Navigating the Hazards of E-discovery



A Manual for Judges in State Courts Across the Nation

INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM

Navigating the Hazards of E-discovery

A Manual for Judges in State Courts Across the Nation

INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM

UNIVERSITY OF DENVER

Institute for the Advancement of the American Legal System

at the

University of Denver

Institute for the Advancement of the American Legal System

at the

University of Denver 2044 E. Evans Avenue, Suite 307 Denver, CO 80208

303.871.6600

The Institute for the Advancement of the American Legal System (IAALS) at the University of Denver is a national, non-partisan legal reform organization whose primary mission is to provide innovative and results-oriented recommendations for the improvement of America's courts.

For more information about us please visit our website at www.du.edu/legalinstitute. We greatly appreciate your interest.

STAFF
Rebecca Love Kourlis Executive Director
Pamela A. Gagel Assistant Director
Jordan M. Singer Director of Research
Dallas N. Jamison Director of Communications and Development
Kim A. Seidman Office Manager
Mac V. Danford Consultant
Michael E. Buchanan Research Assistant

IAALS would like to thank Richard Baer, The Honorable James Bredar, The Honorable Kevin Burke, The Honorable Janice B. Davidson, The Honorable Phillip Garrison, Andrew Halliman, The Honorable Morris Hoffman, Richard Holme, David Isom, Donald McLaughlin, The Honorable Lael Montgomery, Ken Stafford, Stefan Stein, David Thomson, Malcolm Wheeler, and Russell Wheeler for their feedback and assistance in preparing this manual.

Copyright © 2007 Institute for the Advancement of the American Legal System. All rights reserved.

For reprint permission please contact IAALS.

Foreword
Introduction
I. The Nuts and Bolts of E-discovery4
II. The Litigant's Approach to E-discovery
A. The Cost of Production
B. Cost Allocation
C. Preservation of Evidence
III. The Lawyer's Approach to E-discovery
A. Form of Production
B. Waiver of Privilege Through Inadvertent Disclosure
IV. The Courts and E-discovery: Issues and Recommended Approaches
A. Developing E-discovery Procedures: Federal and State Court Experiences20
B. General Recommendations for Judges Approaching E-discovery Disputes
Conclusion
Appendix A: E-discovery Resources
Appendix B: Glossary of Key Terms
Notes

CONTENTS

A MESSAGE FROM THE INSTITUTE'S EXECUTIVE DIRECTOR

FOREWORD

Colleagues:

When I left the Colorado Supreme Court in January of 2006, I had never heard the acronym "ESI." As I have traveled around the country in the intervening months, I have found that many judges are similarly unfamiliar with the basics of ESI- electronically stored information. This is the tidal wave of data we have become so accustomed to creating during the course of our day—word processing documents, e-mails, text messages, even voice mail. But, what is its relevance to your days in court?

On December 1, 2006, amendments to the Federal Rules of Civil Procedure governing e-discovery took effect. The new rules deal with the exchange of electronically stored information as evidence in civil court cases. Given the ubiquitous nature of ESI, the impact of discovery involving this data has rapidly trickled down from FORTUNE 500 companies involved in complex litigation to mid-sized businesses and even individuals involved in domestic relations cases. The full implications of e-discovery could have a staggering impact on litigation: its costs and its management. We do not yet know how the states will deal with e-discovery rules. What we do know is that courts across the country must be well-informed and able to respond to the issue when it arises. You do not need to be "IT experts," but you do need to understand the fundamentals of ESI and e-discovery.

Our Institute was established to improve America's legal system so that the process is cost-effective, timely and reliable. We have concerns that the onslaught of e-discovery may actually represent a giant step backward in this regard and it is our intention to make proposals for ways of addressing that possibility in another context. Here, our intent is simply to offer a convenient tool that will provide you with guidance on this subject. We have organized the concepts, the vocabulary and well-known case law in one manual, developed specifically for you—the state court judges of our nation. It is our hope that you will find this information truly relevant and practical.

REBECCA LOVE KOURLIS

E lectronic Discovery, or e-discovery: what is it? Where has it been, where is it going and what do you as a judge need to know in order to address the significant challenges associated with it? What information about e-discovery will help you develop appropriate strategies and take advantage of available technological advances? The purpose of this manual is to give a careful overview of the language, the law and the issues inherent in e-discovery so as to better equip you to recognize the benefits, and pitfalls, of discovery in the electronic world.

On a purely definitional level, e-discovery refers to the discovery of all electronically stored information (ESI)—information such as e-mail messages, instant messages, voice mails, cell phone and pager text messages, websites, call logs, word processing documents, databases, digital photos, spreadsheets and accounting software, and specialized engineering software, as well as backup and archived copies of that same information. In many important respects, the issues surrounding discovery of electronic information are no different than those in traditional paper discovery: requests must still be relevant and reasonably tailored, and responses and production must be timely and complete. But there are unique aspects to electronic information that intensify the advantages and disadvantages of the traditional discovery process. Indeed, e-discovery might well be thought of as traditional discovery magnified. Where the universe of relevant written communications in a case was once a box of internal memos, today it may be a million e-mails or more.

Magnification is not just an issue of volume. ESI also affects how litigants approach and work through the discovery process. If the parties act cooperatively and focus their discovery requests appropriately, the availability of ESI can make finding relevant information faster and cheaper. Powerful search engines and other emerging tools allow all parties to find important information in a fraction of the time required by a hand search. If the parties are determined to make discovery difficult, however, the presence of ESI can lead to additional costs (which may be hundreds or thousands of times higher than traditional discovery), prolonged delays, fights about privilege, and excessive motion practice. As a result, courts must work harder than ever to focus the parties and to narrow discovery disputes in order to keep costs and schedules under control.

The challenges and opportunities posed by e-discovery cannot be ignored. Five years ago, disputes over the discovery of ESI were largely confined to cases involving large corporations or organizations—the entities which generated thousands or even millions of electronic documents, e-mails, spreadsheets and invoices each day. But the times are changing rapidly. Today, it is not just wealthy and sophisticated parties who wrangle over production of ESI, and disputes are not limited to the federal arena. E-discovery is quickly becoming a fact of life for all courts, at every level. Every kind of civil action, from complex commercial litigation to domestic relations cases, has seen increased use of electronically stored information.

INTRODUCTION



Where the universe of relevant written communications in a case was once a box of internal memos, today it may be a million e-mails or more.

INTRODUCTION

Today, it is not just wealthy and sophisticated parties who wrangle over production of ESI, and disputes are not limited to the federal arena. E-discovery is quickly becoming a fact of life for all courts, at every level. In light of the new challenges posed by e-discovery, organizations such as the Sedona Conference and the Conference of Chief Justices have promulgated guidelines and recommendations. We commend those to the reader, in addition to other publications (set out in Appendix A) that discuss certain e-discovery issues in detail.

This manual proceeds as follows: Part I provides a brief background on the vocabulary and technical aspects of electronic discovery. Part II examines issues of primary concern to litigants, particularly cost of production and preservation of evidence. Part III, in turn, looks at e-discovery challenges from the perspective of the bar. Finally, Part IV focuses on issues of particular concern to courts, and offers suggestions to help courts handle e-discovery disputes with fairness and efficiency. At the end of this manual, you will find a recommended list of materials for further reading, as well as a short glossary of terms. The range of information covered by e-discovery is extensive. In addition to e-mails, voice mails, word processing documents, and other materials consciously created by a human user, ESI also includes information automatically generated by a computer without human intervention, including system history files, temporary files, and metadata. Metadata is information about electronically stored files that is hidden within the files themselves or in a linked database. Metadata typically contains information such as the file's author, all recipients, the dates on which the file was created, modified, read or accessed by recipients, or printed, and all changes that have been made to the file. Accurate metadata therefore provides a wealth of information about the context in which a document was used or accessed, and is often the best source of evidence as to the authenticity of an electronic file. Metadata is not a foolproof form of authentication, however; because metadata may be modified separately from the file to which it relates, its accuracy is not always guaranteed.

Electronically stored information is not only wide-ranging, but is now a fundamental and pervasive part of American life. By all accounts, more than 90% of the information developed today is created and stored electronically, and most will never be printed out. Moreover, the volume of information being created is staggering: for example, it is estimated that American businesses exchange about 2.5 *trillion* e-mails annually, and 75% of those e-mails are believed to contain proprietary information. In an increasing number of disputes, information relevant to the parties' claims and defenses is no longer in a file cabinet but on a hard drive. As one commentator recently noted, "The days of paper-created documents are over."¹

Electronic evidence differs from paper evidence in many important ways. In contrast to a paper document, electronically stored information:

- Is often easily searchable. Using software programs to "read" and search an electronic document is often far quicker than searching a paper document by hand. For example, 100,000 pages of electronic documents might be searched for keywords in a matter of minutes, while a hand search of those same documents in paper form might take 1,000 hours or more. Furthermore, for some information, the printed form is effectively unusable. A large electronic database, for example, may be extremely valuable in native form (because the information contained within it can be selected, sorted, and manipulated), but entirely useless in paper form (when no sorting or selection can take place, and the printed version consists of thousands of pages).
- Is often invisible. Invisible data can take many forms. A significant amount of electronic information (such as temporary files or backup data) is created by the computers themselves, and is unseen by and usually unknown to human users. Other information, such as the formulae used to calculate figures on a financial spreadsheet, may be input

I. THE NUTS AND BOLTS OF E-DISCOVERY



It is estimated that American businesses exchange about 2.5 trillion e-mails annually, and 75% of those e-mails are believed to contain proprietary information. In an increasing number of disputes, information relevant to the parties' claims and defenses is no longer in a file cabinet but on a hard drive.

I. THE NUTS AND BOLTS OF E-DISCOVERY

The amount of electronic data in a complex litigation between two large corporate parties can generate the equivalent of more than one hundred million pages, which would require 6,250 trees to print out and would take about 30 person-years of review for each party. by human users but not displayed on the spreadsheet itself. In addition, electronic documents contain metadata that is often not easily accessible. Moreover, some electronic files may continue to exist on computers even after they are assumed to be deleted or lost.

- Often can be read only with special software. Many businesses, for example, have developed proprietary software to help organize data related to their customers, inventory, sales, and the like. The underlying data may be relevant and discoverable, but cannot be accessed without disclosing the proprietary software to the opposing party. This poses confidentiality issues not just for the underlying data, but also for the form in which those data are produced. Similarly, if data are created with software that has since become outdated, there may be additional costs and burdens associated with the production of such data notwithstanding that the information itself is discoverable.
- Creates challenges in distinguishing between originals and copies. Unlike paper documents, there is no obvious "original" version of an electronic document. Rather, multiple copies of identical records can exist simultaneously without any having claim to originality. Furthermore, most electronic documents can be copied in seconds or minutes at little or no cost, whereas creating copies of paper documents can quickly become expensive and time-consuming.
- Exists in massive quantities. The days when discovery involved a few—or even several dozen—boxes of paper documents are rapidly disappearing. Today, the average desktop computer can store millions of pages of text. Furthermore, the amount of electronic data in a complex litigation between two large corporate parties can generate the equivalent of more than one hundred million pages, which would require 6,250 trees to print out and would take about 30 person-years of review for each party.²
- Can be stored easily and inexpensively. The price of electronic storage capacity keeps dropping precipitously. By mid-2003, the cost of storing electronic data was falling by 50% every nine months. Furthermore, the physical storage of electronic documents remains minimal: a commercial database of 1 terabyte can be stored easily in a relatively small hard drive (less than one-fourth of a cubic foot), whereas storing that same information in print form would require 150 *miles* of bookshelves. It is important to note, however, that while the per unit expense of electronic storage continues to fall, much more information is also being created and saved, meaning that the overall cost of storage for many companies and organizations has not changed considerably.

n a paper world, civil discovery for litigants is a relatively straightforward process (albeit too often a time-consuming and unpleasant one). The litigant reviews the opposing party's document requests, collects files and information that are potentially responsive, and makes the files accessible to his or her attorney to review for relevance and privilege. This task is usually helped by the fact that paper documents have a clear life cycle: they are created (through writing, typing, or printing); sometimes duplicated or circulated; stored (in files or boxes); and ultimately destroyed (by shredding, recycling, burning, or just throwing away). Companies and large organizations usually have document retention policies that specify what documents are retained and for how long. When documents are destroyed, they are presumed gone forever. When they are retained, there are often organized or stored in a rational way.

This process breaks down when electronic files are at issue because the life cycle of electronically stored information is much more complicated. Relevant ESI may be created by people, but also independently and automatically by computers and electronic data systems. ESI may be modified or transmitted on an ongoing basis. And ESI is extremely difficult to destroy or delete completely. Furthermore, depending on the media and format in which it is stored, electronic information may or may not be readily accessible, and the relative accessibility of electronic information is frequently determinative of the cost of producing and reviewing the information.

The most accessible form of electronic data is called *active data*. This category includes electronic files such as spreadsheets, word processing documents, databases, e-mail messages, and electronic calendars, which are easily and currently accessible on a home or business computer.

Archival data are data that are no longer stored directly on a computer or network, but which usually can be retrieved in the ordinary course of business; they are the rough equivalent of paper files located in off-site storage. Similar to archival data but generally more difficult to access, *legacy data* are data from a computer system that is no longer in use (think of data stored on 5¹/₄" floppy disks). Because computer systems evolve so quickly, data going back even a few months or years may be entirely inaccessible by a party's current system, and require specialized computers to access and review.

Backup data, like archival data, are deliberately saved onto a storage medium separate from the computer or computer network. Unlike archival data, however, backup data are used to restore an entire system in the case of catastrophic failure. A system administrator typically takes a "snapshot" of an entire computer system or network at a moment in time, and places that unfiltered information onto a storage disk. E-mails, word processing documents, spreadsheets, websites, multimedia presentations, and the like are all lumped together on the disk without recourse to a filing system. From a business perspective, this

II. THE LITIGANT'S APPROACH TO E-DISCOVERY



On backup tapes, ESI such as e-mails, word processing documents, spreadsheets, websites, and multimedia presentations, are all lumped together without recourse to a filing system. From a business perspective, this process makes sense because it simply preserves the entire system in case of catastrophic failure. From a litigation perspective, however, it is the equivalent of dumping all paper files into a huge, unsorted pile.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

Many files are recoverable long after they have been deleted even if neither the computer user nor the computer itself is aware of their existence. process makes sense because it simply preserves the entire system in case of catastrophic failure. From a litigation perspective, however, it is the equivalent of dumping all paper files into a huge, unsorted pile. Moreover, because backup data capture the existing ESI at a specific moment in time, items later thought deleted by users may in fact still exist on backup storage. As a consequence of this storage method, backup data may be a rich source of discoverable information. However, because the information is simply collected and is not organized in any meaningful way, sorting through the information may be costly and time-consuming unless specific electronic search tools are used.

Replicant data are automatically created by certain computer systems and programs for short-term recovery in the event of a system failure. For example, a word processing program may automatically make a copy of a document the user is creating, so that the document can be recovered if the computer malfunctions. Replicant data are rarely requested in the course of discovery.

Finally, *residual data* are data that still exist on a computer system even though they have been "deleted" by the user. As one set of commentators has explained,

"Deleting" a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status—thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, [they] may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted—even if neither the computer user nor the computer itself is aware of their existence. Such data [are] referred to as "residual data." ³

These differences in how paper documents and ESI are created, accessed and deleted pose three specific challenges for litigants of which courts should be aware: (1) the cost of sorting through and producing electronic documents and the related cost of restoring backup or legacy data; (2) preventing opposing parties from using the cost of responding to electronic document requests as a tactical sword to force settlement; and (3) developing a viable document retention strategy.

A. THE COST OF PRODUCTION

As alluded to above, four factors significantly influence the cost of electronic discovery. First, the volume of ESI is typically much greater than that of paper documents, in part because of the massive amounts of e-mail and instant messages which are now being created, most of which are being retained. Second, the magnetic tapes and disks commonly used to store ESI are rarely organized by subject matter (as a paper file cabinet may be), and often are not labeled at all, making the search for responsive information more difficult.⁴ Compounding this problem is the fact that the custodianship of electronic information is frequently more difficult to ascertain than it is with paper documents (although metadata can often provide accurate custodian information that paper documents cannot). Third, electronic files are often not directly accessible, meaning the data they contain must be recovered or translated before they can be used. Finally, experts with specialized knowledge of computers are often needed to convert ESI into indexed and reviewable files, and/or search for deleted documents, missing e-mail, and system data. All of these differences contribute to the potential of electronic discovery being considerably more time-consuming and more expensive than traditional discovery—no small feat given the astonishing costs of even traditional discovery in some cases. Indeed, the costs of electronic discovery can be staggering, often totaling hundreds of thousands, or even millions, of dollars in a given case. In one relatively recent case, the parties told the court that restoration of 200 backup tapes would cost \$9.75 million.⁵ In another case, the cost of restoring 93 backup tapes was estimated to be \$6.2 million—a cost of nearly \$67,000 per tape.⁶

While increased discovery costs are due in part to inherent features in the way ESI is created and stored, other factors contributing to high e-discovery costs are entirely preventable. For one thing, parties frequently enter the discovery phase with very little idea of what information is actually contained in the electronically stored information they seek. Requesting parties simply assume that e-mails, spreadsheets, word processing documents, and the metadata buried within them is to some degree relevant, and accordingly issue broad, expansive requests. Responding parties counter that the cost of production cannot justify what little new information may be gained from it. But in many cases, the parties are arguing from ignorance. Until the potentially relevant electronic information is identified, collected and analyzed—at least on a preliminary basis—neither party can truly appreciate what electronic data, if any, are likely to be available that are relevant to the claims and defenses of the parties.

Given these concerns, a number of solutions have been proposed to lower the costs of electronic production. One idea, requiring the parties to conference on e-discovery issues at the onset of litigation, has garnered considerable traction, and was adopted as part of the 2006 amendments to Federal Rules of Civil Procedure 16, 26(a)(1) and 26(f).

There are several benefits to early conferencing. At an initial stage in the litigation, parties can discuss which computer systems should be subject to preservation and discovery, what the relevant time period for discoverable information should be, and the identities of individuals who are likely to have relevant ESI. Parties can also discuss the most useful form of privilege logs for voluminous documents, and whether draft expert reports and materials will be requested. By reaching clear and specific agreements about the scope of production early in the process, parties should be able to reduce both the cost of producing unnecessary materials and collateral litigation to fight about that production.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

In one relatively recent case, the parties told the court that restoration of 200 backup tapes would cost \$9.75 million. In another case, the cost of restoring 93 backup tapes was estimated to be \$6.2 million a cost of nearly \$67,000 per tape.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

A recent survey by the American Bar Association found that 10% of corporate counsel chose to settle a case rather than incur the costs associated with electronic discovery. In one case, for example, a broker-dealer who sought damages of \$175,000 against a former employee was forced to settle the case when it realized that compliance with the court's discovery order would cost it \$225,000.

Early conferencing is not the only tool in the court's arsenal to help control e-discovery (and indeed, all discovery) costs. Consistent with the applicable civil rules in your jurisdiction, you may: (1) require the parties to serve more focused and narrowly tailored document requests, (2) limit the amount of electronically stored information that can be requested, (3) suggest that the parties use advanced search techniques or benchmarking standards to electronically search data for relevant and responsive information, and/or (4) where backup tapes are at issue, initially require that only a small portion of the total number of tapes at issue be restored to determine whether they really contain relevant evidence.

B. COST ALLOCATION

Not only are electronic discovery costs high, but they are frequently allocated disproportionately between the parties. Under the Federal Rules of Civil Procedure and the procedural rules of most states, the producing party bears the cost of readying documents for production. This rule works well most of the time for traditional discovery, because the costs and burdens of collecting the requested information are relatively low in the grand scheme of all discovery costs. Electronic discovery, however, can raise the cost of readying information for production dramatically, because the potential universe of responsive information can be much greater. Potentially responsive ESI must be searched for, collected, and reviewed for relevance and privilege, often at volumes that may be hundreds or thousands of times greater than for paper documents. Backup and legacy data may need to be restored to a useable form before review can even take place. As discussed above, such restoration often requires the use of outside vendors, at the cost of tens of thousands of dollars per restored tape or disk.

For some, the costs of collecting and reviewing electronic documents are so significant that even proceeding to the discovery phase becomes impossible. Indeed, a recent survey by the American Bar Association found that 10% of corporate counsel chose to settle a case rather than incur the costs associated with electronic discovery. In one case, for example, a broker-dealer who sought damages of \$175,000 against a former employee was forced to settle the case when it realized that compliance with the court's discovery order would cost it \$225,000.⁷

The disproportionate allocation of cost under traditional discovery rules has led to a surge in motions to shift costs to the requesting party when ESI is at issue. When federal courts first encountered the cost-shifting issue in earnest in the late 1990s, they generally adhered to the traditional rule, reasoning that if companies made the conscious decision to use computer technology in their businesses, they should be prepared to reap both the costs and benefits of that choice. By the turn of the century, however, computers had become so ubiquitous that their use could no longer be seen as voluntary. As one court noted in 2001, the "cost of business" rationale "assumes an alternative. It is impossible to walk ten feet into

the office of a private business or government agency without seeing a network computer, which is on a server, which, in turn, is being backed up on tape (or some other media) on a daily, weekly or monthly basis. What alternative is there? Quill pens?"⁸ Accordingly, shifting all or part of electronic discovery costs to the requesting party became an acceptable practice under some circumstances. The Federal Rules, however, provided little guidance on how to perform a cost-shifting analysis, only stating generally that a court could issue an order to protect a party against "undue burden or expense," interpreted to permit cost-shifting in certain circumstances.

Federal courts responded by devising their own balancing tests, the most well-known of which was set out by Judge Shira Scheindlin of the Southern District of New York in *Zubulake*, *v. UBS Warburg LLC*.⁹ In *Zubulake*, a former employee of UBS brought gender discrimination and retaliation claims against her former employer, and requested that the defendant produce "all documents concerning any communication by or between UBS employees concerning Plaintiff." UBS declined to produce e-mails, arguing that they had been deleted, and that restoration of the deleted files from archived backup tapes was prohibitively expensive. The court distinguished between what it called "accessible" data (which is "stored in a readily usable format" such as active data) and "inaccessible" data (which is not "readily usable," such as backup or legacy data). The court held that the cost of producing "accessible" data should be borne by the producing party, in accordance with the traditional rule. With respect to "inaccessible data," the court set forth a seven-factor test to determine whether the cost of restoration and production should lie with the producing party or the requesting party. The seven factors are:

- 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 its incentive to do so;
- 6. The importance of the issues at stake in the litigation; and
- 7. The relative benefits to the parties of obtaining the information.

The court also instructed that the seven factors should be weighted in descending order, thereby giving the most weight to whether the requests were narrowly tailored and whether the information was available from other sources. Applying the seven factors to the case before it, the *Zubulake* court eventually concluded that the plaintiff should bear one-fourth of the estimated \$166,000 cost of restoring the backup tapes.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

Before the December 2006 amendments, the Federal Rules provided little guidance on how to perform a cost-shifting analysis, only stating generally that a court could issue an order to protect a party against "undue burden or expense," interpreted to permit cost-shifting in certain circumstances.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

Because "accessible" data cannot be subject to cost-shifting, the Zubulake test encourages parties to make broad requests for accessible data, even if it may be only marginally relevant or responsive. The Zubulake test has been celebrated by many as a reasonable approach to cost-shifting that emphasized practical matters such as availability of the evidence and relative cost of production. However, the test is not without significant flaws. First, because the responding party can only ask the court to shift costs when the ESI in question is "inaccessible," Zubulake provides at least some incentive for parties to use inefficient and inaccessible storage systems. Second, and relatedly, because "accessible" data cannot be subject to cost-shifting, the Zubulake test encourages parties to make broad requests for accessible data, even if it may be only marginally relevant or responsive. The responding party may still object based on overbreadth or irrelevance, but since there is no real risk of cost-shifting there is little incentive for the requesting party not to ask.

Because the accessibility threshold can be abused by both requesting and producing parties, one commentator has suggested an alternative test which focuses on the general burden of ESI production and limits cost-shifting to the most unduly burdensome production requests.¹⁰ Another set of commentators proposes a series of questions that bridge the distinction between accessibility and burden. They suggest that whether information is not "reasonably accessible" should be based in part on answers to the following questions: (1) How frequently does the IT department restore files from backup tapes for users? (2) When was the last time a file was restored from a backup tape? (3) What was the oldest file restored within the past several years? (4) How long does it take to restore a file? (5) When was the last time, if ever, that a full system restore was performed? (6) Does the responding party have a development or test environment on which a full system restore can be done so as not to disrupt operations?¹¹

Despite these alternative proposals, the 2006 amendments to the Federal Rules of Civil Procedure were heavily influenced by the *Zubulake* approach and base the cost-shifting analysis on the accessibility of the requested information. As amended, Federal Rule 26(b)(2)(B) provides:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Further channeling *Zubulake*, the Advisory Committee Notes for Rule 26 state that the decision whether to require a party to search for and produce ESI deemed not reasonably accessible "depends not only on the burdens and costs of doing so, but also on whether those

burdens and costs can be justified in the circumstances of the case." The Committee then sets out the seven *Zubulake* factors as "[a]ppropriate considerations" for evaluating burdens and costs.

Predictably, the amended Rule 26 has also invited criticism, for many of the same reasons as the Zubulake test. Some complain that the Rule will encourage parties to keep information in a form that is not "reasonably accessible" so it would be more difficult to discover. Indeed, parties could simply and unilaterally claim information was "not reasonably accessible" without any real basis, reversing the traditional rule that a party claiming undue burden has to seek protection from the court. Furthermore, the provision in the Rule that allows discovery for "good cause" notwithstanding the cost and burden of production is toothless, since it merely tracks other provisions in Rule 26 about the court's discretion to compel the production of documents. The "good cause" provision can only have an independent meaning if "good cause" is interpreted to require a higher standard than the default considerations already in Rule 26, or if the term "not reasonably accessible" is defined to distinguish between backup and legacy data (which is recoverable) and truly inaccessible deleted data (which is not). Finally, one commentator has argued that the Advisory Committee Note errs by defining "reasonable accessibility" as a function of the cost and burden to retrieve the information, when the better test would be whether the responding party routinely accesses the information for business purposes.¹²

A small number of states have worked to address the cost-shifting issue, and have gravitated toward more bright-line tests than the federal courts. Interestingly, all have placed the burden of production costs on requesting parties. Texas Rule of Civil Procedure 196.4, in place since 1998, explicitly instructs the court to shift costs to the requesting party if the requested data are not available in the ordinary course of business, a test applauded by some as more realistic than whether the data are "accessible." Mississippi adopted a nearly identical rule in 2003, although the wording of the rule appears to give the court slightly more discretion in determining whether cost-shifting is appropriate.¹³ In a rare decision on discovery issues, the California Court of Appeals read that state's civil rules to require the requesting party to bear the costs of translating backup data into a usable form if the restoration costs were found to be a "reasonable expense for a necessary translation."¹⁴ Finally, a New York court has held that even for electronic information, under the state's discovery rules, "the party seeking discovery should incur the costs incurred in the production of discovery material."¹⁵

C. PRESERVATION OF EVIDENCE

Electronically stored information also poses challenges to litigants by adding new dimensions to the duty to preserve and maintain documentary evidence. The rapid advance of technology has made it possible to retain e-mails, voice mails, and other electronically

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

A small number of states have worked to address the cost-shifting issue, and have gravitated toward more bright-line tests than the federal courts. Interestingly, all have placed the burden of production costs on requesting parties.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

At least one commentator has argued that attaching a duty to preserve at the moment litigation may be anticipated effectively creates a permanent disruption in ordinary document destruction procedures, especially for organizations and corporations that are frequently sued. stored information on a relatively inexpensive and essentially permanent basis, creating the expectation that such documents will be retained. ESI may also be expected to be available because it is hard to delete completely. Sometimes, however, ESI *can* be lost permanently. This can happen unintentionally through accidental physical destruction of hard drives or backup tapes, or by routine business practice of overwriting backup tapes every few months. But permanent loss may also be intentional, through efforts to "scrub" electronic documents of metadata or remove documents altogether from hard drives.

The classic example of bad faith spoliation—improper shredding of relevant documents is not without electronic analogues. Perhaps the most egregious examples involve commercial computer software such as "Evidence Eliminator" designed to wipe a hard drive clean of relevant and responsive electronic information. Less egregious, but still of concern, is the removal of all metadata from native electronic files before production to the opposing party. Concerns about spoliation are particularly strong for companies and organizations with a large number of employees, but case law suggests that failure to preserve evidence is just as likely to occur where the party is an individual.

It is, of course, the duty of counsel to make sure that all potentially relevant documents are preserved, including without exception ESI. Many entities now have affirmative duties to retain certain documents in accordance with administrative regulations or statutes (such as Sarbanes-Oxley). Accordingly, most businesses and organizations are already advised to have a regular document preservation policy in place, and to follow it closely. Beyond this general affirmative duty to retain information, corporate counsel typically also circulate a "litigation hold" letter to all relevant employees at the onset of litigation. While it is generally accepted that the specific obligation to preserve evidence relevant to the litigation attaches at the time the complaint is filed, the growing trend is to attach the obligation as soon as the party has knowledge that the information may be relevant to a potential claim. At least one commentator, however, has argued that attaching a duty to preserve at the moment litigation may be anticipated effectively creates a permanent disruption in ordinary document destruction procedures, especially for organizations and corporations that are frequently sued.¹⁶

The preservation of ESI, like its production, is more complicated than with paper documents. Unlike paper documents, in which information is preserved in a tangible medium, a "distinctive feature of computer operations" is that the routine alteration and deletion of information attends ordinary use.¹⁷ Routine alteration and deletion may include, for example, automatic deletion of e-mails after a set period of time, deletion of e-commerce transaction journals that record credit card purchases, and databases that update accounts receivable in real time. Parties cannot reasonably be held responsible for changes to data that occur without conscious human intervention. Accordingly, some litigant representatives have sought

a "safe harbor" for information destroyed through ordinary or good faith computer use. Such a "safe harbor" was codified in the amendments to Federal Rule of Civil Procedure 37(f), which now provides that:

Absent exceptional circumstances, a court may not impose sanctions under these rules 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.

Rule 37(f) has been interpreted to apply in the very narrow circumstances involving (1) the routine operation of an electronic information system, (2) a party acting in good faith (*i.e.*, complying with a court order or party agreement, to the extent one exists), and (3) no independent duty to preserve evidence. Proponents of the amendment have pointed out that it would only apply to good faith loss of information, and would not shield parties from sanctions who intentionally destroy specific information due to its relationship to litigation, or who allow such information to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system. The Rule therefore gives a modicum of comfort to those who regularly create and store electronic information that they will not be punished merely because their business—or everyday lives—require regular computer use.

Rule 37(f), however, was not greeted with unanimous accolades prior to its adoption. Judge Scheindlin, the author of the *Zubulake* opinions, argued that the "safe harbor" of Rule 37(f) was unnecessary, since the typical sanctioned party was not one who had lost information in good faith through the routine operation of a computer, but rather one who had destroyed electronic information in violation of a court order, in a willful or bad faith manner, or in a way that had caused prejudice to the opposing party. Others have argued that Rule 37(f) is skewed heavily to benefit large corporations by encouraging destruction of data on a more frequent basis. As of this writing in the spring of 2007, Rule 37(f) is facing its first significant test in an antitrust suit between computer chip designers Intel and AMD.¹⁸ In March 2007, Intel admitted that despite implementing a "litigation hold" on e-mails for 1000 employees after the suit was filed in June 2005, it lost many e-mails from key employees and witnesses. The court appointed a special master to investigate the circumstances of the missing e-mails. Based on the special master's eventual findings, Intel may become the first major company to face sanctions despite Rule 37(f)'s apparent "safe harbor."

The "good faith" principles embodied in Rule 37(f) may be an appropriate starting point for courts wishing to address spoliation issues. Good faith, however, is only part of the spoliation discussion. Indeed, a comprehensive approach to sanctions for the spoliation of electronic evidence must include not only an analysis of whether the information was destroyed in bad faith, but also the likelihood that the evidence was actually lost (not just deleted) and, if so, the prejudice to the opposing party from the loss.

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

In March 2007, Intel admitted that despite *implementing* a *"litigation hold" on* e-mails for 1,000 employees after the suit was filed in June 2005, it lost many e-mails from key employees and witnesses. The court appointed a special master to investigate the circumstances of the missing e-mails. Based on the special master's eventual findings, Intel may become the first major company to face sanctions despite Federal Rule 37(f)'s apparent "safe harbor."

II. THE LITIGANT'S APPROACH TO E-DISCOVERY

One commentator has noted that willfulness and prejudice usually operate on a sliding scale: if one exists very strongly, sanctions may be appropriate even if the other is weak or even nonexistent. As noted above, deletion of ESI frequently does not result in its actual destruction. Rather, the information is merely rendered "inaccessible," and it may be possible to restore it through backup tapes. If the information can be restored and produced to the requesting party in a timely manner, there is little or no prejudice to the requesting party *even if the information was initially deleted willfully or in bad faith*. Therefore, bad faith alone cannot lead to a spoliation instruction, because the information itself may not be lost.

Furthermore, even if the information is lost, sanctions may not be appropriate if the opposing party has not suffered prejudice. Judge Scheindlin has argued that prejudice is as significant a factor as willfulness in determining the appropriateness and severity of sanctions, although she acknowledges that willfulness and prejudice usually operate on a sliding scale: if one exists very strongly, sanctions may be appropriate even if the other is weak or even nonexistent.¹⁹ Prejudice may be alleviated by requiring the parties to confer early in the litigation and negotiate their own stipulation about what data should and should not be produced; if each party understands its obligations from the outset, it is somewhat less likely that they will be surprised or prejudiced later in the litigation.

Just as the retention and collection of electronic information poses special challenges for litigants, preparing that information for production and reviewing the materials produced by opposing parties raises particular challenges for attorneys. It is well-settled that electronically stored information is as discoverable as information written on paper. But preparing that information for production is considerably more complicated. First, attorneys must choose between a host of competing production formats: should the information be printed out? Produced in its native format? Converted to an electronic image such as a PDF or TIFF file? Second, the information must be reviewed for privilege, a task made considerably more difficult by a high volume of electronic information. Preventing privileged information from slipping through the cracks may become exponentially more difficult when a voluminous amount of ESI is involved. Third, attorneys must consider the most efficient and cost-effective ways to review the information they receive through discovery, again taking into account the volume and quality of information likely to be produced.

A. FORM OF PRODUCTION

When a document is available only in paper form, providing a paper copy is a simple process. But for information stored electronically, the form of production can be much more complex. The same information may be delivered in hard copy, imaged to an unalterable electronic file (such as a TIFF file), or produced as a native file, with each method carrying its own benefits and drawbacks.

Native files are files in their original electronic format, which are read (and manipulated) by programs such as Microsoft Word, Excel, Outlook or Access. Native files can easily be searched or sorted, and may include metadata and "hidden" comments. Because of this manipulability, however, native files are also susceptible to accidental or intentional alteration. Among the challenges to producing native files in discovery are: (1) maintaining document integrity, (2) the inability to label individual pages with Bates numbers, (3) the inability to redact privileged material, (4) the inability of receiving parties to read files originating on less commonly used software, and (5) difficulty in using native files in depositions, motion practice, or at trial.

PDF files are created from native files, and provide a snapshot of the native file at the time the PDF was created. A PDF file cannot be manipulated or altered like a native file, and may not disclose metadata or hidden data about the native file. But while they are more permanent than native files and sometimes can be text searchable, PDF files may have less utility than native files. For example, a large spreadsheet in native format can be sorted by category, allowing the user to search for specific entries. A PDF form, by contrast, cannot be sorted, and may be only marginally more useful than reviewing the spreadsheet on paper.

III. THE LAWYER'S APPROACH TO E-DISCOVERY



The more ESI there is to review, the higher the likelihood that information subject to the attorney-client privilege or the attorney work product doctrine will be inadvertently produced.

III. THE LAWYER'S APPROACH TO E-DISCOVERY

One of the greatest emerging costs in electronic discovery is the cost of screening ESI for privileged communications. The exponential growth in discoverable information has led to a commensurate growth in the time needed to review that information. TIFF files, like PDF files, are created from native files and work essentially as an electronic "picture" of the native file. TIFF files can easily show text and graphics. They can be individually Bates numbered and may be text searchable. (Not all TIFF files, however, are automatically searchable.) Like PDF files, TIFF files do not allow the recipient to see any metadata or hidden data that would otherwise be available in a native file.

As with cost issues, debates over the form of production can frequently be resolved by a conference early in the litigation about the types of electronic information each party is likely to request and what type of information is actually available. Where corporate parties are involved, the most productive conferences typically include information technology (IT) representatives who can speak directly to the company's technical processes and capabilities. Federal courts in the District of New Jersey even require parties to identify an IT representative to address discovery inquiries. If IT personnel do not attend, each party's representatives nevertheless should be well versed in the company's technological capabilities.

Early intervention on the form of electronic discovery allows the court (or better, the parties themselves) to fashion remedies before discovery costs skyrocket. For example, if there is a concern that the opposing party will tamper with native files (willfully or accidentally), the court can require the implanting of anti-tampering technology or allow the producing party to produce an identical copy of the files to the court at the same time so the character of the original production is preserved. To prevent abuse regarding the form of production, the court may also wish to design default rules specifying how ESI is to be produced or to allow the requesting party to specify the format it prefers. The latter approach is the default position of the new Federal Rules, and has the advantage of requiring the parties to think carefully about (and hopefully discuss together) the most useful production format.

B. WAIVER OF PRIVILEGE THROUGH INADVERTENT DISCLOSURE

One of the greatest emerging costs in electronic discovery is the cost of screening ESI for privileged communications. The exponential growth in discoverable information has led to a commensurate growth in the time needed to review that information. Furthermore, the more ESI there is to review, the higher the likelihood that information subject to the attorney-client privilege or the attorney work product doctrine will be inadvertently produced. Lawyers have a fixed amount of time each day and a finite ability to concentrate on reviewing ESI; when the volume of information to be reviewed grows rapidly, even the most conscientious and well-meaning attorneys are more likely to let privileged information slip through pre-production screening. As the amount of privileged information that are accidentally produced goes up, so does the number of disputes over its return.

Courts can—and still do—use traditional approaches to privilege waiver in electronic contexts. The problem is that there is not one but at least three "traditional" approaches, each with radically different consequences. A strict liability approach, for example, holds that any inadvertent disclosure is a waiver of privilege, while an "intent-required" approach waives privilege only when the producing party knowingly makes the disclosure. Moreover, one commentator has asserted that the standards used to determine whether an inadvertent disclosure waives the privilege "are inconsistent and inconsistently applied—both at the federal and state levels."²⁰ As a result, the same inadvertent disclosure could constitute an absolute waiver of privilege in front of one judge and a non-waiver in front of another—even within the same jurisdiction. This uncertainty may invite forum shopping among parties who recognize early on that significant electronic discovery is likely.

From the attorneys' perspective, then, none of the traditional approaches works very well. Lawyers desire the flexibility to retrieve an inadvertently produced document but, on the other hand, they need the stability of knowing that evidence they intend to introduce at summary judgment or at trial will not be demanded back from opposing counsel at the last minute. To balance these concerns, more and more lawyers are reaching agreements among themselves (often with the court's express blessing) to produce documents subject to a "claw-back" or "quick peek" provision. A "claw back" agreement allows the producing party to demand the return of an inadvertently produced privileged document within some "reasonable" time after the production. A "quick peek" agreement allows the requesting party to inspect the producing party's documents in order to identify those which it would like to have produced, which the producing party subsequently reviews for privilege before production.

Both the "claw-back" and "quick peek" approaches have become accepted solutions to the privilege dilemma, and have been codified in formal rules and guidelines. The ABA Civil Discovery Standards combine the two options, and expressly suggest that parties reach their own stipulation about how to handle inadvertent privilege waiver. After significant debate, Federal Rule of Civil Procedure 26(b)(5) was also amended to include a claw-back provision, subject to the receiving party's right to petition the court under seal to keep the document. Under the amended rule, there is no deadline for requests for the return of documents; conceivably, many weeks or months could pass before the request is made, but the receiving party would still have to return, destroy or sequester the inadvertently produced documents. However, the court retains the power to examine whether an unreasonable delay resulted in a privilege waiver. Texas's "claw back" rule, by contrast, gives the producing party only ten days to request return of a document after the party learns of the inadvertent production.²¹

III. THE LAWYER'S APPROACH TO E-DISCOVERY

Both the "claw-back" and "quick peek" approaches have become accepted solutions to the privilege dilemma, and have been codified in formal rules and guidelines. The ABA Civil Discovery Standards combine the two options, and expressly suggest that parties reach their own stipulation about how to handle inadvertent privilege waiver.

III. THE LAWYER'S APPROACH TO E-DISCOVERY

Critics argue that the "quick peek" and "claw back" approaches provide false comfort because once opposing counsel has seen a privileged document, the information is in her head forever; even if the document is returned, the proverbial genie is out of the bottle.

The growing acceptance of these approaches, however, has not silenced critics, who claim that they cut against both established law concerning the waiver of privilege and the Rules of Professional Conduct in most jurisdictions. Critics also argue that the "quick peek" and "claw back" approaches provide false comfort because once opposing counsel has seen a privileged document, the information is in her head forever; even if the document is returned, the proverbial genie is out of the bottle, and opposing counsel can use the information to develop a litigation strategy going forward. Opponents of "claw back" agreements also note the difficulty or impossibility of enforcing such agreements against non-parties to the suit. If a document is inadvertently produced and bears no confidentiality stamp, it may be disclosed to non-parties who are under no specific obligation to return the information. Finally, "claw back" agreements are open to abuse from a timing perspective: unless there is a set deadline for demanding the return of documents, receiving parties cannot proceed with the confidence that the documents they intend to use at trial or in a dispositive motion will not be "clawed back" at the last minute. Judges approving "claw back" agreements should carefully consider whether they adequately protect the interests of all parties.

A related problem posed by e-discovery is the broad application of subject matter waiver to information otherwise privileged or covered by the attorney work product doctrine. In some jurisdictions, the inadvertent production of any piece of privileged information constitutes a waiver of privilege for all information regarding that subject matter. Given the sheer volume of ESI in many cases, however, broad application of subject matter waiver would provide virtually no protection at all to parties producing ESI. Accordingly, some have proposed expanding the doctrine of "selective waiver" for ESI, which would limit waiver of privilege to the specific information inadvertently produced. Proposed changes to Federal Rule of Evidence 502 attempt to accomplish exactly that. he scope and nature of electronic discovery disputes tend to be driven by the litigant and attorney concerns discussed above. The court, however, has an obvious role in guiding parties through the e-discovery process in as efficient a manner as possible. To this end, courts have three fundamental responsibilities specifically with respect to e-discovery issues: (1) to facilitate resolution of e-discovery disputes, either by promulgating specific rules and protocols or by letting case law on the subject develop organically, or both; (2) to monitor new technological developments that may impact how e-discovery is conducted and what is discoverable; and (3) to think proactively about the next major development to hit the courts: the use of ESI in motion practice and at trial.

A. DEVELOPING E-DISCOVERY PROCEDURES: FEDERAL AND STATE COURT EXPERIENCES

The federal courts have been wrestling with discovery issues concerning electronically stored information for more than a quarter-century. Beginning in the late 1990's, however, the number of disputes over electronic discovery exploded. An increasing number of courts struggled to apply existing discovery rules to difficult new problems posed by electronic information, including cost and form of reproduction, accidental privilege waiver, and sanctions. Two lines of cases, the aforementioned *Zubulake* as well as *Rowe Entertainment*, *Inc. v. William Morris Agency, Inc.*,²² distinguished themselves as offering thoughtful solutions to the issue of undue burden and appropriate cost-shifting for production of electronically stored information. For the most part, however, courts had little to work with as they faced the discovery challenges of a digital world.

Certain federal courts responded by implementing their own local rules or guidelines for handling electronic discovery.²³ Some, like the U.S. District Court for the District of Maryland, have recently implemented extensive protocols for the discovery of ESI.²⁴ While the degree to which local rules and protocols were actually used varied by judge, they represented an effort to give critical thought to the growing issues surrounding electronic discovery.

The growth of e-discovery at the turn of the twenty-first century also led to the formation of the Sedona Conference Working Group on Electronic Document Production, a collection of attorneys and consultants with e-discovery experience. In March 2003, the Working Group issued its draft set of fourteen electronic discovery guidelines known as the Sedona Principles. As the Working Group explained, it had become evident that all electronically stored data may be saved and available for litigation, and "[i]t seemed doubtful to us that the normal development of case law would yield, in a timely manner, best practices for organizations to follow in the production of electronic documents." The Sedona Principles have been revised and refined several times since 2003, but the fourteen principles remain largely the same, and their mere presence has informed the discussion at the federal level.

IV. THE COURTS & E-DISCOVERY: Issues and Recommended Approaches



The number of disputes over electronic discovery has exploded. An increasing number of courts have struggled to apply existing discovery rules to difficult new problems posed by electronic information, including cost and form of reproduction, accidental privilege waiver, and sanctions. IV. THE COURTS & E-DISCOVERY: Issues and Recommended Approaches

At present, there is no universally accepted set of approaches to resolving the issues posed by electronic discovery. Part of the reason may be that the issues that plague e-discovery cost, delay, privilege, and spoliation are not unique to electronically stored information, but rather are endemic to any system of largely unfettered discovery. A concerted effort to provide uniformity in the federal courts began in early 2000, when the federal Civil Rules Advisory Committee held its conference to discuss electronic discovery issues. By August 2004, the Advisory Committee had developed an initial draft of proposed amendments to the Federal Rules of Civil Procedure. After several rounds of drafting, the final amendments were adopted by the Judicial Conference of the United States in September 2005 and later approved by the U.S. Supreme Court. The rules went into effect on December 1, 2006. The final rules codified a number of approaches developed through federal case law, particularly in the *Zubulake* line of cases. However, as noted above, they were not universally applauded.

Perhaps spurred on by the work of the Civil Rules Advisory Committee, several other groups have floated their own proposals for e-discovery standards at the state level. Some, like the Conference of Chief Justices Working Group on E-Discovery and the National Judicial College, have proposed their own guidelines which are separate from the Federal Rules, while still addressing the same concerns of cost, privilege and delay. Others, like the National Conference of Commissioners on Uniform State Laws, have promoted policies that largely echo the Federal Rules, based on the conclusion that the salient issues in electronic discovery were exhaustively debated during the six-year process of passing the new federal amendments, and that there was to need "to reinvent the wheel." In addition, some commentators and groups have made a significant push for states to adopt the Federal Rules in the interest of promoting uniformity across courts.²⁵

At present, there is no universally accepted set of approaches to resolving the issues posed by electronic discovery. Part of the reason may be that the issues that plague e-discovery—cost, delay, privilege, and spoliation—are not unique to electronically stored information, but rather are endemic to any system of largely unfettered discovery. Still, within the current discovery system are solutions for keeping the use of e-discovery appropriate. As the parties' concerns rise over the volume of information produced, costs, and privilege, so do the court's concerns about relevance, overbreadth, and undue burden.

B. GENERAL RECOMMENDATIONS FOR JUDGES APPROACHING E-DISCOVERY DISPUTES

Whether or not your jurisdiction has adopted formal rules applying to e-discovery, there are a number of strategies you can use to help the parties reap the benefits and avoid the horrors of ESI production.

• Use existing rules governing production of information. Every jurisdiction already has rules in place that govern the discovery process and allow the court to stop excessive or burdensome discovery. If it is not readily apparent why certain electronically stored information should be produced, challenge the parties to explain why it is absolutely necessary. It may well be that e-mails from ten years ago, or a legacy database that

would require expensive restoration, would be relevant, but before going through a complicated balancing test to determine who should pay, let the parties convince you that the information is needed in the first place.

- Encourage or require early conferencing. Many potential disputes over electronic discovery may be prevented or narrowed early in the litigation. An early conference reminds producing parties about their preservation obligations, and may allow requesting parties to refine the scope of their demands. Parties can discuss the form, method, and potential costs of production before production commences, lowering the possibility of a future dispute. Where possible, inclusion of the parties' IT professionals can help streamline the discussion.
- Let the parties educate you about the technology. Courts are not expected to be experts in information technology. If a dispute arises and the technology is unfamiliar, request a tutorial. Ultimately, to "adjudicate disputes in this area, courts will need to understand the highly variable [computer] systems at issue in order to assess the burden and cost of extracting information from them."²⁶
- Keep apprised of technological solutions to e-discovery disputes. To the extent technology exists that can assist the parties and cut through disputes, encourage the parties to use it. New technologies can run faster searches of ESI, and allow the information to be shared in more useful formats. You quickly may become more familiar with certain applicable technology than the parties who appear before you; encourage those parties to use the technology to their advantage.
- To the extent possible, let the parties work out their own agreements. There are different ways to address the return of inadvertently produced documents, the form of production, or the allocation of cost. The parties and their experts are in the best position to tailor the right solutions for their case. Even if your jurisdiction establishes rules or guidelines, you may want to allow the parties to contract around them.
- Recognize that e-discovery issues can raise the stakes—and the blood pressure—of the parties. Litigation is often unpleasant and stressful even under the best of circumstances. Having to produce millions of company e-mails, and the cost and privacy issues associated with that production, makes matters worse. The courts cannot mollify every litigant, of course, but a clear grasp on the issues will help resolve the issues in an expedient and effective fashion.
- Think ahead to how the requested ESI will be used in the courtroom, and challenge the parties to do the same. Traditional paper discovery, of course, is designed in part to uncover the critical documents that parties expect to introduce at trial or on summary judgment. In this respect, electronic discovery is no different. Particularly as

IV. THE COURTS & E-DISCOVERY: Issues and Recommended Approaches

Many potential disputes over electronic discovery may be prevented or narrowed early in the litigation. Where possible, inclusion of the parties' IT professionals can help streamline the discussion.

IV. THE COURTS & E-DISCOVERY: Issues and Recommended Approaches

litigants seek ESI that does not readily transfer to documentary form—such as databases, animations, and video clips—the court and the parties should think early on about how the material will be presented to judge and jury alike in a meaningful way.

E lectronic discovery poses new challenges for the civil justice system, and for individual courts. But even if you are entirely new to the issues surrounding e-discovery, you are not starting from square one. The same principles of case management apply whether the information at stake is digitized or written in pencil; e-discovery merely asks you to transfer those case management traditional skills to an electronic age. One of the keys to managing e-discovery is early intervention in the case, so as to assure that the parties do not engage in unnecessary expense.

For courts that are willing to embrace change, e-discovery offers a special opportunity. Not since the late 1930's, when the current discovery structure emerged, have courts been in such an excellent position to suggest meaningful improvements to the discovery process. Because the universe of e-discovery is so fraught with expense and uncertainty, parties can be amenable to cooperative solutions in ways that historically have not been available. Once established, those cooperative solutions can spill over into traditional discovery as well. As judges, you must remember that delay in addressing e-discovery issues may cause enormous expense to at least one party. One the other hand, a court that understands e-discovery may be uniquely positioned to guide the litigation in a way that works better for all litigants—and for the court itself. The digital world is here to stay. The courts that embrace it will lead the way.

CONCLUSION



Not since the late 1930's, when the current discovery structure emerged, have courts been in such an excellent position to suggest meaningful improvements to the discovery process. Kucala Enters., Ltd. v. Auto Wax Co., Inc., 2003 WL 21230605 (N.D. Ill. May 27, 2003)

Lipco Elec. Corp. v. ASG Consulting Corp., 798 N.Y.S.2d 345 (Sup. Ct., Nassau Co., Aug. 18, 2004) (unpublished disposition)

McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001)

Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 WL 246439 (E.D. La. 2002)

Rowe Ent., Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002)

Toshiba Am. Elec. Components, Inc. v. Superior Ct., 21 Cal. Rptr.3d 532 (Cal. App. 2005)

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005)

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)

GENERAL E-DISCOVERY RESOURCES

Michael Arkfeld, Electronic Discovery and Evidence (2003)

Robert Douglas Brownstone, *Collaborative Navigation of the Stormy E-Discovery Seas*, 10 Rich. J. L. & Tech. 53 (2004)

Adam I. Cohen & David J. Lender, Electronic Discovery: Law & Practice (2004)

Conference of Chief Justices, Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information (August 2006)

Joan E. Feldman, Essentials of Electronic Discovery (2003)

Jay E. Grenig & William C. Gleisner, 1 eDiscovery & Digital Evidence § 6:8 (2006)

Paul W. Grimm et al., Discovery Problems and Their Solutions (2005)

David K. Isom, Electronic Discovery Primer for Judges, 2005 Fed. Cts. L. Rev. 3

James M. Johnston Jr. & Philip A. Whistler, E-Discovery: A Critical Litigation Issue for Franchisors and Franchisees, 26-SUM Franchise L.J. 20 (2006)

Devin Murphy, The Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need to Know, 27 Wm. Mitchell L. Rev. 1825 (2001)

Sharon D. Nelson & John W. Simek, Finding & Securing Electronic Evidence (2002)

George L. Paul & Bruce H. Nearon, The Discovery Revolution: E-Discovery Amendments to the Federal Rules of Civil Procedure (2006)

Pound Civil Justice Institute, The Rule(s) of Law: Electronic Discovery and the Challenge of Rulemaking in the State Courts (2005).

APPENDIX A: E-DISCOVERY RESOURCES

Shira Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation*, 41 B.C. L. Rev. 327 (2000)

Sedona Conference, The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (September 2005)

Howard Speight and Lisa Kelly, *Electronic Discovery: Not Your Father's Discovery*, 37 St. Mary's L.J. 119 (2005)

KEY RESOURCES ON COST OF E-DISCOVERY

Corrine L. Giacobbe, Note, Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data, 57 Wash. & Lee L. Rev. 257, 259 (2000)

Mafe Rajul, *E-Discovery—Can the Producing Party Expect Cost-Shifting?*, 2 Shidler J.L. Com. & Tech. 3 (2005)

Jessica Lynn Repa, Adjudicating Beyond the Scope of Ordinary Business: Why the Inaccessibility Test in Zubulake Unduly Stifles Cost-Shifting During Electronic Discovery, 54 Am. U. L. Rev. 257 (2004)

KEY RESOURCES ON SPOLIATION

J. Brian Beckham, Production, Preservation, and Disclosure of Metadata, 7 Colum. Sci. & Tech. L. Rev. 1 (2006)

Daniel B. Garrie et al., *Hiding the Inaccessible Truth: Amending the Federal Rules to Accommodate Electronic Discovery*, 25 Rev. Litig. 115 (2006)

Shira Scheindlin & Kanchana Wangkeo, *Electronic Discovery in the Twenty-First Century*, 11 Mich. Telecomm. & Tech. L. Rev. 71 (2004)

Lloyd S. van Oostenrijk, Paper or Plastic?: Electronic Discovery and Spoliation in the Digital Age, 42 Hous. L. Rev. 1163 (2005)

KEY RESOURCES ON PRIVILEGE ISSUES

Richard Acello, E-mail to Lawyers: E-Discovery Rules on the Way, ABA J. E-Report, Oct. 7, 2005

Laura Catherine Daniel, Note, The Dubious Origins and Dangers of Clawback and Quick-Peek Agreements: An Argument Against Their Codification in the Federal Rules of Civil Procedure, 47 Wm. & Mary L. Rev. 663 (2005)

Daniel B. Garrie et al., *Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act*, 2005 UCLA J. L. & Tech. 2 (2005)

Dennis Kiker, Waiving the Privilege in a Storm of Data: An Argument for Uniformity and Rationality in Dealing with the Inadvertent Production of Privileged Materials in the Age of Electronically Stored Information, 12 Rich. J.L. & Tech. 15 (2006)

A SHORT GLOSSARY OF E-DISCOVERY TERMS

Byte—the basic unit of memory storage on a computer. Storage capacities on most computers today are measured in gigabytes (GB), or one billion bytes. Increasingly, storage is now being measured in terabytes (TB—one trillion bytes) and petabytes (PB—one quadrillion bytes). As a point of comparison, one petabyte could hold the entire printed collection of the Library of Congress 50 times over.

Claw back agreement—an agreement that allows a producing party in discovery to demand the return of an inadvertently produced privileged document or electronically stored information within some reasonable time after the inadvertent production.

Data-

Active data—data that are easily and currently accessible on a computer or other electronic device.

Archival data-data that are stored separate from an active computer or network, but which can be retrieved in the ordinary course of business-the rough equivalent of offsite storage for paper documents. Some archival data that is rarely used is known as a "dark archive."

Backup data—data that are saved onto a storage medium separate from a computer or computer network, specifically to assist recovery in the case of catastrophic failure. Backup data typically represent a "snapshot" of an entire computer system, and are not deliberately sorted or organized.

Legacy data-data from a computer system that is no longer in use.

Replicant data—data that are automatically created by certain computer systems and programs for short-term recovery in the event of system failure.

Residual data-data that still exist on a computer system even though they have been thought "deleted" by a user.

Deduping-the process of removing duplicate electronic files prior to production.

Disk array—a storage system containing multiple disk drives.

Electronic discovery/e-discovery-the discovery of electronically stored information.

Electronically stored information (ESI)—all information that is stored on an electronic medium, including audio and video files, e-mail messages, instant messages, websites, word processing documents, databases, spreadsheets, digital photos, information created with specialized business or engineering software, and backup and archival copies of that same information.

APPENDIX B: GLOSSARY

APPENDIX B: GLOSSARY

File-

Native file—an electronic file in its original electronic format; that is, the format in which it is most commonly created, read and manipulated.

JPEG file—a file commonly used to store photographic images, particularly for use on the World Wide Web. JPEG files compress the image to save storage space, which reduces file size but also reduces the quality of the image.

PDF file—a PDF file is created from a native file and depicts the same information, but in a less manipulable form that a native file. Essentially, a PDF captures the text or graphics on another file and displays it cleanly. PDF's may be text searchable, but generally cannot be altered or manipulated. PDF's do not allow access to metadata unless the metadata is itself converted to a PDF file.

Temporary file—a file that is designed to store information for a short time, and typically deleted automatically by a computer after use.

TIFF file—a TIFF is created from native files and work essentially as a mapped "picture" of the native file. A TIFF is actually a bit-by-bit graphical representation of the image of the file—the original file is divided into tiny plots, and each plot is separately transferred to recreate the image on the TIFF file. TIFF files can show text and graphics, and may be made text searchable. They do not show metadata. TIFF files may be Bates numbered.

Metadata—information about an electronically stored file that is hidden within the file itself or in a linked database. Metadata usually includes information such as the file's creator, creation date, and dates on which the file was opened, read, modified or printed. Accurate metadata can assist in the authentication of electronic files.

Multimedia—a combination of methods of presenting information, such as the combined use of audio, video, and text files.

OCR—an abbreviation for optical character recognition, a technology that allows a user to scan handwritten or typewritten text into a computer and create a searchable or editable document. This technology is still improving, and does not have 100% accuracy.

Open standards—in contrast to proprietary software designed and marketed by specific corporations, open standards allow data to be read by many different types of computer systems. Older data may be more easily read on open standard systems.

Quick peek agreement—an agreement that allows a requesting party in discovery to inspect the producing party's documents or electronically stored information in order to identify the information it would like to have produced. The producing party then reviews the selected information for privilege before production.

Safe harbor—in the e-discovery context, a term generally referring to rules that protect a party from sanctions when that party, in good faith, inadvertently loses or destroys electronically stored information.

APPENDIX B: GLOSSARY

Sedona Principles—a series of fourteen principles for electronic document production, developed by the Sedona Conference. The Sedona Principles have been influential in the growth and development of e-discovery rules and case law at the federal and state levels.

Source code—the code for a computer program, written in a programming language that is readable by humans. Source code may be relevant in certain cases, such as those involving intellectual property claims for a computer program.

Tape—a common form of storing electronic data, now being replaced rapidly by disk drives. Because of the speed of technological advancement, tapes more than four years old are usually not compatible with current computer systems, and the ESI they contain is not readily accessible.

True deletion—a process by which electronic files are permanently and irretrievably removed from a hard drive, and cannot be restored.

URL-an address on the World Wide Web, such as http://www.du.edu/legalinstitute.

NOTES

- Transcript of testimony of Greg McCurdy, on behalf of Microsoft Corp. (04-CV-001) at 5, quoted in George L. Paul & Bruce H. NEARON, THE DISCOVERY REVOLUTION: E-DISCOVERY AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE 17 (2006).
- Robert Douglas Brownstone, Collaborative Navigation of the Stormy E-Discovery Seas, 10 RICH. J.L. & TECH. 53, *21 (2004).
- 3. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 327 (2000).
- 4. See, e.g., McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) ("Unlike a labeled file cabinet or paper files organized under an index, the collection of data by the backup tapes in this case was random.... It is therefore impossible to know in advance what is on these backup tapes.").
- 5. Rowe Ent., Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002).
- 6. Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 WL 246439, *3 (E.D. La. 2002).
- See Pete S. Michaels & Derek C. Anderson, Applying Zubulake in Securities Arbitrations: When Is Cost-Shifting Appropriate?, 1554 PLI/Corp 71, 81 (2006).
- 8. McPeek, 202 F.R.D. at 33.
- 9. 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I).
- 10. See Daniel B. Garrie et al., *Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act*, 2005 U.C.L.A. J. L. & TECH. 2 (2005).
- 11. PAUL & NEARON, supra note 1, at 134.
- 12. See Sarah A.S. Phillips, Discoverability of Electronic Data Under the Proposed Amendments to the Federal Rules of Civil Procedure: How Effective Are Proposed Protections for "Not Reasonably Accessible" Data?, 83 N.C. L. REV. 984, 1010 (2005).
- 13. See Miss. R. Civ. P. 26(b)(5) (providing that "If the court orders the responding party to comply with the request, the court *may* also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.")(emphasis added).
- 14. Toshiba Am. Elec. Components, Inc. v. Superior Ct., 124 Cal.App. 4th 762, 773 (2004).
- See Lipco Elec. Corp. v. ASG Consulting Corp., 798 N.Y.S.2d 345, *9 (Sup. Ct., Nassau Co., Aug. 18, 2004) (unpublished disposition).
- 16. Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 624-25 (2001).
- 17. Fed. R. Civ. P. 37(f) advisory committee's note.

In re Intel Corp. Microprocessor Antitrust Litig., MDL Docket No. 05-1717-JJF, Civ. A. No. 05-441-JJF (U.S.D.C., D. Del.).

- 19. Shira Scheindlin & Kanchana Wangkeo, *Electronic Discovery in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71, 89 (2004).
- 20. See Dennis R. Kiker, Waiving the Privilege in a Storm of Data: An Argument for Uniformity and Rationality in Dealing with the Inadvertent Production of Privileged Materials in the Age of Electronically Stored Information, 12 RICH. J.L. & TECH. 15, *25 (2006).
- 21. See Tex. R. Civ. P. 193.3.
- 22. 205 F.R.D. 421 (S.D.N.Y. 2002).
- See, e.g., U.S. Dist. Ct. Ark. L. R. 26.1; U.S. Dist. Ct. N.J. L. R. 26.1(d); U.S. Dist. Ct. Wyo. L. R. 26.1(d)(3)(B). These rules and guidelines were superseded by the amendments to the Federal Rules of Civil Procedure in December 2006.
- 24. Suggested Protocol for Discovery of Electronically Stored Information ("ESI"), *available at* http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited May 9, 2007).
- 25. It is worth noting, however, that recent scholarship suggests that state conformity with federal rules, an accelerating trend throughout the 1980's, "substantially reversed itself" in the 1990's and that "[f]ederal procedure is less influential in state courts today than at any time in the past quarter-century." John B. Oakley, *A Fresh Look at the Federal Rules in State Courts*, 3 Nev. L.J. 354, 355 (2003).
- 26. PAUL & NEARON, supra note 1, at 115.



Institute for the Advancement of the American Legal System University of Denver 2044 E. Evans Avenue, Suite 307 Denver, CO 80208 Telephone: 303.871.6600 www.du.edu/legalinstitute