

<sup>9</sup> Proposed Rule 45(d)(1)(C) differs from the proposed addition to Rule 26(b)(2) in the following respects shown by bracketed words for additions and stricken words for deletions:

A party [person responding to a subpoena] need not provide discovery of electronically stored information that the party [person] identifies as not reasonably accessible. On motion by the requesting party, the responding party must show that the information [sought] is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause and may specify terms and conditions for such discovery.

The Section recommends that proposed Rule 45(d)(1)(C) be modified to conform to proposed Rule 26(b)(2) by adding the last clause to clarify that, in regard to not reasonably accessible electronically stored information, courts may specify terms and conditions for such discovery from non-parties as well.

<sup>10</sup> Judicial use of the term “accessible data” in connection with discovery of electronically stored information appears to have originated with Judge Scheindlin in *Zubulake I*, 217 F.R.D. at 318-20. In a description that the Section endorses as a guide to be used under the proposed Rules, Judge Scheindlin wrote:

Information deemed “accessible” is stored in a readily usable format. Although the time it takes to actually access the data ranges from milliseconds to days, the data does not need to be restored or otherwise manipulated to be usable. “Inaccessible” data, on the other hand, is not readily usable. Backup tapes must be restored using a process . . .

reasonably accessible,” the proposed Advisory Committee Note to Rule 26 focuses on the effort and expense required to locate, retrieve and produce such information and whether the person routinely uses the information. Amendments, at 11-12. The proposed Advisory Committee Note states that designation of information by a person as “not reasonably accessible” requires such person to “identify the information it is neither reviewing nor producing on this ground.”

Amendments, at 13. As proposed, the degree of specificity required in identifying such information will vary based on circumstances. Under the proposed Rules, if the requesting party moves to compel the information designated as “not reasonably accessible,” the responding person must make some kind of a showing demonstrating the relative inaccessibility of the information in dispute. If the responding person satisfies that burden, then the requesting party may obtain discovery of the information only for “good cause” and, pursuant to Rule 26(b)(2), upon such terms and conditions as the court imposes.

The proposed Advisory Committee Note to Rule 26 describes one potential referent for accessibility as whether a party “routinely accesses or uses the information.” Amendments, at 12.

---

fragmented data must be de-fragmented, and erased data must be reconstructed, all before the data is usable. That makes such data inaccessible.

*Id.*, 217 F.R.D. at 320.

We are concerned that the use of “routine” in this context may be confused with the use of “routine” in the context of the proposed safe harbor under proposed Rule 37(f) and is otherwise undefined.<sup>11</sup> The Section suggests that the Advisory Committee Note explicitly state that accessibility is determined by the steps that need to be taken for the electronically stored information to be usable. *See Zubulake I*, 217 F.R.D., at 320. A court should not consider merely the medium on which the information is stored, such as a backup tape. A court should consider the frequency with which the electronically stored information has been accessed in the past.

For example, a party may access some portion of otherwise inaccessible information as a sample to demonstrate the effort and expense of doing so. Making the required showing in this manner should not be discouraged.

Similarly, simply because a person has in the past accessed a backup tape for some particular purpose, such backup tapes should not necessarily be “fair game” in discovery despite the effort and expense involved in achieving such access. In other words, the mere fact that a source of information was accessed in the past does not necessarily mean that it is “reasonably accessible.”<sup>12</sup>

With respect to what identification of information that is not reasonably accessible is contemplated, the proposed Rule is unclear. For example, is it sufficient for a party to identify the source and nature of such information as “backup tape data” or “data that may reside on hard drives” or does the Rule contemplate a more detailed description of the inaccessible information? One difficulty in this regard is that information that is not reasonably accessible may be difficult to identify with specificity precisely because it is inaccessible. For example, while it may be

---

<sup>11</sup> For example, backup tapes may be “routinely” accessed in connection with disaster recovery efforts, but this should not necessarily mean they would be “reasonably accessible” for discovery purposes.

<sup>12</sup> On the other hand, if a producing entity claims that electronically stored information is not reasonably accessible and later retrieves and uses the information in the case, a court should have little difficulty in finding “good cause” for the production of the remainder of the information similarly stored.



theoretically true as a general proposition that hard drives may contain deleted e-mails, whether or not this is the case in any particular instance – especially with respect to deleted e-mails that contain relevant and responsive information – may be unknown. Moreover, the ability to describe such information may be limited by the constraints of the particular computer systems at issue. The Advisory Committee should provide further guidance as to the type of identification of information that is not reasonably accessible which is contemplated by the proposed Rule.

The proposed Advisory Committee Note to Rule 26 describes examples of not reasonably accessible information, including deleted data that may still reside on a hard disk of a personal computer retrievable only with resort to expensive and uncertain forensic techniques and data on backup tapes stored solely for disaster recovery purposes and difficult to use for other purposes. Such data would ordinarily not be subject to production under the proposed Rule without a showing of good cause, although “it is important not to conflate the purpose of retention with accessibility,” *Zubulake I*, 217 F.R.D. at 322 n.68. This distinction is consistent with developing case law. Courts have generally permitted hard disk inspections aimed at recovering deleted e-mail only upon a special showing as to why such discovery is warranted and then often under protocols designed to address concerns regarding preservation of privilege and protection of the integrity of the data.<sup>13</sup> See *Simon Prop. Group, supra*, 194 F.R.D. at 641-642 (having demonstrated troubling discrepancies with respect to defendant’s production, plaintiff was allowed to recover deleted computer files in computers used by defendant’s employees, but protective measures were taken,

---

<sup>13</sup> Generally, protocols have required a neutral computer forensics expert to extract all potentially relevant data from the hard drive in question, whereupon the data is provided to the producing party for review and an opportunity to identify information that should not be produced, for privilege or other reasons. See *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 653-54 (D. Minn. 2002); *Playboy Enter., supra*, 60 F. Supp. 2d at 1055; *Simon Prop. Group LP v. mySimon, Inc.*, 194 F.R.D. 639, 643-44 (S.D. Ind. 2000). The Advisory Committee Note should cite to cases where courts have used such protocols to address the terms and conditions under which discovery of “not reasonably accessible” electronically stored information might occur.

including the appointment of an expert to copy the information.); *Playboy Enter., supra*, 60 F. Supp. 2d at 1051 (to determine whether defendant deleted and continued to delete relevant e-mails, the court permitted plaintiff to inspect defendant's e-mails under a protocol with expert assistance). Similarly, backup tapes generally have been subject to production only where they are shown likely to contain relevant information not available from more readily accessible sources. *See Wiginton, supra*, 2004 WL 1895122, at \*8 (ordering the production of backup tapes after preservation problems with active e-mails arose, but with the requesting party paying 25% of the cost); *Zubulake I*, 217 F.R.D. at 324 (employee was entitled to discovery of relevant e-mails that had been deleted and resided only on backup tapes). The Advisory Committee Note should cite to some of this case law for examples of what would constitute "good cause" to obtain electronically stored information that is not reasonably accessible.

### **III. Early Attention To Issues Relating To Discovery Of Electronically Stored Information As Part Of Case Management**

#### **A. Current Rules**

Under Rule 26(f), the parties must, as soon as practicable, and, in any event, at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer in order to develop a plan for discovery and then submit to the court a joint written report outlining the discovery plan. As described in Rule 26(f), in most cases the initial disclosure requirements set forth in Rule 26(a) must be dealt with in the parties' initial planning meeting, as well as in the proposed discovery plan to be submitted to the court. These requirements include, among other things, the items described in Rule 26(a)(1)(B), namely: "a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment."

## **B. Proposed Amendments**

A proposed amendment to Rule 16 adds discovery of electronically stored information to the existing list of topics that a court's scheduling order may address. In particular, proposed Rule 16(b)(5) would expressly mention that the scheduling order may include "provisions for disclosure or discovery of electronically stored information." As indicated in the proposed Advisory Committee Note, this revision is "designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur." Amendments, at 3.

The proposed revision to Rule 16 goes hand in hand with proposed amendments to Rule 26(f) and Form 35 with respect to topics to be discussed at and reported from the parties' planning meeting. The amendment to Rule 26(f) adds that the discovery plan, which is to be jointly prepared by the parties, would address the parties' respective views and proposals on the topic of "(3) any issues relating to disclosure or discovery of electronically stored information, including the form in which it should be produced." The change in Form 35, Report of Parties' Planning Meeting, calls for a report to the court on the results of the parties' discussions regarding how to handle disclosure or discovery of electronically stored information. Amendments, at 51. The proposed Advisory Committee Note to Rule 26 describes the intended scope of the discussion and report to the court:

Any aspects of disclosing or discovering electronically stored information discussed under Rule 26(f) may be included in the report to the court. Any that call for court action, such as the extent of the search for information, directions on evidence preservation, or cost allocation, should be included. The court may then address the topic in its Rule 16(b) order.

Amendments, at 18.

### C. Comments

According to the Advisory Committee, the proposed amendments to Rule 16, Rule 26(f) and Form 35 “present a framework for the parties and court to give early attention to issues relating to the disclosure or discovery of electronically stored information.” Report, at 6. Early attention to issues relating to discovery of electronically stored information should go a long way toward preventing the outbreak of related problems at times when they will disrupt the litigation process. Similar rules requiring early attention to electronic discovery issues have been enacted by several local district courts. *See* Rule 26.1(4) of the Rules of the United States District Court for the Eastern and Western Districts of Arkansas; Civ. Rule 26.1(b)(2)(d) and (g) of the Local Civil and Criminal Rules of the United States District Court for the District of New Jersey; Rule 26.1(d)(3) of the Local Rules of the United States District Court for the District of Wyoming; the Electronic Discovery Guidelines of the United States District Court for the District of Kansas, ¶ 4; and the Default Standard for Discovery of Electronic Documents of the United States District Court for the District of Delaware, ¶ 2. The many cases in which parties have been sanctioned for failing to preserve or produce electronically stored information doubtless include situations that might have been avoided had the parties discussed issues of electronically stored information preservation and production at the outset of the case.

Discussion about storage, preservation and retrieval of electronically stored information during the Rule 26(f) conference will help to avoid miscommunications and misunderstandings between counsel as to what was sought through discovery by a requesting party and the corresponding obligations of the responding party. A responding party should not have to guess at what a requesting party is seeking, particularly under circumstances where it may not be clear due to the nature of the case or course of conduct in the litigation that a requesting party is interested in

a particular source of electronic information. Discussion at the Rule 26(f) conference may go a long way toward facilitating the ability to fashion specific discovery requests targeting particular sources of electronically stored information, including the type of electronically stored information sought and the sources of electronically stored information the requesting party expects the responding party to search.

In most current cases, discovery of electronically stored information has not become a subject of dispute, and the topic is not addressed explicitly. The proposed Rule will force parties to develop and disclose positions on discovery issues concerning electronically stored information at the outset of the case, which at least in some cases will have the effect of creating disputes. Nevertheless, the prevention of problems arising from undisclosed, disparate views regarding discovery obligations relating to electronically stored information, which are uncovered only when a case has progressed to an advanced stage or after loss of potentially relevant information, is a far more important consideration. The proposed Rule represents a judgment that the benefits of mandatory early discussion of issues relating to electronically stored information outweigh the risks of additional disputes.

#### **IV. Providing Electronically Stored Information In Response To Interrogatories**

The only proposed change in Rule 33 is to add in Rule 33(d) that electronically stored information is included within the "business records" that may be specified in an answer to an interrogatory. The proposed Advisory Committee Note to Rule 33 points out that the term "electronically stored information" has the same broad meaning in proposed Rule 33(d) as in proposed Rule 34(a)(1).

Although proposed Rule 33(d) does not on its face impose additional requirements on how electronically stored information may be used to respond to an interrogatory compared to hard

copies of business records, the proposed Advisory Committee Note restates that such information may be provided as an answer where “the burden of deriving the answer will be substantially the same for either party.” Amendments, at 24. In other words, the responding party, *if it elects to respond to an interrogatory by providing electronically stored information*, must ensure that the interrogating party is able to locate or identify the electronically stored information from which the answer may be ascertained “as readily as can the party served.” *Id.* In order to meet this requirement, under existing Rule 33(d), the responding party must provide the interrogating party a “reasonable opportunity to examine, audit or inspect” the information and “to make copies, compilations, abstracts or summaries.” Where electronically stored information is involved, the proposed Advisory Committee Note states that this may mean providing “some combination of technical support, information on application software, access to the pertinent computer system, or other assistance.” Amendments, at 24. *See In re Honeywell Int’l, Inc. Sec. Litig.*, No. M8-85 WHP, 2003 WL 22722961, at \*2 (S.D.N.Y. Nov. 18, 2003) (directing Price Waterhouse to produce a copy of its workpapers on CD-ROMs that could be viewed only by using Price Waterhouse’s proprietary software, along with the proprietary software itself).

The Section supports the change in Rule 33(d). An example where the proposed Rule would apply would be where a responding party provides the requesting party with access to a database upon which to run certain queries in order to extract relevant information. Disputes as to the manner and extent of access to electronically stored information provided in response to interrogatories, as well as cost allocation, will continue to arise,<sup>14</sup> but there is no reason the Rule

---

<sup>14</sup> *See Multitechnology Servs.*, *supra*, 2004 WL 1553480, at \*2 (requiring the parties to split the expenses of deriving interrogatory answers from Verizon’s databases).

should not be updated to reflect the current reality that business records are electronically stored and that answers to interrogatories may be derived from electronically stored information.

## V. Form Of Production

### A. Proposed Amendments to Rule 34(b)

The Advisory Committee proposes the following addition to Rule 34(b):

The request may specify the form in which electronically stored information is to be produced . . . If a request for electronically stored information does not specify the form of production, a responding party must produce the information in a form in which it is ordinarily maintained, or in an electronically searchable form. The party need only produce such information in one form.

The proposed amendments to Rule 34(b) *permit* the requesting party to specify the form in which electronically stored information is to be produced and allow the responding party to object to the requested form. According to the proposed Advisory Committee Note, the “grounds for the objection depend on the circumstances of the case.” Amendments, at 31. The proposed Note points out that, if an objection is made, Rule 37(a)(2)(B) requires the parties to meet and confer before a motion to compel is filed. *Id.* Proposed Rule 34(b) does not *require* the requesting party to choose a form of production for electronically stored information.

The proposed Advisory Committee Note clarifies that, “[i]f the request does not specify a form of production for electronically stored information, Rule 34(b) provides that the responding party must – unless the court orders otherwise or the parties otherwise agree – choose between options analogous to those provided for hard-copy materials. The responding party may produce information in a form in which it ordinarily maintains the information.” *Id.*, at 30. Alternatively, the responding party may produce the electronically stored information in an electronically

searchable form. *Id.* If the requesting party specifies a form of production, proposed Rule 34(b) permits the responding party to object to the request (grounds for objections are case-specific). *Id.*<sup>15</sup>

The proposed Advisory Committee Note to Rule 34(b) emphasizes that the “form of production is more important to the exchange of electronically stored information than of hard copy materials” and that the “specification of the desired form may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information.” *Id.*

## B. Comments

There has been much discussion in recent federal case law and among practitioners regarding the form of production of electronically stored information. *See Zakre v. Norddeutsche Landesbank Girozentrale*, No. 03 Civ. 0257 (RWS), 2004 WL 764895, at \*1 (S.D.N.Y. Apr. 9, 2004) (plaintiff’s request to compel defendant to review two CDs for responsive documents denied because the defendant produced documents in text-searchable format that was as close as possible to the way they were kept in the usual course of business); *Northern Crossarm Co. Inc. v. Chemical Specialties, Inc.*, No. 03-C-415-C, 2004 WL 636606, at \*1-\*2 (W.D. Wis. Mar. 3, 2004) (plaintiff’s motion to compel defendant to produce e-mails in electronic form after production in hard copy denied because plaintiff did not request production in electronic form); *Super Film of Am., Inc. v. UCB Films, Inc.*, 219 F.R.D. 649, 656-57 (D. Kan. 2004) (defendant’s motion to compel discovery of electronic versions of e-mails, documents, databases and spreadsheets granted because plaintiff’s conclusory contention it did not have the expertise to retrieve the information was inadequate); *In re Honeywell Int’l Sec. Litig.*, *supra*, 2003 WL 22722961, at \*2 (accountant compelled to produce its workpapers electronically because it had not provided plaintiffs with an adequate means to

---

<sup>15</sup> As discussed above, proposed Rule 26(f) provides that parties must discuss during the discovery-planning conference any issues relating to the disclosure and discovery of electronically stored information, including the form of production.



decipher how the documents were kept in the usual course of business); *see also Sedona Principles*, at 17. Given that the form of production has become a frequent source of controversy in connection with electronically stored information, it makes sense to establish some procedure for the issue to be raised and resolved in discovery. The procedure contemplated by the proposed rule is flexible and reasonable. However, it does raise some issues regarding default production formats.

## 1. Default Formats

### a. Form in which ordinarily maintained

Producing electronic documents in the form in which they are ordinarily maintained suggests producing native electronic files. "Native" refers to the original form of a file when it is created by file-creation software such as Word, Excel, Word Perfect or Access. Producing data in native format has one principal advantage: after gathering the data, it does not need to be further processed for production. However, there are a number of substantial and legitimate disadvantages with current technology, including:

- Potential spoliation of native files – Native files contain embedded metadata that memorializes when a document was created, what computer it was created on, when it was last accessed, and when it was last modified. Some of this information may be relevant to litigated issues. When producing or receiving native files as part of a production, either party can change some or all of that metadata by copying, opening or re-saving the documents. Similarly, the substantive text of the documents is not "locked;" as a result a party can inadvertently or purposely change the text of a native file.
- Disclosure of privileged or confidential information – Certain word processing programs retain a history of edits to the document in a hidden form. Upon receiving such documents in native format, a party could reveal or restore those rejected edits, which may be privileged or confidential.
- Certain native files are unreadable -- While Word, Word Perfect and Outlook files or e-mails are readable when produced in native format, many other kinds of files are not. For example, Groupwise mailboxes, if simply copied to a CD-ROM, cannot normally be read by a receiving party because of encryption issues. Many database files will not function outside of the hardware and security environment in which they were created. Accordingly, for many file types, they must be exported and processed into some readable format such as .txt (text) files, PDFs or .tiffs.

- Inability to redact privileged material – There is no workable way to redact documents in native format. Thus, when it comes to redacted documents, the parties or the court will have to establish an exception form. This exception will likely take the form of processing the native file to an electronic image such as a PDF or .tiff or printing the file and redacting it the old-fashioned way.
- Inability to efficiently sequentially number documents – There is no way to attach control numbers to native documents. Rather, a production of native documents only retains the native page numbering. Control numbering is essential for any significant production in order to avoid confusion, to resolve discovery disputes, and to make a record of what was in fact produced.

**b. Electronically searchable form**

As to the option of producing information in an electronically searchable form, the proposed Advisory Committee Note *concedes* that “although this option is not precisely the same as the option to produce hard-copy materials organized and labeled to correspond to the requests, it should be functionally analogous because it will enable the party seeking production to locate pertinent information.” Amendments, at 30. The Section recommends that the Advisory Committee Note further explain what is “an electronically searchable form,” since it is unclear the extent of “searchability” contemplated.

The process of converting native electronic files to static, but searchable, images requires very substantial technology, time and money. Moreover, there are a number of very different ways of creating searchable data sets, and the field is evolving every day. For example, certain electronic discovery technologies involve creating searchable .tiff images or searchable PDFs of each page in an electronic production and storing those .tiffs in a searchable database. Sometimes that database is exported to a “load file,” which can be loaded into litigation support software like Summation, Concordance or Documatrix. Other technologies make the searchable database accessible on-line through a web browser. A new technology posts the data to an on-line database, but in native format, and allows the user to “promote” only relevant search hits to .tiff, thereby saving on .tiff

conversion costs. The Section believes that the Advisory Committee Note should not designate any specific technology but should provide more guidance on the level of functionality contemplated. However, when it comes to searching electronically stored information, there are issues that are unique to each file format, and a one-size-fits-all mandate for searchability is probably not feasible.

## **2. Additional Searchability Issues Specific to Certain Types of Electronically Stored Information**

### **a. E-mails**

The proposed Rule is unclear as to whether e-mail attachments must be searchable, as opposed to only the message body. In addition, guidance could be provided as to what additional fields must be searchable within an e-mail. For example, "To," "From," "cc," "bcc," and "Subject" are obvious fields, but e-mails can have hundreds of fields, many of them hidden. Such fields include a document ID, or the IP addresses of the servers that handled a received e-mail while it was *en route*. In certain cases such fields are irrelevant; in others they can be important.

### **b. Metadata**

The proposed Rule could address whether embedded metadata in non-e-mail electronically stored documents should be searchable, including Created Date, Last Accessed Date, Last Modified Date, and Author. Again, there are more esoteric forms of embedded metadata in documents such as Revision Number and Last Ten Authors (which shows the names of the last ten computers on which the document was saved). Guidance could be provided about the level of metadata that should be searchable. Implicit in any such guidance would be an expectation that when electronically stored documents are preserved that such metadata be accurately captured and preserved. Such a requirement can be burdensome, as it currently requires forensic tools and knowledge to be used in the preservation process.

**c. Spreadsheets**

The electronic production of spreadsheets often involves problems. Tiffing on a one-page-to-one-tiff basis can reduce the print size of a wide spreadsheet so that it is unreadable and unsearchable. Tiffing on a one-page-to-multiple-tiffs basis can make reading the spreadsheet difficult. Since tiffing or PDFing creates only an image of what is visible on the surface of the spreadsheet, the formulas underlying certain cells are not captured. In addition, when spreadsheets are collected from a producing party, many columns are often "hidden," to enable the user to view only the information she may need. This raises the issue as to whether the Rule should direct that spreadsheets be produced after all columns are un-hidden; in a way to ensure readability; or in a way to display formulas when relevant to the litigation.

**d. Encryption/password protection**

Either by corporate policy or by individual user behavior, electronically stored documents and e-mails can be encrypted or password-protected. Such e-mails and documents cannot be searched until they are decrypted or unlocked. Accordingly, an issue is whether the Rule should require all enterprise e-mail and documents to be decrypted or unlocked, and that reasonable efforts be used to decrypt or unlock individually-encrypted documents.

**e. Databases**

Simple databases, such as those that are created in and operate in Microsoft Access, can be copied and produced electronically in discovery, and the receiving party can load the database in Access and perform searches. Enterprise-level databases can be copied, but in many instances, those copies will not function outside their native hardware or security environments. Thus, the copies are not functional or readable, let alone searchable. In such instances data can be exported

from the database into an Excel spreadsheet or .csv file, which is searchable, but the exported data often appears as meaningless rows of data.

\* \* \*

As this discussion demonstrates, when dealing with the ability to search electronically stored information, one quickly and necessarily gets down into the weeds relating to each file format. The Section's concern is that a broad rule only requiring a "searchable" format will gloss over these substantial issues, leading to a patchwork of judicial interpretation. On the other hand, the Rule cannot speak directly to each of the hundreds of file formats. This suggests that a requirement of production in an electronically searchable form may not be feasible as a blanket rule.

The Section agrees that, in theory, production of electronically stored information in an electronically searchable form is a viable form of production and is to a limited extent functionally analogous to labeling hard copy material to correspond to an individual document request. However, given the uncertainty regarding what "electronically searchable" means in any particular case, the Section recommends that the Advisory Committee Note either provide greater detail in defining an electronically searchable form or decline to employ such terminology in defining default production formats.

## **VI. Requests To Test Or Sample**

Proposed amendments to Rules 34(a)(1), 45(a)(1), 45(a)(1)(C), 45(b)(2), 45(c)(2)(A), and 45(c)(2)(B) would recognize a right to request and a duty to provide a "test, or sample" within the scope of permitted discovery requests. This right would apply to all forms of discoverable information, including electronically stored information.

Explicitly recognizing a right to test or sample has particular application to electronically stored information since courts have used sampling as a means to determine whether discovery of

certain electronically stored information is warranted, and, if so, whether cost shifting is appropriate. See *Zubulake I*, 217 F.R.D. at 324 (“[r]equiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases”); *McPeck v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001) (deciding to take small steps and perform “a test run” on potentially discoverable data); *Wiginton, supra*, 2004 WL 1895122, at \*4 (“the actual results of the test run will be indicative of how likely it is that critical information will be discovered” for purposes of determining whether to shift costs of a search of backup tapes). The Section supports the proposed changes.

## VII. Preservation And Spoliation Of Discoverable Information

Preservation of information in any form is not specifically covered by the Federal Rules of Civil Procedure. Case law has developed the rule that “[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake IV*, 220 F.R.D. at 216 (quoting *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001)). See also *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001); *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984); *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 485-86 (S.D. Fla. 1984); *Bowmar Instrument Corp. v. Texas Instruments, Inc.*, 25 Fed. R. Serv. 2d (Callaghan) 423, 427, 1977 U.S. Dist LEXIS 16078, at \*11 (N.D. Ind. May 2, 1977); Gorelick, Marzen and Solum, *Destruction of Evidence* § 3.12, at 104 (1989). “A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter.” *Zubulake IV*, 220 F.R.D. at 218. “The duty should certainly extend to any documents or tangible things . . . made by individuals ‘likely to have discoverable information that the disclosing party

may use to support its claims or defenses.” *Id.*, 220 F.R.D. at 217-18, quoting Rule 26(b)(1). “The duty also includes documents prepared *for* those individuals.” *Zubulake IV*, 220 F.R.D. at 218 (emphasis in original).

The duty of preservation raises additional issues in the context of electronically stored information. Easily accessible active data is constantly being updated and written over. On the other hand, many organizations currently conduct daily back-ups of their electronic systems for recovery purposes in case of an emergency. Halting all work to preserve the current state of electronically stored information probably is not feasible. Preserving all backup tapes may be equally unrealistic.

Continued operation of computers and computer networks in the routine course of business may alter or destroy existing data, but a data preservation order prohibiting operation of the computers absolutely would effectively shut down the responding party’s business operations. . . . Routine system backups for disaster recovery purposes may incidentally preserve data subject to discovery, but recovery of relevant data from nonarchival backups is costly and inefficient, and a data-preservation order that requires the accumulation of such backups beyond their usual short retention period may needlessly increase the scope and cost of discovery.

Manual for Complex Litigation (Fourth) § 11.442 at 73 (Federal Judicial Center 2004).

Judge Scheindlin’s solution is:

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company’s policy. On the other hand, if backup tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of ‘key players’ to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* backup tapes.

*Zubulake IV*, 220 F.R.D. at 218 (emphasis in original).

The proposed amendments build on these obligations without adopting them by requiring the parties “to discuss any issues relating to preserving discoverable information” during the Rule 26(f) planning conference. The proposed Advisory Committee Note to Rule 26 suggests that “[t]he parties’ discussion should aim toward specific provisions, balancing the need to preserve relevant evidence with the need to continue routine activities critical to ongoing business.” Amendments, at 19. Such a discussion might include whether a party has a duty to preserve electronically stored information that is not reasonably accessible.

The Section endorses these provisions. Early attention to preservation of dynamic electronically stored information is a necessity to avoid later misunderstanding, unnecessary motion practice and potential sanctions.

A party that fails to preserve, significantly alters or destroys evidence in pending or reasonably foreseeable litigation has committed spoliation. *Zubulake V*, 2004 WL 1620866, at \*6. Spoliation may result in sanctions under Rule 37 of the Federal Rules of Civil Procedure where a court order or discovery ruling has been violated or under the court’s inherent power to impose sanctions for abuse of the judicial system. *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at \*3 (N.D. Ill. Oct. 27, 2003), *aff’d*, 2004 WL 1895122 (N.D. Ill. Aug. 10, 2004). Sanctions may be imposed for spoliation of relevant evidence when a party acts with a culpable state of mind (from negligence to intentional), although the appropriate sanction may depend on the level of culpability. *See, e.g., Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002); *Silvestri*, 271 F.3d at 590, 593; *Marrocco v. General Motors Corp.*, 966 F.2d 220, 224 (7th Cir. 1992); *Advantacare Health Partners, LP v. Access IV*, No. C 03-04496 JF, 2004



WL 1837997, at \*4 (N.D. Cal. Aug. 17, 2004); cf. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 47 (1991).

Without addressing the standard for the imposition of sanctions for spoliation, new proposed Rule 37(f) seeks to provide a “safe harbor” from sanctions for a failure to produce electronically stored information lost after the commencement of the case.<sup>16</sup> The proposal of the majority of the Civil Rules Advisory Committee is that, unless a party violates a court order requiring preservation, a court may *not* impose sanctions if: “(1) the party took *reasonable steps* to preserve the information after it knew or should have known the information was discoverable in the action; and (2) the failure resulted from loss of the information because of the *routine operation* of the party’s electronic information system.” (Emphasis added.) The proposal of a minority of the Civil Rules Advisory Committee is that a court may *not* impose sanctions “for failing to provide electronically stored information deleted or lost as a result of the *routine operation* of the party’s electronic information system unless: (1) the party *intentionally or recklessly* failed to preserve the information; or (2) the party violated an order issued in the action requiring the preservation of the information.” (Emphasis added.)

The proposed Advisory Committee Note acknowledges that “routine operation” is undefined. “No attempt is made to catalogue the system features that, now or in the future, may cause such loss of information. Familiar examples from present systems include programs that recycle storage media, automatic overwriting of information that has been ‘deleted,’ and programs that automatically discard information that has not been accessed within a defined period.”

Amendments, at 34. Although any definition of “routine operation” may become obsolete as

---

<sup>16</sup> The proposed Advisory Committee Note acknowledges that proposed Rule 37(f) does not address the loss of electronically stored information before an action is commenced. Amendments, at 34. However, we expect the proposed rule to be persuasive authority regarding any spoliation sanction for such a loss.

technology and office practices change, the Section recommends that the Advisory Committee Note describe some factors that might be considered in establishing what is the “routine operation” of an electronic information system. Factors for a court to consider in determining what is the routine operation of an electronic information system might include: (i) the manner in which the electronic information system (both software and hardware) handles electronically stored information, (ii) any difficulties in modifying the electronic information system to halt operations that might alter or destroy electronically stored information, (iii) whether some portion of the electronic information system is designed to alter or destroy information potentially relevant to litigation, *see Kucala Enter., Ltd. v. Auto Wax Co.*, No. 02 C 1403, 2003 WL 22433095, at \*3 (N.D. Ill. Oct. 27, 2003) (use of Evidence Eliminator software basis for sanctions for spoliation); (iv) any policies of the entity regarding preservation, alteration or destruction of electronically stored information outside the context of anticipated or actual litigation, and (v) any policies of the entity regarding preservation, alteration or destruction of electronically stored information once potential litigation is known.

While there is some concern that a safe harbor will encourage parties not to preserve relevant electronically stored evidence, the Section endorses the safe harbor proposed by a majority of the Advisory Committee. It may help to identify sanctionable, culpable conduct by providing an objective standard against which the alteration, loss or destruction of electronically stored information may be measured.

The minority’s proposal contains a gap between information lost as a result of the routine operation of an electronic information system (within the safe harbor), and a reckless or intentional failure to preserve information (outside the safe harbor). The majority’s proposal clearly places actions in the gap outside the safe harbor, as they should be. For example, in *Zubulake IV*, the court

imposed a less than draconian sanction of paying for additional depositions where the responding party could only be shown to be negligent or possibly reckless in preserving electronically stored information. *Id.*, 220 F.R.D. at 221, 222. However, the additional depositions led to the discovery that the party's personnel had acted willfully in destroying potentially relevant electronically stored information, which led to further, more serious sanctions. *Zubulake V*, 2004 WL 1620866, at \*12. This example shows that precluding the imposition of appropriate Rule 37 sanctions in the absence of willful or reckless conduct, as the minority proposes, may unduly restrict courts from supervising and controlling discovery and deterring or punishing willful spoliation of electronically stored information.

In addition, the majority's proposal applies an objective standard, which could be tied into the routine operation of an entity's electronic information system and steps that should be taken in light of the nature of that system and any policies the entity has adopted for the preservation of electronically stored information. The minority's proposal applies a subjective standard, which may require a greater collateral inquiry into the actions of the entity and its personnel in failing to preserve electronically stored information. That inquiry may well be hindered by invocations of the attorney-client privilege. *See Keir v. UnumProvident Corp.*, No. 02 Civ. 8781 (DLC), 2003 WL 21997747, at \*11 n.3 (S.D.N.Y. Aug. 22, 2003) ("UnumProvident invoked its attorney-client privilege to protect most of its communications concerning the issues addressed at the hearing" on UnumProvident's failure to preserve six days of e-mails). Moreover, the minority's standard may encourage greater disregard for an entity's obligation to preserve electronically stored information, which recent case law shows already is not taken as seriously as it ought to be regarding e-mails. *See Zubulake V*, 2004 WL 1620866, at \*3 ("[n]otwithstanding the clear and repeated warnings of counsel, Zubulake has proffered evidence that a number of key UBS employees . . . failed to retain

e-mails germane to Zubulake's claims"); *United States v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21, 24 (D.D.C. 2004) ("it is astounding that employees at the highest corporate level in Philip Morris, with significant responsibilities pertaining to issues in this lawsuit, failed to follow Order # 1, the document retention policies of their own employer, and, in particular, the 'print and retain' policy which, if followed, would have ensured the preservation of those emails which have been irretrievably lost"); *Rambus, Inc. v. Infineon Technologies AG*, 220 F.R.D. 264, 287 (E.D. Va. 2004) ("Infineon has presented evidence that, taken together, rather strongly indicates that Rambus explicitly linked development of its document retention policy and the shredding of documents with preparing for patent litigation").

#### **VIII. Protection Against Waiver Of Privilege**

Proposed Rules 26(b)(5)(B) and 45(d)(2)(B) add provisions regarding the inadvertent production of privileged information. They are not limited to electronically stored information. The proposed Rules, with the language of Rule 26(b)(5)(A) in brackets where different, provide:

When a person [party] produces information *without intending to waive* a claim of privilege it may, within a *reasonable* time, notify any party that received the information of its claim of privilege. After being notified, any [a] party must promptly *return, sequester, or destroy* the specified information and any copies. The person who produced the information [The producing party] must comply with Rule 45(d)(2)(A) [26(b)(5)(A)] with regard to the information and preserve it pending a ruling by the court.

(Emphasis added.)

The proposed Advisory Committee Note to Rule 26 describes some of the factors that might bear on whether notice was given within a reasonable time: (1) the date when the producing party learned of the production of the information, (2) the extent to which other parties had made use of the information in connection with the litigation, (3) the difficulty of discerning whether the

material was privileged, and (4) the magnitude of the production. Amendments, at 15. These factors appear to be appropriate.

The proposed Advisory Committee Note states that the option of sequestering information was provided “because the receiving party may have incorporated some of the information in protected trial-preparation materials.” *Id.*, at 16. While sequestration straightforwardly applies to hard-copy documents (separate filing with a confidential annotation), it may less straightforwardly apply to electronically stored information, which could reside on storage media with a great deal of other information from which it cannot easily be separated. Further, such electronically stored information may not be able to be “destroyed,” but only to have a pointer to it “deleted.” In any event, the concept that some inadvertently disclosed information may be retained by the party to whom such disclosure is made under an obligation not to make any further use or disclosure, at least pending resolution of its status, is one that the Section approves.

The proposed Advisory Committee Note goes on to state that, “[a]fter receiving notice, a party must not use, disclose, or disseminate the information pending resolution of the privilege claim.” *Id.* The Section suggests that this obligation be stated in the proposed Rule, not just in the Advisory Committee Note. While the Advisory Committee Note does not so state, the Section presumes that the party receiving the notice can use the information on any motion seeking resolution of the privilege claim, although any filing should probably be under seal. *Cf.* The Association of the Bar of the City of New York, Committee on Professional and Judicial Ethics, Formal Opinion No. 2003-04, 2004 WL 837937, at \*4, \*7 (April 9, 2004) (lawyer has ethical obligations to notify, return and refrain from review of inadvertent disclosures of privileged information, except to bring to a tribunal’s attention that the communication does not contain privileged information or that any privilege has been waived by the disclosure); New York County

Lawyers' Association Committee on Professional Ethics, "Topic: Ethical Obligations Upon Receipt of Inadvertently Disclosed Privileged Information," NYCLA Ethics Opinion No. 730, 2002 WL 31962702, at \*4 (July 19, 2002) (a lawyer receiving information the lawyer knows or believes was not intended for the lawyer and contains secrets, confidences or other privileged matter, upon recognition of same, shall, without further review or other use, notify the sender and abide by the sender's instructions regarding return or destruction of the information).

The proposed Advisory Committee Note also imposes on the party receiving the inadvertently disclosed information the obligation to attempt to obtain the return of the information or its destruction by any non-party to whom previous disclosure had been made. Amendments, at 16. This obligation flows from an attorney's obligation not to engage in conduct prejudicial to the administration of justice, ABA Model Rules of Professional Conduct Rule 8.4(d); New York, New York Disciplinary Rule 1-102(A)(5); *cf. American Express v. Accu-Weather, Inc.*, No. 91 Civ. 6485 (RWS), 92 Civ. 705 (RWS), 1996 WL 346388, at \*2 (S.D.N.Y. June 25, 1996) (ethical violation of DR 1-102(A)(5) to open Federal Express package after notice that it inadvertently contained a privileged document).

The Report (at 14) asks whether a party that receives notice that privileged material has been produced must certify that the material has been sequestered or destroyed, if it is not returned. The Section believes that such an obligation is unnecessary, particularly if the obligation not to use the information after notice is stated in the Rule. Further, since attorneys have an ethical obligation not to use privileged information that has been inadvertently disclosed but remains privileged, a certification requirement will not add any deterrence nor will it likely result in any additional punishment if flouted. Moreover, if the question of whether the information should or should not

be privileged will be decided by a court, then certification of sequestration or destruction is premature until that decision is made.

In addition, as discussed above, for information that resides on storage media where it cannot be easily separated from other information, it may be difficult to certify to any statement other than that the information will not be used, disclosed or disseminated except in conjunction with a motion to establish whether it is privileged or not. Such a restatement of a party's obligations under the proposed Rule does not seem worthwhile.

The proposed Rules take no position on the split in the federal courts about whether an inadvertent production should be considered a waiver of privilege, and the proposed Rules probably could not do so in light of Rule 501 of the Federal Rules of Evidence.<sup>17</sup> See *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989) (inadvertent disclosure a waiver); *Alldread v. City of Grenada*, 988 F.2d 1425, 1433-34 (5th Cir. 1993) (balancing test applied to determine whether inadvertent production waived privilege); *Local 851 Int'l Brotherhood of Teamsters v. Kuehne & Nagel Air Freight*, 36 F. Supp. 2d 127, 131 n.4 (E.D.N.Y. 1998) (failure to take reasonable steps waives the attorney-client privilege); *Berg Electronics Inc. v. Molex, Inc.*, 875 F. Supp. 261, 263 (D. Del. 1995) (inadvertent production not a waiver); *Mendenhall v. Barber-Green Co.*, 531 F. Supp. 951, 954 (N.D. Ill. 1982) (inadvertent production not a waiver of the attorney-client privilege); *but cf. In re Lernout & Hauspie Sec. Litig.*, 222 F.R.D. 29, 34 (D. Mass. 2004) (production of e-mail found not inadvertent).

---

<sup>17</sup> Under Rule 501, federal district courts are required to apply state law choice-of-law principles to determine which privilege law to apply in diversity cases. See *CSX Transp. v. Lexington Ins. Co.*, 187 F.R.D. 555, 559 (N.D. Ill. 1999) (applying Illinois privilege law rather than the Florida law governing the underlying dispute); *Tartaglia v. Paul Revere Life Ins. Co.*, 948 F. Supp. 325, 326-27 (S.D.N.Y. 1996) (applying New York privilege law to diversity case where Ohio law would otherwise apply).

Nonetheless, proposed Rules 16(b)(6) and 26(f)(4) and Form 35, ¶ 3, encourage the parties to discuss at their discovery conference and seek to include in the court's case management order a provision protecting the right to assert a privilege after an inadvertent production of information. In the Section's view, these provisions implicitly, but correctly, endorse the position that the inadvertent production of privileged information, especially when dealing with voluminous electronically stored information, should not automatically be considered a waiver of privilege. The Section concurs with the proposed Advisory Committee Note (Amendments, at 19) that frequently, especially in complex cases, parties spend large, and perhaps inordinate, amounts of time reviewing hard-copy discovery materials prior to production to determine whether they are privileged, which can substantially delay access for the party seeking discovery. *See Zubulake III*, 216 F.R.D. at 290 (the producing party decided on a review protocol of having a senior associate at a cost of \$410 per hour read every word of every document rather than having a paralegal at a cost of less than \$170 per hour conduct a series of targeted key-word searches). As the proposed Advisory Committee Note also describes (Amendments, at 20), the time and expense to review electronically stored information can be greater than with hard-copy documents, because there is more of it, including many duplicates, and the informal nature of many e-mails makes it more difficult to determine whether the information is privileged.<sup>18</sup> *See Computer Assocs. Int'l Inc. v. Quest Software, Inc.*, No. 02 C 4721, 2003 WL 21277129, at \*1 (N.D. Ill. June 3, 2003) (cost to remove privileged information from eight hard drives between \$28,000 to \$40,000); *Medtronic Sofamor Danek, Inc. v.*

---

<sup>18</sup> The proposed Advisory Committee Note also indicates that a privilege review of embedded data may be more difficult because of its hidden nature and suggests the same may be true regarding metadata. Amendments, at 20. While the Section agrees that embedded data, containing draft language, editorial comments and other deleted matter, may need to be reviewed for privilege independent of the electronic document to which it relates, the Section suggests that metadata, that is, information describing the history or management of an electronic document, will rarely be privileged if the document is not otherwise privileged, making a privilege review of metadata in most instances superfluous.



*Michelson*, No. 01-2373-MIV, 2003 WL 21468573, at \*7 (W.D. Tenn. May 13, 2003) (estimates of privilege review costs regarding backup tapes between \$16.5 million and \$70 million); *Cognex Corp. v. Electro Scientific Indus., Inc.*, No. Civ. A 01CV10287RCL, 2002 WL 32309413, at \*2 (D. Mass. July 2, 2002) (a seven-person team of lawyers and paralegals took approximately 10 weeks of work to review eight CDs of electronic files).

The Report, at 14, asks whether proposed Rule 26(f)(4) should be less restrictive so as to include “any issues relating to the protection of privileged information in discovery,” rather than the “agreement of the parties . . . protecting the right to assert privilege after production of privileged information.” The Section is uncertain what additional issues would be encompassed within the less restrictive formulation that would not be encompassed within the current proposal.

Accordingly, the Section is indifferent as to which formulation the Advisory Committee adopts.

#### CONCLUSION

The time has come for the Federal Rules of Civil Procedure to foster a uniform approach to discovery of electronically stored information. The amendments proposed by the Advisory Committee represent significant progress in achieving that goal. However, the Section recommends, among other things, that:

- (1) greater guidance be provided or perhaps the language be changed regarding the production under proposed Rule 34(b) of electronically stored information in native format and in electronically searchable form;
- (2) the Advisory Committee Note to Rule 26 state that accessibility be determined by the steps needed to be taken for electronically stored information to be usable;

(3) proposed Rules 26(b)(5)(B) and 45(d)(2)(B) include a statement of the obligation not to use, disclose or disseminate information once notified that it has been inadvertently produced and is privileged; and

(4) there be inserted into the Advisory Committee Note for Rule 37 an explanation of the factors to be used to decide what is the routine operation of an electronic information system for purposes of determining whether a person is within a safe harbor from a sanction for spoliation of electronically stored information.

December 15, 2004

New York State Bar Association  
Commercial and Federal Litigation Section

Committee on Electronic Information

Adam Cohen, Chair  
Kevin Barr  
Robert Carangelo  
Melissa Carvalho  
Will Cruse  
Samantha Fisherman  
Eric Friedberg  
Peter Goodman  
Patricia Harley  
David Lender  
James Lerner  
Gregory McPolin  
Jeffrey Weingart  
Ling Zhong

Committee on Federal Procedure

Gregory K. Arenson, Chair  
Scott A. Barbour  
Robert E. Bartkus  
Ernest T. Bartol  
James A. Beha, III  
Leonard Benowich  
Howard E. Berger  
William J. Brennan  
Mark Budoff  
Larissa A. Cason  
John P. Coll, Jr.  
Robert J. Dinerstein  
Neil P. Forrest  
Margaret J. Gillis  
Richard E. Hahn  
Alan A. Harley  
Richard K. Hughes  
Martin E. Karlinsky  
Madeline Kibrick Kauffman  
Thomas J. Kavalier  
Patrick A. Klingman  
Mitchell A. Lowenthal  
Thomas McGanney  
Michael R. McGee  
Susan L. Meekins

Charles E. Miller  
James F. Parver  
Allan M. Pepper  
Shawn Preston Ricardo  
Stephen T. Roberts  
Michael I. Saltzman  
Doreen A. Simmons  
Alexander R. Sussman  
Elizabeth S. Watson  
David H. Wilder  
Eric C. Woglom  
Scott H. Wyner