

Volume 10, Number 4
April 2006

DROWNING IN *ZUBULAKE*:
THE RULES, PITFALLS,
AND BENEFITS OF
ELECTRONIC DISCOVERY

GEOFFREY A. VANCE
COURTNEY INGRAFFIA BARTON

PREFACE

The topic of electronic discovery, or “e-discovery,” is an incredibly hot topic—both in the mainstream news and in the public courtroom. Indeed, late last year, *U.S.A. Today* ran an article, entitled “E-mail becoming crime’s new smoking gun,” in which the author reported, “e-mail messages and electronic files are a treasure trove of evidence.” Recognizing the importance of e-mail and other electronic information as substantive evidence in a lawsuit, the legal community has placed an increasing emphasis on demanding electronic files to be produced during the pretrial discovery process. At the same time, a number of state and federal judges have imposed severe penalties on litigants who did not do what they were supposed to do with respect to the preservation and production of relevant electronically stored information.

This month’s Briefly is intended to give you a basic understanding of what the commotion related to e-discovery is all about. Its authors, Geoffrey A. Vance and Courtney Ingraffia Barton, provide a synopsis of the difficulties, hazards and benefits associated with electronic discovery. Mr. Vance and Ms. Barton also provide an outline of the e-discovery rules in civil litigation, including a discussion of the proposed amendments of the Federal Rules of Civil Procedure that are intended specifically to address e-discovery issues, and a recitation of some lessons to be learned from a number of judges’ published opinions. The goal of this month’s Briefly monograph is to put you, the reader, in a better position to navigate the sometimes choppy e-discovery waters. I am hopeful that this Briefly achieves that goal.

As with all other publications of the National Legal Center, this month’s Briefly monograph is presented to encourage a greater understanding of an important legal issue. The views expressed in the monograph are those of the authors and do not necessarily reflect the opinions of the advisors, officers, or directors of the Center. This monograph is for general information and should not be used as a substitute for timely legal consultation on a specific matter.

Richard A. Hauser
President
National Legal Center

Volume 10, Number 4
April 2006

**DROWNING IN *ZUBULAKE*:
THE RULES, PITFALLS,
AND BENEFITS OF
ELECTRONIC DISCOVERY**

**GEOFFREY A. VANCE
COURTNEY INGRAFFIA BARTON**

© 2006 National Legal Center
for the Public Interest
ISSN 1089-9820
ISBN 0-937299-46-4
ISBN 1-930742-73-8
Published April 2006

**NATIONAL LEGAL CENTER
FOR THE PUBLIC INTEREST**

1600 K Street, N.W., Suite 800
Washington, D.C. 20006
Tel: (202) 466-9360
Fax: (202) 466-9366
E-mail: info@nlcpi.org
Please visit our Web site at: www.nlcpi.org

The National Legal Center for the Public Interest is a tax-exempt, nonprofit public interest law and educational foundation, duly incorporated under the law of the District of Columbia to provide nonpartisan legal information and services to the public at large. NLCPI is qualified to receive tax-deductible contributions under I.R.C. Sec. 501(c)(3).

TABLE OF CONTENTS

PREFACE

RICHARD A. HAUSER Inside Front Cover

DROWNING IN *ZUBULAKE*: THE RULES, PITFALLS AND BENEFITS OF ELECTRONIC DISCOVERY

GEOFFREY A. VANCE

COURTNEY INGRAFFIA BARTON

INTRODUCTION 1

PART I:

DIFFERENCES BETWEEN ELECTRONIC

AND PRINTED INFORMATION 3

A. Definition of an Electronic Document 3

B. Differences 3

1.E-mails and Other E-Documents Are Informal 4

2.Electronic Documents Include Metadata 4

3.Electronic Documents Are Multiplying Exponentially ... 5

4.Computer Information Is Everywhere 6

5.Computer Information Is Dynamic 7

6.Electronically Stored Information Is Not Always

Readily Usable or Accessible 7

PART II:

COMMON E-DISCOVERY MISTAKES 8

PART III:

THE *ZUBULAKE* OPINIONS 9

A. *Zubulake* Background 9

B. *Zubulake* I and III 10

C. *Zubulake* IV 11

D. *Zubulake* V 13

E. *Zubulake* Verdict 15

PART IV:

OTHER E-DISCOVERY FAILURES IN 2005 16

A. Morgan Stanley 16

B. Other Sanctions Cases in 2005 17

TABLE OF CONTENTS

C. Lesson Learned: Document Retention is King	19
D. Litigation Holds and the Obligation of Outside Counsel . .	20
PART V:	
PROPOSED AMENDMENTS TO THE FEDERAL RULES	
OF CIVIL PROCEDURE	22
A. Discoverability of Electronically Stored Information: Changes to Rule 26(a)(1)(B), Rule 34(a), and Rule 45 . . .	23
B. “Meet and Confer”: Changes to Rules 26(f) and 16(b) and Form 35	24
C. Discovery of Information that Is “Not Reasonably Accessible”: Changes to Rules 26(b)(2)(B) and 45(d)(1)(C)	25
D. Inadvertent Production and Waiver of Privilege: Changes to Rules 26(b)(5) and 45(d)(2)(B)	27
E. Form of Production: Changes to Rules 34 and 45	27
F. Safe Harbor from Sanctions: Changes to Rule 37	29
G. Effect of Proposed Amended Rules	30
PART VI:	
BENEFITS OF E-DISCOVERY	30
PART VII:	
CLOSING THOUGHTS	31
ABOUT THE AUTHORS	33
THE MISSION OF THE	
NATIONAL LEGAL CENTER	Inside Back Cover

DROWNING IN *ZUBULAKE*: THE RULES, PITFALLS, AND BENEFITS OF ELECTRONIC DISCOVERY

**GEOFFREY A. VANCE
COURTNEY INGRAFFIA BARTON**

INTRODUCTION

Over the course of two years, the Honorable Shira A. Scheindlin of the U.S. District Court for the Southern District of New York issued a series of opinions in that helped provide much needed clarity on the topic of discovery of electronically stored information. These opinions, entered in a case captioned *Zubulake v. UBS Warburg LLC*, include a discussion of the obligations imposed on litigants who maintain electronic information and the considerable sanctions a court may impose on litigants who do not follow the electronic discovery rules.

Judge Scheindlin's discussion of the severe, case-changing electronic discovery penalties sent shock waves across the legal industry and beyond. It seemed to confirm what conventional wisdom had taught: electronic discovery involves a complicated maze of unanswered questions with potentially disastrous consequences. *Zubulake* made the message seem even more clear: a case can be *lost* and a client's exposure can *skyrocket* because of a *lawyer's* innocent ignorance and mistakes in electronic discovery.

Digesting all the information in the *Zubulake* opinions and their progeny appears a daunting task for lawyers who are not experienced in dealing with electronic data. Even those well versed in the case law likely feel they are drowning in the *Zubulake* rules.

But take heart: there are life preservers out there. Electronic discovery, or "e-discovery" as it has come to be known, while different from the production of paper files, is not *that* different. There are certainly a few intimidating pitfalls associated with the preservation and production of electronic data; however, e-discovery involves the same fundamental concepts and rules that apply to the discovery of printed files. Courts (like the Southern District of New York) and

commentators (like Judge Scheindlin)¹ are beginning to articulate and clarify the rules that apply to the discovery of electronically stored information. Because of others' misfortunes (like the defendant and lawyers in the *Zubulake* case), the definitions of responsibilities of outside counsel are becoming more concrete, and, in turn, the penalties associated with e-discovery failures are becoming more predictable and consistent in their application.

Regrettably, what is often lost in a broader e-discovery discussion is that there are some significant advantages to dealing with information stored electronically rather than in hard copy. Usually, electronic materials are much easier and cheaper to search, identify, and produce, and the relevant data therein can more easily be reviewed, searched, and located after production.

The purpose of this monograph is to explain some of the principal rules, pitfalls and benefits of e-discovery in order to remove the mystery of this relatively new aspect of litigation. We have divided this monograph into seven parts:

Part I defines the term "electronic document" and explains the differences between electronically stored information and printed materials.

Part II describes the most common mistakes made in e-discovery, including the unknowing failure to talk to the right people about the right things at the right time.

Part III explains the background and teachings of the *Zubulake* series of opinions, which are the first such series to establish a comprehensive set of rules within the federal system.

Part IV continues the discussion initiated by Judge Scheindlin in her *Zubulake* opinions and addresses what happened to other litigants who failed to preserve and produce relevant electronically stored information in the course of discovery.

Part V discusses the proposed changes to the Federal Rules of Civil Procedure that relate to e-discovery, which the authors anticipate are likely to be approved by the U.S. Supreme Court and Congress sometime in 2006.

¹ Judge Scheindlin is a frequent speaker and author on e-discovery issues. *See, e.g.,* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327 (2000).

Part VI steers away from the general “doom and gloom” debate surrounding e-discovery; rather, we illustrate the considerable value of electronically stored information in litigation.

Part VII offers our closing remarks.

**PART I:
DIFFERENCES BETWEEN ELECTRONIC
AND PRINTED INFORMATION**

We begin the dialogue about e-discovery with a discussion of what constitutes an electronic “document,” and continue with the important differences between electronically created and stored materials and printed copies.

A. Definition of an Electronic Document

An “electronic document” is *anything* that was created electronically or converted to an electronic format that is stored *in any electronic form and in any electronic format*. Obvious examples include e-mails and word processing documents created in Microsoft Word and Corel WordPerfect software. These examples are just the beginning of a long and ever-growing list of electronic data that includes that which is housed in BlackBerries™, memory sticks (also known as thumb drives), voice-mail systems, laser printers, and instant messaging software. Electronic “documents” are everywhere.

B. Differences

The differences between hard copy documents and electronically stored information are too extensive to list here. Nonetheless, within the context of litigation there are six principal differences a lawyer should understand in order to participate effectively and appropriately in the e-discovery process.

1. E-mails and Other E-Documents Are Informal

The first difference relates to the fundamental character of electronic materials. Electronically transmitted information, such as e-mails and comments inserted into word processing documents, are generally much more informal in nature than their hard copy counterparts. As a

result, these types of information often contain content that might not have been placed on a sheet of paper. E-mails, for example, are often typed and sent in seconds without the appropriate time devoted to proofreading, spell-checking, and revision. Because e-mails are often sent as cryptic responses to other e-mails,² the responses by themselves are frequently ambiguous and can be misconstrued when taken out of context. “Tongue in cheek” or controversial comments are much more likely to be put into an e-mail than onto a company’s letterhead. The informality of e-mails is likely the reason so many “smoking gun” documents are in the form of e-mails as opposed to more formal letters or memoranda.

2. Electronic Documents Include Metadata

There is more to electronic documents than meets the eye. Clearly, data on a hard copy document is displayed visually on the printed surface. “Not so with an electronic document. Electronic documents carry their history with them”³ through metadata. *Meta* is Greek for “about” or “beyond.” Thus, put simply, metadata is embedded, electronically stored information⁴ describing the history and use of a “document.”

Metadata shows who created, sent, received, and forwarded e-mails; similarly, it shows who created and modified word processing files. Metadata also reveals when files are created, changed, and distributed as well as the importance values (“high,” “normal,” or “low”) and sensitivity values (“normal” or “confidential”) that the author assigned to a particular e-mail or other material.⁵

² The widespread use of e-mail and instant messaging systems spawned an entirely new “e-vocabulary,” including expressions such as “LOL” (laughing out loud in the U.S., and lots of love in the U.K.), “IMO” (in my opinion), and “BRB” (be right back).

³ Scott Nagel, *Embedded Information in Electronic Documents; Why Meta Data Matters*, LAW PRACTICE TODAY, July 2004.

⁴ The seminal case discussing the significance of metadata is *Williams v. Sprint*, 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005).

⁵ Microsoft provides a list on its Web site of some examples of metadata that can be stored in a document. Such metadata can include your name, initials, company, document revisions, document versions, hidden text, and comments embedded in the documents. See <<http://office.microsoft.com/en-us/assistance/>

Metadata is important in the context of discovery⁶ for at least three reasons. First, it includes information that is not generally shown in a printout of an e-mail or word processing document. Second, it includes information that can be lost even though the printout is saved. Third, court opinions and other anecdotal evidence show that metadata is not generally reviewed by the producing party prior to the production of the documents in which it is embedded,⁷ which can lead to a waiver of privilege.

3. Electronic Documents Are Multiplying Exponentially

This leads to a third difference between e-documents and hard copies—the sheer volume of data involved in electronically stored information is overwhelming. The explosion of data is the result of two related principal causes: it is much cheaper to store electronic data; and data is now principally generated and transmitted electronically.

Electronic data is cheap to store and getting cheaper every day. A single compact disc (CD) can store more than 50,000 pages of information. A digital video disc (DVD) can store more than 500,000 pages. A 40-gigabyte hard drive, small by today's standards, can hold more than 3,000,000 pages of information.

HA010776461033.aspx>. Metadata in a Microsoft document can be viewed easily by selecting “Properties” from the “File” menu at the top of the document; however, it might not be so easily revealed in other applications.⁶ Lawyers must also be cognizant of metadata in their own documents, particularly now that word processing documents created electronically may also be filed electronically. The New York State Bar Association Committee on Professional Ethics issued an opinion concluding that attorneys owe their clients a duty to limit the improper disclosure of metadata so that they do not reveal a client's confidential information. N.Y.S.B.A. Op. No. 782 (Dec. 8, 2004).

⁷ Metadata made national mainstream news when the *New York Times* reported “an unsigned Microsoft Word document [about then-U.S. Supreme Court nominee and current Associate Justice Samuel A. Alito, Jr.] was circulated by the Democratic National Committee.” Tom Zeller, Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. TIMES, Nov. 7, 2005. The metadata in the DNC Word document showed precisely who wrote the memo and when it was written. *Id.*

Business critical information is stored almost exclusively in electronic form. E-mail is now the primary form of business communication, and the volume of data involved is staggering. Microsoft Corporation alone receives between 25 million and 30 million e-mails *every day*.⁸ Trillions of e-mail messages are sent and received in the business community each year. Conversely, in this time when businesses are aiming to be entirely paperless, the number of printed documents has declined substantially while the electronic data maintained by our clients has increased and will continue to increase exponentially.⁹

4. Computer Information Is Everywhere

Fourth, printed copies of paper documents are generally stored by the people that sent and received them. The same is true for computer information. However, computer information is also stored in numerous other places. For example, one e-mail can reside on your desktop computer (probably in multiple folders, including the “sent” folder), your assistant’s desktop computer, the recipients’ computers, your company’s server and the recipients’ servers, everybody’s laptop, the BlackBerry devices of everyone who received a copy and on one or more backup tapes maintained by your company and everyone else’s. Similarly, a word processing document can be stored in different places and in entirely different formats. A single file could be saved on your personal hard drive, a shared network drive, a thumb drive, and in an e-mail that you circulated to your colleagues. That same word processing document can be saved as a Microsoft Word (.doc) file, a text (.txt) file, an imaged (.pdf or “TIFF”) file, and a converted WordPerfect (.wpd) file. It can also be compressed, or “zipped,” through the use of other software. All these documents may contain different metadata and other information that make each file slightly different and, thus, independently discoverable..

5. Computer Information Is Dynamic

⁸ *E-Discovery By the Numbers*, CORPORATE COUNSEL, Oct. 12, 2005.

⁹ As a result of the explosion of electronic data, e-discovery lawyers and vendors often discuss data in terms of “terabytes” rather than “megabytes and “gigabytes.” A single terabyte consists of approximately 50 million pages of information (50,000 trees reduced to paper), compared with a megabyte, which consists of approximately 500 pages (an average-size novel) of information.

Next, electronically stored information, unlike hard copies, can include “living,” dynamic data. Information can be altered with a simple keystroke or without any action at all. Plugging a drive to a computer will likely cause the operating system automatically to start making changes to certain files. Word processing documents include fields (such as date and time fields) that are automatically populated when they are retrieved.

6. Electronically Stored Information Is Not Always Readily Usable or Accessible

Finally, electronically stored information is not always “usable” even when preserved. Try opening a Microsoft Word document from the Corel WordPerfect program without using any conversion software. Try opening a complex database with Microsoft PowerPoint software. Unlike paper documents, computer data generally requires a specific system or software for comprehension.

Moreover, some files that are “usable” are not readily accessible when stored. Information stored on disaster recovery backup tapes, for example, is not generally saved in any organized manner. The “backup” information (kept mainly for disaster recovery purposes) is usually compressed and stored in a manner that allows for the most amount of information to be stored in the smallest amount of space.¹⁰ As a result, restoring backup tapes can be a very expensive and lengthy process.

PART II: COMMON E-DISCOVERY MISTAKES

¹⁰ Computer files are also different because they are not easily deleted from storage media. A person who “deletes” a file from their hard drive, for example, does not usually remove the file from the drive but, rather, erases the file from the drive’s directory. In time, the computer may allow another file to be saved over the previous file. However, the previous file would generally remain recoverable unless and until it is overwritten. Moreover, the fact that a person deletes an e-mail from his or her own computer does not typically mean that he or she has deleted that e-mail from the company’s server or from any backup tapes maintained by that company.

It is important to keep in mind the differences between e-documents and hard copies throughout the course of any litigation. The failure to heed these differences can, in some cases, result in massive discovery costs, particularly because the same information may be stored in many locations and in many nonidentical forms. Even more terrifying, a lawyer's ignorance of these differences can, and likely will, also result in the unknowing destruction of data.

There are three types of e-discovery mistakes that seem to be the most common in recent litigation. First, lawyers and their clients do not communicate with the appropriate people once the litigation is reasonably anticipated. While all litigators know it is crucial to contact the key people involved in the conduct underlying the litigation, those people are not usually in charge of the retention and destruction of electronic data; information technology (IT) and records retention staff *are*.

Second, even the lawyers and clients that do communicate with the appropriate IT people too often take "no" or "too expensive" for an answer without testing and challenging the response. True, e-discovery can be expensive, but blindly accepting the answers of a person who might think he or she is too busy to assist in e-discovery functions will often lead to the acceptance of inaccurate information, which, in turn, is often conveyed to a court—with disastrous results.

Third, lawyers and their clients often act too late. As discussed above, electronically stored information is dynamic and can change or be destroyed systematically without any action on anyone's part. A failure to communicate with the appropriate people at the appropriate time can be extremely harmful. Unless and until a client representative suspends or modifies an automated destruction policy, a significant amount of relevant information could be irretrievably lost in just a few days or even minutes.

All of these mistakes could lead to the same devastating effect. If you do not preserve the proper information, then you cannot identify and ultimately produce it later. If you cannot produce it, then you cannot use it at trial. And even worse, if you fail to produce it, you may be sanctioned.

PART III: THE *ZUBULAKE* OPINIONS

The failure to recognize the differences between electronic data and hard copies led to the *Zubulake* opinions, which by all accounts are the

first series of judicial opinions in the country where a judge has memorialized and commented on the electronic discovery process from start to finish. The defendant in *Zubulake* made all three of the common mistakes discussed in Part II of this monograph. UBS did not properly communicate with the right people, its lawyers did not challenge the IT personnel's assessments, and UBS neglected to act before electronic data was altered or lost.

A. *Zubulake* Background

Ms. Zubulake, an equities trader, sued her former employer for gender discrimination and unlawful retaliation. In the course of discovery in her lawsuit, Ms. Zubulake asked for “[a]ll documents concerning any communication between UBS employees concerning the plaintiff.” Her employer produced only 100 pages of e-mails, compared with the approximately 450 pages of e-mails that she produced to her employer. The bulk of the e-mails Ms. Zubulake produced were to or from UBS e-mail addresses. Ms. Zubulake contended that UBS's production of e-mails was deficient and insisted her employer review its backup tapes to search for and produce all of the e-mails it neglected initially to produce. The employer refused, forcing Ms. Zubulake to file a motion to compel.

B. *Zubulake* I and III¹¹

Ms. Zubulake's first motion to compel prompted Judge Scheindlin to consider, “To what extent is inaccessible electronic data discoverable, and who should pay for its production?”¹² In *Zubulake* III, Judge Scheindlin concluded that “inaccessible” data, such as archived backup tapes on which information is not stored in a readily usable format, are properly the subject of discovery under the Federal Rules of Civil

¹¹ The opinion known as “*Zubulake* II” did not relate to electronic discovery, but, rather, related to Ms. Zubulake's request to provide securities regulators a copy of the transcript of the deposition of UBS's Manager of Global Messaging. Judge Scheindlin denied that request. *Zubulake*, No. 02 Civ. 1243, 2003 U.S. Dist. LEXIS 7940, at *11 (S.D.N.Y. May 13, 2003).

¹² *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (*Zubulake* I); *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (*Zubulake* III).

Procedure. However, Judge Scheindlin also concluded that seven factors should be applied to determine whether the requesting party (in this case, Ms. Zubulake) should share in the costs associated with restoring the information to a usable form and then searching for and identifying relevant information. These factors, which Judge Scheindlin tailored to “balance the competing needs of broad discovery and manageable costs,” include:

1. The extent to which the request is specifically tailored to discover relevant information.
2. The availability of such information from other sources.
3. The total cost of production, compared to the amount in controversy.
4. The total cost of production, compared to the resources available to each party.
5. The relative ability of each party to control costs and incentives to do so.
6. The importance of the issues at stake in the litigation.
7. The relative benefits to the parties of obtaining the information.¹³

After applying the seven factors, Judge Scheindlin concluded that Ms. Zubulake should pay for 25 percent of the “costs of restoring any backup tapes,” and the employer should pay for 75 percent of the restoration costs as well as “[a]ll other costs” related to the search for and production of responsive data.¹⁴ This appears to be one of the first times a U.S. district judge ruled that backup tapes must be restored and produced and that a requesting party may be forced to pay for some of the restoration and production costs.¹⁵

¹³ 217 F.R.D. at 311, 322.

¹⁴ 216 F.R.D. 280, 292 (S.D.N.Y. 2003).

¹⁵ Prior to the *Zubulake* opinions, several federal magistrate judges, such as U.S. Magistrate Judge James C. Francis IV of the Southern District of New York and U.S. Magistrate Judge John M. Facciola of the District of Columbia, had the opportunity to author opinions that addressed e-discovery disputes. The prevalence of the involvement of U.S. magistrate judges rather than U.S. district judges is likely because of the frequency that discovery disputes are referred to magistrates.

C. *Zubulake IV*

Upon the entry of *Zubulake III*, the employer began the process of restoring its backup tapes. During that process, the parties learned some of UBS's backup tapes were missing and other responsive e-mails had been deleted. This led Ms. Zubulake to file another discovery motion. This time the motion sought a variety of sanctions, including an adverse inference instruction suggesting to jurors that they "can infer from the fact that UBS destroyed certain evidence that the evidence, if available, would have been favorable to Zubulake and harmful to UBS."¹⁶ In response to this motion, Judge Scheindlin issued another opinion and order known as *Zubulake IV*.

Zubulake IV consisted of a two-part analysis. First, Her Honor asked (and then answered) two threshold questions: (1) when must a litigant begin to preserve evidence, including electronic evidence, and (2) what is the scope of a litigant's obligation to preserve inaccessible backup tapes? Judge Scheindlin answered the first question succinctly: "The duty to preserve attached at the time that litigation was reasonably anticipated."¹⁷ The court summarized the answer to the second question as follows:

... 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

¹⁶ 220 F.R.D. 212, 219 (2003).

¹⁷ *Id.* at 217.

should be preserved if the information on those tapes is not otherwise available. This exception applies to all backup tapes.¹⁸

“All” backup tapes included inaccessible backup tapes kept exclusively for disaster recovery purposes.¹⁹

Having found UBS to have failed to preserve backup tapes containing “key players” *after* its duty to preserve arose (thus concluding that spoliation of relevant information had occurred), Judge Scheindlin proceeded to the second part of her two-part analysis to determine whether an adverse inference instruction was appropriate, given the particular circumstances in the *Zubulake* case. To reach that determination, Judge Scheindlin raised two questions: (1) did UBS act negligently²⁰ in destroying the backup tapes, and (2) was the information on those backup tapes relevant to the litigation?

The first question was essentially already answered because Judge Scheindlin had already concluded that UBS had an obligation to preserve, but did not preserve, “key player” backup tapes. This met the classic definition of “negligence.”²¹

Next, the court asked whether Ms. Zubulake had met her burden of showing “that a reasonable trier of fact could find that the missing e-mails [stored on the missing backup tapes] would support her claims.”²² She did not, according to Judge Scheindlin. The “likelihood of obtaining relevant information from the six-plus lost backup tapes is even lower than for the remainder of the tapes.”²³ Moreover, the majority of the e-mails on the tape “most likely to contain relevant e-mails” were also preserved on another tape that UBS had in fact

¹⁸ *Id.* at 218.

¹⁹ *Id.*

²⁰ In the U.S. Court of Appeals for the Second Circuit, the “culpable state of mind” for purposes of an adverse spoliation instruction “includes simply negligence.” *Id.* at 220. Other circuits require a showing of “bad faith,” or intentional conduct. *See, e.g.,* *United States v. Wise*, 221 F.3d 140, 156 (5th Cir. 2000); *Mathis v. John Morden Buick, Inc.*, 136 F.3d 1153, 1155 (7th Cir. 1998).

²¹ *Zubulake*, 220 F.R.D. at 221.

²² *Id.*

²³ *Id.*

produced.²⁴ Thus, Zubulake did not “demonstrate that the lost evidence would have supported her claims.”²⁵ Consequently, Judge Scheindlin concluded that “it would be inappropriate to give an adverse inference instruction to the jury.” Instead, Judge Scheindlin ordered UBS to bear Zubulake’s costs in “re-deposing certain witnesses for the limited purpose of inquiring into issues raised by the destruction of evidence and any newly discovered e-mails.”²⁶

D. *Zubulake V*

UBS did not fare well in the depositions of the five witnesses that Ms. Zubulake’s lawyers re-deposed. Those depositions proved there were even more deleted e-mails than earlier thought, and they also demonstrated there were e-mails remaining on UBS’s active servers that were preserved but had never been produced. Ms. Zubulake filed another motion for an adverse inference instruction. She was more successful this time.

In *Zubulake V*, Judge Scheindlin concluded that “UBS personnel unquestionably deleted relevant e-mails from their computers . . . , even though they had received at least two directions from counsel not to.”²⁷ Having found that “UBS acted willfully in destroying potentially relevant information,” Judge Scheindlin granted Ms. Zubulake’s motion and ordered an adverse inference instruction to be given to the jury.²⁸

Perhaps just as important as the fact that Judge Scheindlin determined an adverse inference instruction was appropriate in light of UBS’s conduct are the comments and conclusions that surrounded the court’s conclusion. Judge Scheindlin held:

1. It is the duty of counsel, including lawyers at a law firm hired by a client, to locate relevant information.
2. Outside counsel have a continuing duty to ensure the preservation of responsive information by communicating directly with “key players” in the litigation and “periodically

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ 229 F.R.D. 442, 429 (S.D.N.Y. 2004).

²⁸ *Id.* at 436-37.

remind[ing]” the client of its continuing obligations to preserve information.

3. The duty to supplement discovery responses “really falls” on a client’s lawyer.
4. Outside counsel are responsible for issuing “litigation hold” notices whenever litigation is reasonably anticipated.
5. Outside counsel “should instruct all employees to produce electronic copies of their relevant active files.”²⁹

The overarching message of Judge Scheindlin in her *Zubulake V* opinion is that the dialogue between lawyer and client regarding the preservation and production of electronically stored information (and all other responsive information) must be a continuing dialogue that begins when a lawsuit is anticipated and runs throughout the lawsuit. *Zubulake V* ended with a word of caution to litigants and their lawyers: “There have been a flood of recent opinions— including a number from appellate courts—and there are now several treatises on the subject Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information.”³⁰

E. *Zubulake* Verdict³¹

On April 6, 2005, more than three years after Ms. Zubulake sued UBS, the jury to whom Judge Scheindlin gave an adverse inference instruction awarded Ms. Zubulake more than \$29 million.

²⁹ *Id.* at 430-35.

³⁰ *Id.* at 440-41.

³¹ Judge Scheindlin issued another opinion, often referred to as “*Zubulake VI*,” between *Zubulake V* and the trial. In *Zubulake VI*, Judge Scheindlin agreed with UBS and held that Ms. Zubulake could not introduce the court’s previous opinions as evidence at trial. 382 F. Supp. 2d 536, 2005 U.S. Dist. LEXIS 4085, at *22 (S.D.N.Y. Mar. 16, 2005). Judge Scheindlin also prohibited Ms. Zubulake from calling UBS’s lawyers as witnesses at trial. *Id.* at *29-*30. However, Judge Scheindlin warned UBS that its introduction of evidence as to whether the failure to preserve or produce information was reasonable would, in turn, open the door to the introduction by Ms. Zubulake of “correspondence between counsel on discovery matters.” *Id.* at *22.

Approximately \$20.1 million of the total verdict was for punitive damages that were very likely related to UBS's destruction of electronic data.³²

**PART IV:
OTHER E-DISCOVERY FAILURES IN 2005**

In the wake of *Zubulake*, 2005 saw similar outcomes in other cases involving the failure to preserve and produce relevant information in the course of discovery. Probably the most notable is *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*,³³ although there are numerous other cases that demonstrate the severe consequences of a party's electronic discovery failures. All of these cases teach valuable lessons that apply to almost all of the various types of litigation.

A. Morgan Stanley

In this case, Coleman (Parent) Holdings (CPH) filed an action against Morgan Stanley alleging conspiracy and aiding and abetting after Morgan Stanley served as CPH's financial adviser in a trans-

³² In his closing argument in support of a punitive damages award, which was given after the jury rendered the compensatory damages verdict, Ms. Zubulake's lawyer discussed UBS's deletion of e-mails as a basis for a punitive damages award:

They can destroy evidence or fail to preserve it in an intentional way. They can cover up, and they can lie. And they think they can get away with it. Not here, not in this city, not in this courthouse, and not before this jury. This misconduct belittles all of us. It should stop. How do you stop it? The law shows the way. And that's through exemplary [punitive] damages. You should make it too costly for this defendant to ever think, ever think about fabricating an employee's records, violating their lawyers' instructions to save evidence, and about taking an oath on that witness stand and not telling you the truth about who was responsible for that termination and who knew about that EEOC complaint.

³³ 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005).

action involving the sale of Sunbeam stock. Sunbeam subsequently went bankrupt. During the discovery process, Morgan Stanley only produced a handful of e-mails to CPH, prompting a motion to compel. In response to that motion, Morgan Stanley asserted the e-mails CPH had requested were housed on backup tapes that would be cost prohibitive to produce. The court then ordered limited backup tape restoration and required Morgan Stanley to certify to the court it had complied with the court's order. Morgan Stanley subsequently produced an additional 1300 pages of e-mails to CPH and ultimately certified to the court it had produced everything.

Several months later, counsel for Morgan Stanley disclosed that, in fact, Morgan Stanley had discovered additional e-mail backup tapes, which would take several more months to restore and search. Thus, the certification to the court was false. It was later found that even the director of IT did not know where all of the potentially relevant information was stored when he testified in court. Once he undertook an investigation, even more tapes were discovered. The court then ordered an adverse inference instruction, which "reversed the burden of proof on aiding and abetting and conspiracy elements and included a statement of evidence of [Morgan Stanley's] efforts to hide its e-mails to be read to the jury as relevant of both [Morgan Stanley's] consciousness of guilt and the appropriateness of punitive damages."³⁴

After the March 1, 2005, order granting the adverse inference instruction, more information came to light about Morgan Stanley's discovery abuses, including the fact that Morgan Stanley "desperately wanted to hide an active SEC inquiry into its e-mail retention practices" and that Morgan Stanley "did not want to admit the existence of the historical e-mail archive, which would expose the false representations it had made to the Court."³⁵ Citing 23 counts of wrongdoing by Morgan Stanley and the fact that the prejudice to CPH "cannot be cured," the court granted CPH's motion for partial default judgment. On May 18, 2005, a jury awarded CPH \$1.4 billion in damages. The court also revoked the *pro hac vice* admission of Morgan Stanley's out-of-state counsel.

B. Other Sanctions Cases in 2005

³⁴ *Id.* at 9.

³⁵ *Id.* at 10.

Other courts in 2005 had been equally unforgiving on issues of spoliation and discovery abuses. In *Advantacare Health Partners v. Access IV*,³⁶ defendants were sanctioned \$20,000 and an adverse inference instruction was ordered after the court found the defendants had deleted thousands of files from their computers after the issuance of a temporary restraining order requiring preservation of evidence.

After these sanctions were imposed, defendants agreed to comply with discovery conditions imposed by the court. Subsequently, it was revealed that at the time the plaintiff's previous motion for sanctions was under submission, defendants returned two hard drives that were wiped clean. Even after the court issued its prior order imposing monetary and evidence sanctions, numerous files were deleted from the defendants' servers and hard drive, and several compact discs were burned on one of the hard drives. In addition to their continued destruction of evidence, the defendants failed to remove all of the plaintiff's proprietary materials from their computers. The court issued an order striking the defendants' answer and entered a default judgment against the defendants. (Similarly, in *Whitehall Specialties v. Delaporte*,³⁷ the court entered a default judgment jointly and severally against the defendants for \$2.2 million after they had failed to produce critical invoices in discovery and changed their story several times about why the invoices did not exist.) In *E*Trade Secrets, LLC v. Deutsche Bank AAG*,³⁸ the court ordered adverse inference instruction because of the defendant's inconsistent preservation of evidence once on notice of litigation. Finally, in *Beck v. Atlantic Coast PLC*,³⁹ the court ordered dismissal of the suit with prejudice and ordered the plaintiff and his counsel to pay \$25,000 to the defendant and \$2500 to the court for failure to turn over key e-mail communications.

Sanctions in 2005 for spoliation and discovery abuses also include unfettered access to computers after failure to preserve evidence (such as in *Ball v. Versar Inc.*),⁴⁰ disallowing the use of certain evidence, allowing additional discovery, and awarding costs and attorneys' fees in producing e-mails due to inadequate searching (e.g., *Lava Trading*,

³⁶ 2005 U.S. Dist. LEXIS 12794 (N.D. Cal. June 14, 2005).

³⁷ 2005 U.S. Dist. LEXIS 4345 (W.D. Wis. Mar. 10, 2005).

³⁸ 2005 U.S. Dist. LEXIS 3021 (D. Minn. Feb. 17, 2001).

³⁹ 2005 Del. Ch. LEXIS 15 (Del. Ch. Feb. 11, 2005).

⁴⁰ 2005 U.S. Dist. LEXIS 24351 (S.D. Ind. Sept. 23, 2005).

Inc. v. Hartford Fire Ins. Co.).⁴¹ For example, in *Ball*, the trial judge held that the defendant was entitled to access to all of the work and home computer systems known to have been used by the plaintiff for the past eight years (so that the defendant's technical consultant could inspect and analyze the data) because the plaintiff did not preserve the e-mails of one of the key players in the case.

On the other hand, in *Jinks-Umstead v. England*,⁴² the court did not sanction a party for missing evidence. There,

the record [did] not support the allegation that defendant is engaging in protracted, calculated attempts to deprive plaintiff of relevant documents. Indeed, the cases plaintiff cites in support of her motion are quite distinguishable from the case at bar because the district courts had found that either: (1) the sanctioned party engaged in clear and willful discovery violations, or (2) a party's document retention policy was so haphazard that it inexcusably denied its opponent potential evidence, severely prejudicing the other party because the destroyed records had been permanently lost.⁴³

C. Lesson Learned: Document Retention Is King

Many lessons can be learned from these cases. Above and beyond the ethical implications, the principal lesson from the *Morgan Stanley* case and other cases is the importance of having a good, comprehensive document retention policy that can be explained and defended in court, if needed. Although Morgan Stanley did have a policy, its policy wasn't thorough enough to point Morgan Stanley in the direction of all of its documents stored in all of their different sites and formats. An effective policy should address not only how documents should be discarded at the end of their business lifetime, but it should also act as a roadmap to where documents are stored and how they should be kept. Essentially, a document retention policy can be used as a litigation preparedness tool as well as a way to decrease considerably a company's exposure.

⁴¹ 2005 U.S. Dist. LEXIS 2866 (S.D.N.Y. Feb. 26, 2005).

⁴² 2005 U.S. Dist. LEXIS 5813, at *20 (D.D.C. Apr. 7, 2005).

⁴³ *Webb v. District of Columbia*, 331 U.S. App. D.C. 23, 146 F.3d 964, 969-71 (D.C. Cir. 1998).

In 2005, document retention policies were endorsed by the U.S. Supreme Court in *Arthur Andersen, LLP v. United States*.⁴⁴ In that case, which reversed the conviction of Arthur Andersen for destroying documents in violation of 18 U.S.C. § 1512 (b)(2)(A) & (B) based on improper jury instructions, the Supreme Court held:

Document retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. . . . It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.⁴⁵

The Supreme Court acknowledged the value of having a reasonable document retention policy as long as it is properly implemented and then suspended if required by law. (Note that in *Zubulake*,⁴⁶ the court stated “A party is under no duty to ‘preserve every shred of paper, every e-mail or electronic document’ and the like.”)

D. Litigation Holds and the Obligation of Outside Counsel

While document retention policies define the general rules for what a company must retain and destroy, those general rules are not without exception. As the Supreme Court acknowledged, the exception can be just as important as the rule. Indeed, it is probably the exception to the policy (which includes a timely *suspension to* that policy when faced with a subpoena or threat of litigation) that is often the most complicated part of implementing an electronic management system. This is especially true when the company is a frequent participant in investigations and litigation, which usually means that a reasonable policy needs to be flexible enough to handle consistent and ongoing litigation that relates to the fundamental business practices of a concern.

It should come as no surprise that the burden of implementing a reasonable document retention policy and then communicating a “litigation hold” rests with the client. However, courts have increasingly

⁴⁴ 125 S. Ct. 2129, 2005 U.S. Dist. LEXIS 4348 (May 31, 2005).

⁴⁵ *Andersen* at *17 (citations omitted).

⁴⁶ 220 F.R.D. at 217.

concluded that these burdens also extend to the clients' executives and their in-house and outside counsel. Moreover, courts have held with increasing frequency that telling employees what they should and should not be doing is not enough. A company (and its lawyers) must also take steps to monitor and enforce that policy and take immediate corrective action, and in some cases disciplinary action, once someone fails to comply.

For example, in *Heng Chan v. Triple 8 Palace*,⁴⁷ the trial judge noted:

The preservation obligation runs first to counsel, who has a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction. . . . Where the client is a business, its managers, in turn, are responsible for conveying to the employees the requirements for preserving evidence. . . . Thus, 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. When the failure to meet these obligations results in the destruction of evidence, sanctions are warranted. And, though the nature of the sanction depends in part on the state of mind of the destroyer, some remedy may be appropriate even where the destruction is merely negligent.⁴⁸

Similarly, in *Clark Construction Co. v. City of Memphis*,⁴⁹ the court admonished the defendant for *allowing* destruction of evidence by an employee in light of its litigation hold obligations. The court found that the destruction of documents was grossly negligent and ordered a rebuttable adverse inference instruction.⁵⁰ Also of note is *Broccoli v. Echostar Communications Corp.*⁵¹ In *Broccoli*, the court granted an adverse inference instruction at trial for the company's "bad faith" in its failure to suspend its e-mail and data destruction policy or preserve

⁴⁷ 2005 U.S. Dist. LEXIS 16520, at *16 (S.D.N.Y. Aug. 11, 2005).

⁴⁸ *Id.* (citations omitted).

⁴⁹ 2005 U.S. Dist. LEXIS 13808 (W.D. Tenn. Mar. 14, 2005).

⁵⁰ *Id.*

⁵¹ 2005 U.S. Dist. LEXIS 16000, at *14 (D. Md. Aug. 4, 2005).

essential personnel documents in order to fulfill its duty to preserve the relevant documentation for purposes of potential litigation.

**PART V:
PROPOSED AMENDMENTS TO THE FEDERAL RULES
OF CIVIL PROCEDURE**

At the time *Zubulake* was being decided, the process for amending the Federal Rules of Civil Procedure to better address electronic discovery began to build momentum. Although this process began in 1999, the approval of the proposed amendments moved closer to final approval in 2005 through their acceptance by various rule committees. The proposed amendments are expected to be approved by the Supreme Court and Congress in 2006.

The Civil Rules Advisory Committee first drafted the proposed amendments in August 2004 in response to what the committee saw as a need to address the sheer volume and dynamic nature of electronic material that was being sought—and produced—during the discovery process. After 180 written comments, public hearings in San Francisco, Washington, D.C., and Dallas, and 74 live witnesses, the rules were approved by the Civil Rules Advisory Committee in April of 2005. After receiving input from the public, the rules were revised and sent to the Standing Committee on Rules (Committee on Rules of Practice and Procedure), where they were approved in June. Although the rules themselves were approved, the Standing Committee revised some of its notes. From there, the rules were submitted to the Judicial Conference on July 25, 2005. On September 20, 2005, the Judicial Conference approved the rules without discussion and sent them to the Supreme Court. The Supreme Court has until May 1, 2006, to report to Congress, and then Congress has six months to adopt the rules. If there are no objections—and none are anticipated—the rules will go into effect on December 1, 2006.

It is hard to say how things will change, if they change at all, once the rules go into effect. Although the effective date is still months away, the concepts and issues embodied in the amendments are playing themselves out in *Zubulake* and other important cases we have noted. This is no coincidence, as many of the judges involved in some of the early e-discovery cases testified and were on committees responsible for the changes to the rules, such as Judge Scheindlin, who penned *Zubulake*.

There are six main areas affected by the proposed amendments:

A. Discoverability of “electronically stored information”

- B. “Meet and confer” requirements
- C. Discovery of information “not reasonably accessible”
- D. Inadvertent production and waiver of privilege
- E. Form of production
- F. “Safe harbor”

**A. Discoverability of Electronically Stored Information:
Changes to Rule 26(a)(1)(B), Rule 34(a), and Rule 45**

Since 1970, the only reference to electronic information in the Federal Rules has been that “data compilations” along with “documents” are discoverable. Under the proposed amendments, Rules 26(a), 33, 34, and 45 would be amended to add that, along with documents, “electronically stored information” is discoverable. This change was made to account for electronic information that did not fall under the traditional definition of a “document” or of “data compilations.” Because “data compilations” falls under either “document” or “electronically stored information,” the Civil Rules Advisory Committee (the committee) felt keeping reference to “data compilations” in Rule 26(a)(1)(B) would be redundant.⁵²

It is doubtful much will change after this rule is in effect. For example, currently courts use the “data compilations” language in Rule 34(a) to include the discovery of electronic information, even relevant information on hard drives, such as in *BG Real Estate Services, Inc. v. American Equity Ins. Co.*⁵³ On the other hand, having a broader definition such as “electronically stored information” will allow for future discovery of information from electronic sources that may not even be conceived of today.

**B. “Meet and Confer”: Changes to Rules 26(f) and 16(b)
and Form 35**

⁵² See Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005). This report will be referenced throughout this monograph as the “Committee Notes.” A copy of the report can be found at <www.applieddiscovery.com>.

⁵³ 2005 U.S. Dist. LEXIS 10330, *15 (E.D. La. May 18, 2005).

The proposed changes to Rule 26(f) require parties to address issues relating to electronic discovery at the beginning of the case, and they are probably the most important of all the rules changes. To the extent the parties can agree on issues related to electronic discovery, the other rule changes will have little or no effect on the parties. Proposed Rule 26(f)(3) requires the parties to discuss three broad categories of topics related to e-discovery:

1. ***The preservation of evidence.*** The committee made it clear they did not want preservation orders to become “common” or “automatic,” but given the dynamic nature of electronic information and the fact that companies often employ technologies that delete or overwrite information on a regular basis for purposes of document retention or management, the committee felt it was important for the parties to discuss these systems and the preservation of evidence up front. A dialogue such as this can prevent spoliation claims later on as the parties understand what each is capable of preserving and what the other’s expectations are. Of course, in order to have these types of conversations, attorneys will need to understand their clients’ IT systems and capabilities before the Rule 26 Conference—a requirement already imposed by many local district court rules.
2. ***Form of production.*** As technology changes, the form in which information is produced will also change. Form of production can also vary widely depending on the volume of information. Although the proposed amendments contain default provisions for form of production, initial agreements about form of production can make for a smoother discovery process as parties will have time to plan ahead and determine whether their clients’ IT departments can handle the discovery process or if an outside vendor is needed.
3. ***Consideration of inadvertent production and potential waiver of privilege.*** Parties are encouraged to discuss how inadvertent production will be handled. The committee saw a need for these issues to be addressed given that privilege review for electronic documents can be incredibly time consuming and hard to identify on its face when looking at documents such as e-mails with attachments and corresponding metadata that may make a document privileged. Although the amendments contain a

default procedure for handling inadvertent production and potential waiver of privilege, agreements between the parties may be a better alternative since there is no consistency in the federal courts regarding waiver of privilege for inadvertently produced documents.

The proposed changes to Rule 16(b) correspond to the changes in Rule 26(f). Amended Rule 16(b) provides that the scheduling order the court enters may include “provisions for disclosure or discovery of electronically stored evidence” and “any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production.” Amendments to Form 35 would provide that the report to the court includes proposals about the parties’ treatment of electronic information and any agreed orders regarding claims of privilege or of protection as trial-preparation material asserted after production.

C. Discovery of Information that Is “Not Reasonably Accessible”: Changes to Rules 26(b)(2)(B) and 45(d)(1)(C)

Under the current rules, a party may seek discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.⁵⁴ The proposed rule would change that general rule such that electronic information from sources not reasonably accessible due to undue burden or cost is no longer discoverable. However, the producing party does have to provide the requesting party with a description of the sources of the material it is not producing so that the requesting party has enough information to evaluate the burdens and costs. The responding party may file a protective order, and the requesting party may file a motion to compel. If either motion is filed, the producing party has the burden of showing the information is in fact “not reasonably accessible due to undue burden or cost.” Even if that showing is made, if good cause is shown, a judge can still order production of the material, which can open the door to conditions such as cost shifting.

This proposed rule begs the question, however, as to what exactly is meant by “reasonably accessible.” While undue burden or cost is the

⁵⁴ FED. R. CIV. P. 26(b)(1).

defining factor, technology appears to be driving the definition. The Committee Notes reflect this fact: “[E]xamples from current technology include back up tapes intended for disaster recovery purposes that are often not indexed, organized or susceptible to electronic searching, legacy data that remains from obsolete systems and is unintelligible on the successor systems, etc.”⁵⁵ Thus, what is considered “accessible” will change as technology changes. What *is* clear is that the information must not be accessible for any purpose and not just litigation, that is, if the company can access and use the information, it is accessible.

We are seeing the essence of this rule played out in the courts already. For example, in *United States of America v. Americagroup Illinois, Inc.*,⁵⁶ the court held the burden was on the responding party to prove by “affirmative and compelling proof” that producing e-mails on backup tapes constituted an undue burden.⁵⁷ After reviewing the evidence, which showed that to restore the backup tapes would be costly in terms of “expense, equipment and man-power” (18 weeks of manpower to complete the restoration), the court held that “in the hierarchy of accessibility, it is clear that electronic data stored on media such as the backup tapes involved here is near the bottom.”⁵⁸ Thus, even under the current rules, accessibility of data is already a consideration in the discovery context.

**D. Inadvertent Production and Waiver of Privilege:
Changes to Rules 26(b)(5) and 45(d)(2)(B)**

This proposed rule constructs a procedure for handling privileged or work product materials that have been inadvertently produced, but the rule does not change the substantive law of privilege. The purpose of Rule 26(f) is to address the sheer volume and unique circumstances of electronic information. Electronic data may contain privileged information that is not apparent on its face but (due to metadata) must be retrieved, and in the case of e-mails, through attachments. These layers of privilege can add to the already costly and time-consuming process of privilege review.

⁵⁵ Committee Notes at 40.

⁵⁶ 2005 U.S. Dist. LEXIS 24929 (N.D. Ill. Oct. 21, 2005).

⁵⁷ *Id.* at *8.

⁵⁸ *Id.* at *11-12.

Under the proposed rule, if information is produced in discovery that is subject to a claim of privilege or work product protection, the party making the claim may notify another party that received the information of that claim and the basis for it. The notified party must promptly return, sequester, or destroy the information and any copies of it and may not disclose or use the information until the claim is resolved. A receiving party may also promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified of the privilege or work product claim, the receiving party must take reasonable steps to retrieve it. The producing party must also preserve the information until the privilege claim is resolved.⁵⁹

E. Form of Production: Changes to Rules 34 and 45

It is hoped that the parties will reach an agreement about the form in which electronic information should be produced during the “meet and confer” discussed above. If the form of production is not agreed upon at the Rule 26(f) Conference, however, the proposed rules provide the parties with some options.

First, a party may specify the form or forms of production it would like. The responding party can comply with this request or it can object and state the form or forms it intends to use. Second, if no form is requested, a party can produce the electronically stored information either in the form in which it is ordinarily maintained or in a reasonably usable form.

Some question has arisen over what “form or forms in which it is ordinarily maintained” means and whether that is analogous to “native format.” The committee specifically noted that native format “can have disadvantages ranging from an inability to redact, leading to privilege problems; an inability to bates-stamp⁶⁰ the ‘document’ for purposes

⁵⁹ For an in-depth look at the problems of inadvertent production of privileged material, see *Hopson v. Mayor*, 2005 U.S. Dist. LEXIS 29882 (D. Md. Nov. 22, 2005).

⁶⁰ “Bates-stamping” is the process of marking documents produced by a party with alphanumeric production labels for ease of reference and an organized production. The term “Bates Number” originates from the Bates Manufacturing Company, which manufactured automatic handheld numbering machines. Interestingly, Thomas Edison purchased the Bates Manufacturing Company

of litigation management and control, which is not an insignificant consideration, particularly in complex multi-party cases; and the receiving party's ability to create 'documents' from the produced native format data and present them back to the producing party as deposition and/or proposed trial exhibits that, while based on the native format data produced are totally unfamiliar to the producing party."⁶¹ Similarly, in *In re Priceline.com Inc. Securities Litigation*,⁶² the court ordered production in PDF or TIFF rather than native format.

Thus, "ordinarily maintained" means just that: how the information is maintained by the party, which in many instances may include a database.⁶³ Moreover, even though this rule states it is an either/or proposition—either in the form in which it is ordinarily maintained *or* a reasonably usable form, the Committee Notes make it clear that the former must include the latter—documents must always be produced in a reasonably usable form.⁶⁴ In addition, a party may still request that electronically stored information be produced in hard copy. A party need only to produce documents in one form.

This amendment is consistent with current rules. For example, courts have held that electronically stored information must be "translated, if necessary, by the respondent through detection devices into reasonably usable form," such as in *BG Real Estate Services, Inc.*⁶⁵

F. Safe Harbor from Sanctions: Changes to Rule 37

The change to Rule 37 received the most attention during the comment period, and it was redrafted many times before the final version was approved. The rule states that, absent exceptional

in 1892.

⁶¹ Committee Notes at 64.

⁶² 2005 U.S. Dist. LEXIS 33636 (D. Conn. Dec. 8, 2005).

⁶³ *But see* Williams v. Sprint United, 2005 U.S. Dist. LEXIS 21966 (Sept. 29, 2005), where "ordinarily maintained" with respect to Excel spreadsheets appeared analogous to "native format." However, because of the unique aspects of the metadata of Excel spreadsheets, the holding in this case should be limited to Excel spreadsheets, as other file formats can be produced in converted formats such as PDF and TIFF with all of the metadata intact.

⁶⁴ Committee Notes at 65, 75.

⁶⁵ 2005 U.S. Dist. LEXIS 10330, at *15 (citing FED. R. CIV. P. 34(a)).

circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine good faith operation of an electronic information system.

The purpose of the proposed rule is to account for the fact that businesses often employ document retention policies that automatically overwrite and delete information on a regular basis. If information is lost as a result of the good faith operation of these systems, then a party cannot be sanctioned absent exceptional circumstances, which allows for judicial discretion to impose sanctions if the facts so warrant. The committee recognized that the types of automatic processes contemplated here are often essential to the operation of electronic information systems. Although the committee stated, “[I]t is unrealistic to expect parties to stop such routine operation of their computer systems as soon as they anticipate litigation,” the committee also noted that “good faith” may require a party to intervene to suspend certain features of the routine operation of an information system to prevent loss of information subject to preservation obligations. Such intervention is often called a “litigation hold.”⁶⁶ The rule “is not intended to provide a shield for parties that intentionally destroy information because of its relationship to litigation,” and good faith will likely depend on the intent and obligations of the parties at the time material was destroyed.

G. Effect of Proposed Amended Rules

Because these rules will not likely go into effect until December of 2006, and the concepts embodied in the rules are already being employed, it is unlikely much will really change with the implementation of the amended rules. However, it is clear courts will no longer tolerate attorneys who do not understand or seek to understand their clients’ information technology systems. Lawyers who intend to litigate in the future will need to grasp the basics of information technology and if necessary, seek out experts who can help them along the way. For example, in *Americagroup Illinois, Inc.*,⁶⁷ the court was

⁶⁶ Committee Notes at 83.

⁶⁷ 2005 U.S. Dist. LEXIS 24929.

not persuaded by the defendant's lack of knowledge of plaintiff's information technology system, as the defendant could have deposed the information technology officer or employed an expert. Beyond that, there is no doubt that as technology changes, so will the definition and scope of such terms as "reasonably accessible," and "good faith." Stay tuned.

**PART VI:
BENEFITS OF E-DISCOVERY**

This publication would be incomplete if we did not mention some of the benefits that e-discovery and electronic information have to offer. For example, metadata usually includes precisely the types of information that clients typically pay vendors a lot of money to "code." Metadata also provides an easy way for lawyers to track relationships between e-mails and other documents, to match e-mails with their attachments, and to follow a trail of e-mails that were forwarded or prompted a response.

Lawyers do not have to search electronically stored information; software performs this task at a much cheaper cost to the client. Computers are indefatigable. People get tired and lose efficiency.

Moreover, the use of agreed upon word searches and ontology can lead to a search process that is much more reliable and efficient than a human review. For example, the use of computers ensures you only have to review the same document once, and decisions made with respect to one document (i.e., whether a document should be produced, is privileged, or deserves a "confidential" designation) can be applied to a universe of other documents that share the same characteristics. Computer software can employ algorithms to locate exact duplicates to dramatically reduce review time—the most expensive part of any document review.

Finally, review times can also be drastically reduced by the use of online review systems. Most of these systems are easy to use. Many of them are Web-based, which means that clients, lawyers, and paralegals can access them at any time and at any place where there is Internet access. Only a small number of these systems require software to be downloaded and run from the particular computer that the reviewer is using.

All of these values associated with electronically stored information make the review process a much more consistent and reliable process.

In fact, electronic “documents” often come self-coded and ready for computer review.

**PART VII:
CLOSING THOUGHTS**

E-discovery has come a long way. It was not too long ago that we sat in conference rooms and witnessed stunned looks from lawyers and clients who realized their document retention protocols fell far short of what was required. Fortunately for all of us, Judge Scheindlin and many of her colleagues on the bench devoted a great deal of time and resources addressing e-discovery. Because of Judge Scheindlin and other judges, we are all on notice that e-discovery is an important part of litigation loaded with pitfalls and benefits.

However, much as we cannot know how technology will change, Judge Scheindlin could only address the issues that were raised by the litigants before her. As technology continues to change, so will the issues that will need to be addressed by the courts. As the new Federal Rules of Civil Procedure become effective and enforced, those rules will also need to be interpreted to reflect changes in technology. Thus, although *Zubulake* and its progeny answered many questions, the evolution of technology will undoubtedly result in even more questions in the future.

Nonetheless, this should not come as bad news to lawyers. True, technological changes will likely complicate and confuse the legal implications of electronic discovery, but there is a reason we are sometimes referred to as “counselors.” It is our job to counsel our clients on what their current legal obligations are and how best to position themselves so they can adapt to new and perhaps even unforeseen rules and legal holdings in light of our ever-changing legal and technological environment. We do this on a daily basis in all areas of law. The topic of e-discovery is and should be no different.

If anything, e-discovery should be viewed in a positive light. The very same cause of discomfort with e-discovery (the evolution of technology) will also be the source of the answers to future questions. Put another way, technology got us into this mess and technology will get us out! Technology will help create the tools that will allow for a much more efficient and painless discovery process. Technology will lead the way.

Indeed, recent developments have made the e-discovery process more reliable and affordable. Recent cases have made the e-discovery

process more understandable. And recent verdicts have made the e-discovery process a more significant part of litigation.

So what does all of this mean? It means that e-discovery is here to stay. Learn it. Embrace it. Take advantage of it. There is absolutely no reason for any of us to drown in the same waters of the *Zubulake* defendant's demise. Many thanks to Judge Scheindlin and others who provided us with life preservers. It is now much easier to stay afloat of our e-discovery obligations and stay above water in litigation.

ABOUT THE AUTHORS

GEOFFREY A. VANCE, ESQ. Mr. Vance is a partner in the Trial Department of McDermott Will & Emery LLP and works out of McDermott's Chicago office. He concentrates his practice in the areas of complex commercial litigation, internal investigations, white-collar criminal defense, and professional services liability. Each of these areas involves electronic discovery, a topic about which Mr. Vance frequently speaks and writes in a variety of settings.

COURTNEY INGRAFFIA BARTON, ESQ. Ms. Barton is the Vice President of Industry Relations at LexisNexis Applied Discovery, where she publishes and lectures extensively on electronic discovery issues. Prior to joining Applied Discovery, Ms. Barton was a trial attorney with the U.S. Department of Justice. Before that, she was a senior associate at Arnold & Porter in Washington, D.C.