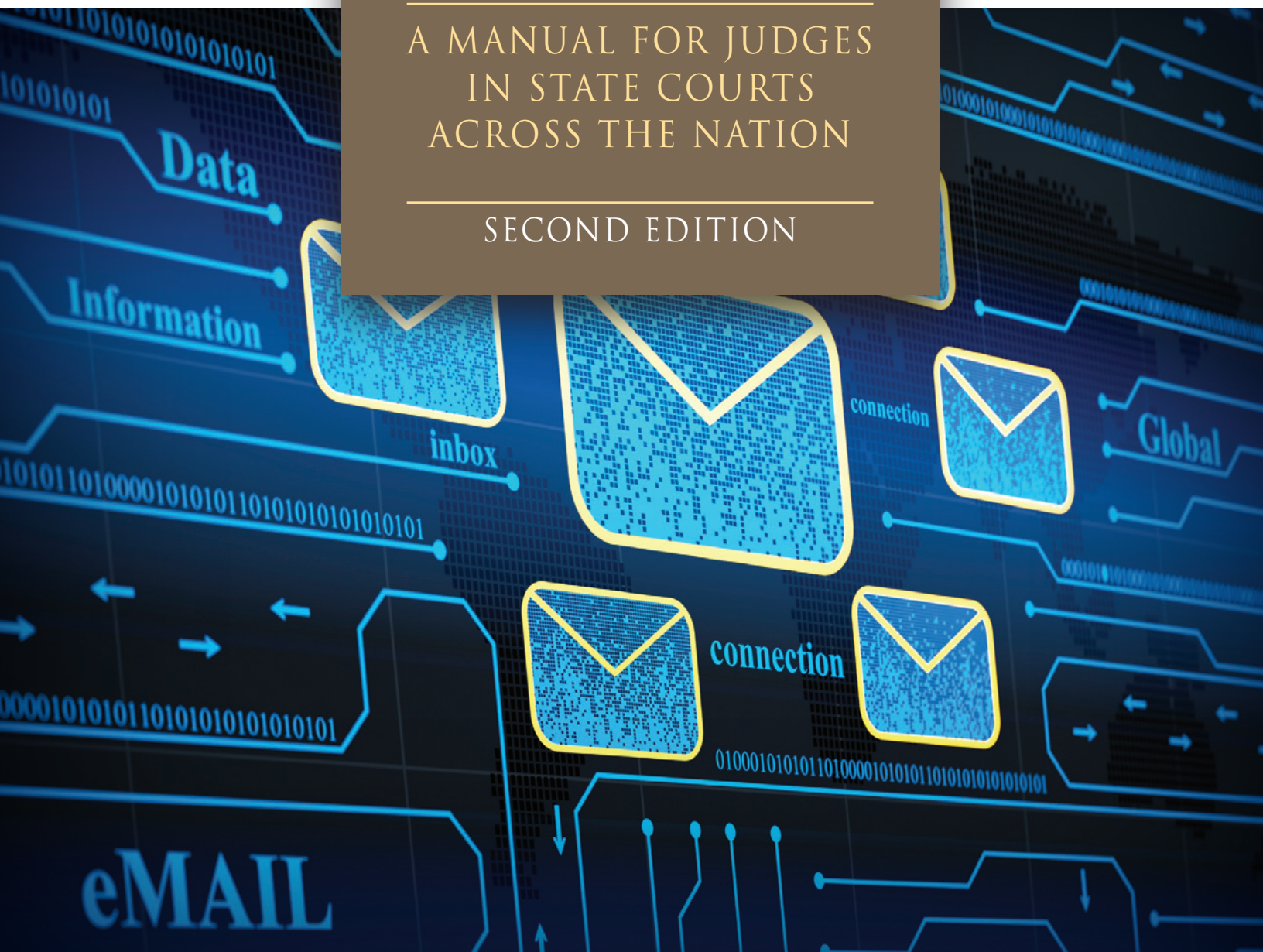


# NAVIGATING THE HAZARDS OF E-DISCOVERY

A MANUAL FOR JUDGES  
IN STATE COURTS  
ACROSS THE NATION

SECOND EDITION







Message

inbox

connection

connection

eMAIL

# NAVIGATING THE HAZARDS OF E-DISCOVERY

---

A MANUAL FOR JUDGES  
IN STATE COURTS  
ACROSS THE NATION

---

SECOND EDITION





INSTITUTE *for the* ADVANCEMENT  
*of the* AMERICAN LEGAL SYSTEM

John Moyer Hall, 2060 South Gaylord Way, Denver, CO 80208

Phone: 303-871-6600

<http://iaals.du.edu>

IAALS, the Institute for the Advancement of the American Legal System, is a national independent research center at the University of Denver dedicated to continuous improvement of the process and culture of the civil justice system. By leveraging a unique blend of empirical and legal research, innovative solutions, broad-based collaboration, communications and ongoing measurement in strategically selected, high-impact areas, IAALS is empowering others with the knowledge, models and will to advance a more accessible, efficient and accountable civil justice system.

Rebecca Love Kourlis      Executive Director

Brittany K.T. Kauffman      Manager, *Rule One Initiative*

Cindy Pham      Student Research Assistant

With special thanks to the Honorable Morris Hoffman  
for his assistance in updating this manual.

For reprint permission please contact IAALS.

Copyright © 2012 IAALS, the Institute for the  
Advancement of the American Legal System.

All rights reserved.



# TABLE OF CONTENTS

A Message From IAALS’ Executive Director . . . . .	1
Introduction . . . . .	2
I. The Nuts and Bolts of E-Discovery . . . . .	5
II. The Litigant’s Approach to E-Discovery . . . . .	8
A. The Cost of Production . . . . .	10
B. Cost Allocation . . . . .	11
C. Preservation of Evidence . . . . .	16
III. The Lawyer’s Approach to E-Discovery . . . . .	20
A. Form of Production . . . . .	20
B. Reviewing ESI for Privilege . . . . .	22
C. Waiver of Privilege Through Inadvertent Disclosure . . . . .	22
IV. The Courts and E-Discovery: Issues and Recommended Approaches . . . . .	26
A. Issues to be Resolved Early: Federal and State Court Experiences . . . . .	26
B. General Recommendations for Judges Approaching E-Discovery Disputes . . . . .	28
Conclusion . . . . .	30
Appendix A: E-Discovery Resources . . . . .	31
Appendix B: Glossary of Key Terms . . . . .	35

# A MESSAGE FROM IAALS' EXECUTIVE DIRECTOR

## MEMBERS OF THE STATE COURT BENCH:

Questions regarding discovery of ESI (electronically stored information) are becoming more and more prevalent in state court litigation. What began as a big-case phenomenon now has the promise of being an every-case phenomenon. ESI includes word processing documents, e-mails, text messages, social media, Twitter, blogs and even voice mail. It also clearly includes technologies yet to be invented or adopted. The question of what is or should be discoverable in that universe of possible ESI is a complex one indeed. Making that decision requires knowledge of the fundamentals of ESI and how discovery of ESI proceeds. What are the litigant's IT systems, if any? How expensive would the requested discovery actually be? What parameters would be reasonable for that discovery?

All of those questions are ones that may well end up before you, the judge, and YOU are in a position to make the system work well, or to allow it to devolve into near-chaos. Making good decisions requires a foundation of good information. You do not need to be "IT experts," but you do need to understand the fundamentals of ESI and e-discovery. The mission of IAALS is to advance a more accessible, efficient, and accountable civil justice system. In service of that goal, our intent here is simply to offer a convenient tool that will provide you with guidance on the subject of e-discovery. 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. We thank all of you for your dedication to serving the public and providing access to justice across the nation.





# 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.*

Electronic 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 paper is to give a careful overview of the language, the law, and the issues inherent in e-discovery so as to better equip judges 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 documents 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 of 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 potentially relevant written communications 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 traditional paper review. If the parties are determined to make discovery difficult or are simply not equipped for the task, 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 narrow discovery disputes in order to keep costs and schedules under control.

The challenges and opportunities posed by e-discovery cannot be ignored. In the early 2000s, 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. That rapidly changed over the course of the decade. By 2005, it was not just the wealthy and sophisticated parties who wrangled over the production of ESI, and disputes were no longer limited to the federal arena. From 70% to 95% of company information was stored solely in electronic form.<sup>1</sup> To address the

<sup>1</sup> Robert D. Brownstone, *Preserve or Perish; Destroy or Drown – eDiscovery Morphs Into Electronic Information Management*, 8 N.C.J.L. & TECH. 1, 2 (2006).





growing difficulties of locating, retrieving, and producing ESI, the Federal Rules of Civil Procedure were amended in 2006.<sup>2</sup> In 2008, Federal Rule of Evidence 502 was enacted to address the waiver of the attorney-client privilege and work-product doctrine. The rule was promulgated in response to the complaint that litigation costs to protect against waiver were becoming prohibitive, particularly in cases involving e-discovery.<sup>3</sup>

Today, ESI has become a fact of life for all courts, at every level. Every kind of civil action, from complex commercial litigation to domestic relations cases, has been influenced by the increased use of electronically stored information. Experts and practitioners at all levels continue to wrestle with best practices and procedures in light of each party's needs. Today 99.9% of all cases involve electronically stored information.<sup>4</sup> Given the exponential growth of ESI, and the associated complexities of its preservation, collection, and production, the Discovery Subcommittee of the Civil Rules Committee is considering additional proposed amendments related to preservation.<sup>5</sup> There are also numerous state and federal jurisdictions around the country that have implemented innovative approaches by rule or other procedure addressing the unique challenges of discovery in an electronic age. Thirty states have enacted e-discovery rules based in whole or in part on the 2006 Amendments as of May, 2012.<sup>6</sup> Similar proposals are being considered or are pending approval in Florida, Massachusetts, and the District of Columbia, while unique approaches have been adopted or are being considered in others, including Texas, Idaho, Mississippi, Texas, Oregon, Pennsylvania, and Utah.<sup>7</sup> Activity has also occurred at the local level.<sup>8</sup>

---

2 See FED. R. CIV. P. 26(b)(2) advisory committee's note ("The amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information.").

3 FED. R. EVID. 502 explanatory note (citing *Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D. Md. 2005) (stating electronic discovery may encompass "millions of documents" and insisting upon "record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation"))).

4 See, e.g., Information Provided to IAALS (May 2012).

5 See Mark Michels, *Federal Judicial Advisory Committee Ponders New E-Discovery Rules*, LAW TECH. NEWS, Apr. 6, 2012, [www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202548101854&slreturn=1](http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202548101854&slreturn=1) (noting that the soonest such an amendment would come into effect is December 2015).

6 See Thomas Y. Allman, *E-Discovery in Federal and State Courts: The Impact of the 2006 Federal Amendments 1-2* (June 1, 2012) (including Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, South Carolina, Tennessee, Utah, Vermont, Virginia, Wisconsin, and Wyoming).

7 See *id.* at 2-3.

8 See *id.* at 6 (pointing to the New York State Bar's *Best Practices in E-Discovery in New York State and Federal Courts* Guidelines, available at <http://www.nysba.org/AM/Template.cfm?Section=Home&Template=/CM/ContentDisplay.cfm&ContentID=58331>).



The Sedona Conference® has been on the forefront of issues related to e-discovery since before the 2006 Amendments, and remains a key player to-day. In 2008, The Sedona Conference® published its Cooperation Proclamation, which calls on jurists, trial attorneys, corporate counsel, government lawyers, and others to “engage in a comprehensive effort to promote pre-trial discovery cooperation.”<sup>9</sup> As an additional example: the Conference of Chief Justices has adopted its own set of *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information*, which draws on the wisdom of its membership and provides practical advice to trial judges.<sup>10</sup> We also commend to the reader IAALS’ and the American College of Trial Lawyers Task Force on Discovery’s Final Report, published in 2009, which recommends a proposed set of Principles to guide improvements to the American civil justice system, including Proposed Principles related to discovery and e-discovery.<sup>11</sup> These and additional publications that discuss e-discovery issues in detail are set out in Appendix A.

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.

---

9 THE SEDONA CONFERENCE®, THE SEDONA CONFERENCE® COOPERATION PROCLAMATION 3 (2008).

10 CONFERENCE OF CHIEF JUSTICES, GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION (2006), *available at* <http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf>.

11 See JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND THE INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM FINAL REPORT (Rev. Apr. 15, 2009). The name of the Task Force was subsequently revised to the Task Force on Discovery and Civil Justice to acknowledge that the problems we identified were not confined to discovery.

# I. THE NUTS AND BOLTS OF E-DISCOVERY

*The volume of information being created is staggering: one Fortune 500 company reports that its employees generate approximately 100 million e-mails each month.*

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. In the six years since the 2006 Amendments, technology has advanced by leaps and bounds. Beyond personal computers, Americans now use smart phones, tablets, social media, and cloud storage. Less than 1% of business information is created on paper. Instead, 99% of the world's information initially exists as a data file.<sup>12</sup> According to one survey, 28% of the companies sampled are using cloud computing, and of those companies, 40% have had to preserve or collect data from the cloud in connection with actual or threatened litigation.<sup>13</sup> Moreover, the volume of information being created is staggering: one Fortune 500 company reports that its employees generate approximately 100 million e-mails each month.<sup>14</sup> Thus, in most disputes, information relevant to the parties' claims and defenses is no longer in a file cabinet but on a hard drive, a phone, or a tablet. In 2006, one commentator noted, "The days of paper-created documents are over."<sup>15</sup> This is even more true today, with the number of electronic documents being generated growing exponentially. 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. For some information, the printed form is effectively unusable.

12 Brownstone, *supra* note 1, at 2.

13 FULBRIGHT & JAWORSKI L.L.P., 8<sup>TH</sup> ANNUAL LITIGATION TRENDS REPORT 52 (2011), available at <http://www.fulbright.com/images/publications/Report3.pdf>.

14 Information Provided to IAALS from Fortune 500 Company (May 2012).

15 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).



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 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 have all but disappeared. 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 upwards of a terabyte of data, or approximately 75,000,000 pages.<sup>16</sup> This is the equivalent of 30,000 boxes of paper.<sup>17</sup>

<sup>16</sup> Information Provided to IAALS (May 2012).

<sup>17</sup> Bob Sweat, OPEN DOOR SOLUTIONS, LLP, WHAT’S YOUR MEASUREMENTS? VERSION 2.0 (2002), available at <http://www.opendoorsolutions.com/downloads/whats-your-measurement.pdf>.





- **CAN BE STORED EASILY.** The price of electronic storage capacity keeps dropping precipitously. 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. And while electronic storage costs are much less than paper, they can still be prohibitive, especially where companies are preserving documents as a result of multiple litigations. One Fortune 500 company reports that it spent approximately \$1.4 million in outside vendor hosting costs in 2011 for its pending litigations.<sup>18</sup>

---

<sup>18</sup> Information Provided to IAALS (May 2012); *see also* NICHOLAS M. PACE & LAURA ZAKARAS, WHERE THE MONEY GOES: UNDERSTANDING LITIGANT EXPENDITURES FOR PRODUCING ELECTRONIC DISCOVERY xix (2012) (noting that preservation has evolved into a significant portion of companies' overall e-discovery expenditures, and in some cases more than production costs).



## II. THE LITIGANT'S APPROACH TO E-DISCOVERY

*On backup tapes, ESI such as e-mails, word processing documents, spreadsheets, websites, multimedia presentations, and the like are all lumped together on the disk without any particular 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.*

In 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 finite by virtue of 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. Think, for example, of engineering plans for a project: is each version a separate document, or is the document more like an evolving organism? In addition to those complexities, 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 may be 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 5¼-inch 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. (Remember microfiche??)

**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 any particular 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. Moreover, because backup data captures 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 (or other user) 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.”<sup>19</sup>

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) sorting through and producing electronic documents and the related cost, including the 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.

---

<sup>19</sup> 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).

## 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 messaging that 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.<sup>20</sup> 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, a federal agency spent over \$6 million responding to an individual defendant's discovery requests. This cost constituted more than 9% of the agency's entire annual budget.<sup>21</sup> Despite such expenditures, given the timing of the production and the failure of the agency to meet the court's deadlines, the court imposed sanctions, concluding the agency's efforts were "not only legally insufficient, but too little too late."<sup>22</sup>

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 are 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.

<sup>20</sup> See, e.g., *McPeck 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.").

<sup>21</sup> In re *Fannie Mae Securities Litig.*, 552 F.3d 814, 817 (D.D.C. 2009).

<sup>22</sup> *Id.* (internal citations omitted).







The bottom line is that electronic discovery can either be much more efficient and tailored than paper discovery might have been – or it can be a nightmare. The difference rests in the hands of the litigants, counsel, and the judge. Given these concerns, a number of solutions have been proposed to lower the costs of electronic production. One idea, requiring the parties to confer on e-discovery issues at the onset of litigation, garnered considerable traction and was adopted as part of the 2006 Amendments to Federal Rules of Civil Procedure 16(b), 26(a)(1) and 26(f).

There are several benefits to early conferencing. At an initial stage in the litigation, parties can discuss which information systems should be subject to preservation and discovery, what the relevant time period for discoverable information should be, whether the information is reasonably accessible to the party that has it, the burden or cost of retrieving and reviewing the information, 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.

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 (*e.g.*, search terms, number of custodians, type of media), (3) suggest that the parties use advanced search techniques or benchmarking standards to electronically search data for relevant and responsive information, (4) order the requesting party to bear some of the discovery costs for requested information not deemed reasonably accessible, and/or (5) 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, 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 outside vendors, all of which comes at a cost. A recent study reported the cost of e-discovery expenditures ranging from \$17,000 to \$27 million per case, with a median value of \$1.8 million.<sup>23</sup>

In evaluating the costs versus benefits of a potential settlement, both parties must factor in the expected cost of electronic discovery. For some, the costs of collecting and reviewing electronic documents are so significant that even proceeding to the discovery phase becomes impossible. 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 \$225,000.<sup>24</sup>

New technology continues to be developed to assist in reviewing and analyzing electronically stored information.<sup>25</sup> New programs are being developed to assist in reducing the amount of data early in the process so that overall costs of review and production can also be reduced.<sup>26</sup> Technological advancements are also lessening the burden and cost of restoring backup tapes.<sup>27</sup> Despite these advancements, however, the costs of storage, collection, and review continue to rise because of the overwhelming increase in the amount of ESI being generated.

The disproportionate allocation of costs to the producing party 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

---

<sup>23</sup> PACE & ZAKARAS, *supra* note 18, at 17.

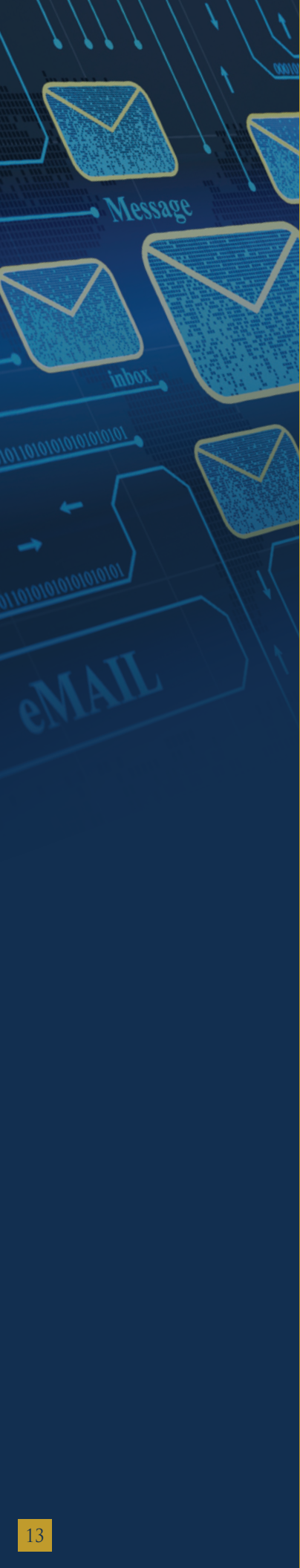
<sup>24</sup> See Pete S. Michaels & Derek C. Anderson, *Applying Zubulake in Securities Arbitrations: When Is Cost-Shifting Appropriate?*, 1554 PLI/CORP 71, 81 (2006).

<sup>25</sup> Jennifer Keadle Mason & Joshua D. Baker, *Using Technology to Reduce E-Discovery Costs*, 1 DRI FOR DEF. 26, 28-30 (2010), available at [http://dritoday.org/articles/2010/01\\_January/FTD-1001-MasonBaker.pdf](http://dritoday.org/articles/2010/01_January/FTD-1001-MasonBaker.pdf).

<sup>26</sup> See *id.* at 28; see also, e.g., CASECENTRAL, <http://www.casecentral.com/> (last visited June 11, 2012); CLEARWELL SYSTEMS, INC., <http://www.clearwellsystems.com> (last visited June 11, 2012); FTI CONSULTING, INC., <http://www.ftitechnology.com> (last visited June 1, 2012).

<sup>27</sup> *Index Engines Wins Gold LTN Award for New Product of the Year*, INDEX ENGINES (Dec. 15, 2009), [http://www.indexengines.com/news\\_release\\_12\\_15\\_09.html](http://www.indexengines.com/news_release_12_15_09.html).





alternative is there? Quill pens?”<sup>28</sup> 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*.<sup>29</sup> 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.

---

<sup>28</sup> *McPeck*, 202 F.R.D. at 33.

<sup>29</sup> *Zubulake v. UBS Warburg LLC (Zubulake I)*, 217 F.R.D. 309 (S.D.N.Y. 2003).



*Zubulake* was 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 its problems. 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 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.

Despite these criticisms, the 2006 Amendments to the Federal Rules of Civil Procedure were heavily influenced by the *Zubulake* approach, basing 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 borrowed heavily from the *Zubulake* factors and introduced seven similar factors as “[a]ppropriate considerations” for evaluating burdens and costs:

- (1) the specificity of the discovery request;
- (2) the quantity of information available from other and more easily accessed sources;
- (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;





- (5) predictions as to the importance and usefulness of the further information;
- (6) the importance of the issues at stake in the litigation; and
- (7) the parties' resources.<sup>30</sup>

There are two key differences between this test and the *Zubulake* court's seven-factor test. First, the Rule-based factors are not hierarchically weighed. That is, a trial court has greater discretion under the Rule to look at all the factors in a Gestalt fashion, and to shift costs in reliance even on the presence of just a single one. Second, the dispositive question under the Rule is whether the information is not reasonably accessible because of undue *burden or cost*, rather than, under *Zubulake*, whether the information is from an accessible or inaccessible *source*. That is, the Rule allows trial courts to shift production costs even for accessible ESI, if the burden of such access is great enough.

Predictably, the amended Rule 26 has also invited criticism – mainly because the Rules themselves provide little guidance as to how to determine whether information is not reasonably accessible due to undue burden or cost. While the Committee Notes suggest sampling to determine accessibility, sampling is still merely a suggestion, and the Rule leaves the entire issue of cost-shifting, including sampling and other methods of determining the cost of accessibility, to the judge's discretion.

Although neither the *Zubulake* test nor the Rule-based test is flawless, courts today still rely on these two basic approaches to decide cost-shifting. That said, a number of federal courts, such as those in the Seventh Circuit, rely on their own cost-shifting tests.<sup>31</sup>

While most states have adopted portions of the 2006 Amendments, including provisions that allow trial judges to shift costs, a handful of states have attempted to address the cost-shifting issue in a more explicit manner and have gravitated toward more bright-line tests than the federal courts. 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 is not available in the ordinary course of business, a test applauded by some as more realistic than whether the data is “accessible.”<sup>32</sup> 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.<sup>33</sup> In a rare decision on discovery

---

30 FED. R. CIV. P. 26(b)(2) advisory committee's note.

31 See *Annex Books, Inc. v. City of Indianapolis*, No. 1:03-CV-918-SEB-TAB, 2012 WL 892170, at \*3 (S.D. Ind. Mar. 14, 2012) (“Within the Seventh Circuit, district courts have used an eight-factor test to determine when it is appropriate to shift costs for seemingly inaccessible data.”); *Clean Harbors Envtl. Services, Inc. v. ESIS, Inc.*, No. 09 C 3789, 2011 WL 1897213, at \*2 (N.D. Ill. May 17, 2011).

32 TEX. R. CIV. P. 196.4.

33 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).

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."<sup>34</sup> 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."<sup>35</sup>

## 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 stored information on an initially inexpensive and essentially permanent basis, creating the expectation that such documents will be retained. The availability of ESI may also be assumed 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 the routine business practice of overwriting backup tapes every few months. It can even happen as advances in data reading leave behind obsolete methods of data recording. For example, NASA has lost data from its earliest moon missions simply because the machines used to read the data were scrapped and cannot be rebuilt. Data preserved on today's CDs and USB thumb-drives similarly may be unreadable to the hardware and software of the future. So these ESI preservation issues encompass not only the retaining of data, but its retention in forms that will be usable in the future.

Of course, 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 spoliation – improper shredding of relevant documents – is not without electronic analogues. Perhaps the most egregious examples involve commercial computer software such as the "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 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

<sup>34</sup> Toshiba Am. Elec. Components, Inc. v. Superior Ct., 124 Cal. App. 4th 762, 773 (Cal. App. 6th Dist. 2004).

<sup>35</sup> See Lipco Elec. Corp. v. ASG Consulting Corp., No. 8775/01, 2004 WL 1949062, at \*9 (N.Y. Sup. Ct. Aug. 18, 2004).







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. Under the comments to Rule 37(f), the specific obligation to preserve evidence relevant to the litigation attaches at the time a party reasonably anticipates litigation, rather than at the time the complaint is actually filed.

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.<sup>36</sup> 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 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. Supporters of the amendment have pointed out that it only applies to good faith loss of information, and does 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, has not received unanimous accolades since its adoption. Judge Scheindlin, the author of the *Zubulake* opinions, has voiced the criticism that since most sources will be held to be reasonably accessible, even if a party somehow overcomes the good-faith hurdle, parties may be sanctioned for incorrectly deciding that the source was not reasonably accessible. Judge Scheindlin has called the rule a “toothless” safe harbor that is “essentially a warning to

---

<sup>36</sup> Fed. R. Civ. P. 37(f) advisory committee’s note.

counsel.<sup>37</sup> Others have argued that courts have not shown a propensity to give the safe harbor broad and ready application. One commenter noted that from 2006 to 2010, only 30 federal court decisions cited to the safe harbor provision. Of these 30 cases, only seven invoked the safe harbor provision to protect a party from sanctions.<sup>38</sup>

Most state courts follow these general principles about preservation. Indeed, the duty to preserve evidence is a common law duty that originated in state court decisions. By contrast, only a few state courts have embraced safe harbor principles akin to Rule 37(f). Moreover, the Discovery Subcommittee of the Civil Rules Committee has been actively studying the rules related to preservation. As of this publication, the scope of any such changes appears limited to potential amendments to Rule 37(e), although there are divergent views regarding the focus and content of any such amendments.<sup>39</sup>

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.

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.<sup>40</sup> In the frequently cited case of *Pension Committee of University of Montreal Pension Plan v. Banc of American Securities*, defendants moved for sanctions before Judge Scheindlin, alleging each plaintiff failed to preserve and produce documents and

37 *The Philip D. Reed Lecture Series: Panel Discussion: Sanctions in Electronic Discovery Cases: Views From the Judges*, 78 *FORDHAM L. REV.* 1, 30-31 (2009).

38 Dan H. Willoughby, Jr. et. al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 *DUKE L.J.* 789, 825-27 (2010).

39 See Discovery Subcommittee Sanctions/Preservation Issues Memo to Rules Committee, Agenda Book, at 249-78 (March 2012), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Civil/CV2012-03.pdf>.

40 Shira Scheindlin & Kanchana Wangkeo, *Electronic Discovery in the Twenty-First Century*, 11 *MICH. TELECOMM. & TECH. L. REV.* 71, 89 (2004).





submitted false and misleading declarations regarding their document collection and preservation efforts.<sup>41</sup>

Judge Scheindlin stated that to determine whether conduct requires the court to impose a sanction for the spoliation of evidence, courts should consider four factors: 1) the level of the party's culpability – whether negligent, grossly negligent, or willful; 2) the interplay between the duty to preserve evidence and the spoliation of evidence; 3) which party should bear the burden of proving that evidence has been lost or destroyed and the consequences resulting from that loss; and 4) the appropriate remedy for the harm caused by the spoliation.<sup>42</sup> Applying these factors, Judge Scheindlin ordered sanctions against all plaintiffs as she found the plaintiffs failed to act diligently and search thoroughly at the time they reasonably anticipated litigation.<sup>43</sup> However, Judge Scheindlin emphasized, “The goal of discovery is to obtain evidence, not to issue sanctions.”<sup>44</sup>

But the federal law on spoliation remains in conflict. In many circuits, sanctions are available so long as there is culpability of some kind, including simple negligence. But others require a showing of bad faith before harsh sanctions such as dismissal or even spoliation instructions may be imposed.<sup>45</sup>

The federal uncertainty about spoliation is mirrored in the states. Even in those states that have adopted counterparts to the 2006 Amendments to federal Rule 37(f), state courts remain in conflict about the extent to which sanctions require culpability, and what exactly culpability means in the context of ESI. The central challenge is how to describe the duty, and failure, to preserve ESI. It might have been one thing under traditional spoliation analysis for a litigant to fail to extend its customary document retention policies, and quite another, for example, for it to fail to invest in new hardware and software necessary to read old data.

The spoliation problem can often be avoided simply by requiring the parties to confer early in the litigation. They might reach their own negotiated stipulations about what data should and should not be produced. Even if they cannot agree, the trial court can make early rulings about the duty to preserve, which will at least remove spoliation issues as regards post-litigation preservation.

---

41 *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F. Supp. 2d 456, 463 (S.D.N.Y. 2010).

42 *Id.*

43 *Id.* at 497.

44 *Id.*

45 *Pension*, 685 F. Supp. 2d at 471-72; *Casale v. Kelly*, 710 F. Supp. 2d 347, 365 (S.D.N.Y. 2010); *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 533 (D. Md. 2010) (“The harshest sanctions may apply not only when both severe prejudice and bad faith are present, but also when, for example, culpability is minimally present, if there is a considerable showing of prejudice, or, alternatively, the prejudice is minimal but the culpability is great, as discussed *infra*. For example, in some, but not all, circuits, conduct that does not rise above ordinary negligence may be sanctioned by dismissal if the resulting prejudice is great.”); *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 614 (S.D. Tex. 2010) (holding that courts may not impose severe sanctions absent evidence of bad faith.); *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, No. 09-60351-CIV, 2010 WL 3368654, at \*12-13 (S.D. Fla. Aug. 23, 2010) (holding that courts may not impose severe sanctions absent evidence of bad faith).



### 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.*

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. Indeed, stand-alone paper data is an increasingly vanishing phenomenon. But preparing ESI for production is considerably more complicated than turning over paper documents.

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 page such as a PDF or TIFF file?

Second, and perhaps even more important, the information must be reviewed for privilege, a task paradoxically made both easier and more difficult by the electronic character of the information.

#### A. FORM OF PRODUCTION

When a document is available only in paper form, providing a paper copy or scanned image 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) the 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.

TIFF files, like PDF files, are created from native files and work essentially as an electronic “printout” 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. Moreover, native files, such as some Excel documents, may be largely unintelligible when turned into a TIFF 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. Federal Rules of Civil Procedure 16(b)(5) and 26(f)(3) now expressly require the parties to meet and confer about e-discovery issues, and the magistrate judge to address e-discovery at the scheduling conference. State rules remain in flux, with only a handful of states – Alaska, Arizona (complex cases only), Arkansas, California, New Hampshire, North Carolina (business cases only), Wisconsin, and Utah – having rules that require ESI to be addressed at this early “meet and confer” stage. But even in states with no such requirements, there is nothing that prohibits trial judges from ordering parties in for an early conference to address ESI issues. In fact, in a set of guidelines prepared for state court judges, the Chief Justice of the United States has recommended, based on the 2006 Amendments to the federal rules, that state court judges encourage parties to meet early to discuss and resolve e-discovery issues.

Addressing ESI early in a case is critical because so many of the common e-discovery issues by their very nature require early resolution. 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 2006 Amendments to the federal rules, and has the advantage of requiring the parties to think carefully about (and hopefully discuss together) the most useful production format.

## B. REVIEWING ESI FOR PRIVILEGE

One of the greatest emerging costs in electronic discovery today is the cost of screening ESI for privileged communications. ESI is usually searchable, so finding potentially privileged drops of data in an ocean of responsive data is theoretically easier than in the old days, when counsel actually had to read through boxes of produced documents looking for privileged ones. In fact, “[i]n many settings involving electronically stored information, reliance solely on a manual search process for the purpose of finding responsive documents may be infeasible or unwarranted. In such cases, the use of automated search methods should be viewed as reasonable, valuable, and even necessary.”<sup>46</sup> Because document review is one of the largest expenses associated with e-discovery, hundreds of private companies now offer electronic discovery services. This includes search and retrieval products, which range from the familiar keyword and natural language searches to much more advanced search methodologies including probabilistic search models, fuzzy search models, clustering searches, and concept and categorization tools.<sup>47</sup>

But complications about how to draft search terms, or apply even more advanced search tools, in a way that efficiently reduces the amount of individual document review, without letting too many privileged documents slip through the mesh, can be an enormous challenge, particularly in jurisdictions, described below, with punitive rules regarding waiver by inadvertent disclosure. Moreover, the larger the amount of electronic material produced in native format, the more likely that privileged content will be disclosed. As Magistrate Judge Grimm has cautioned in an opinion addressing the inadvertent disclosure of electronically stored documents, “[w]hile keyword searches have long been recognized as appropriate and helpful for ESI search and retrieval, there are well-known limitations and risks associated with them, and proper selection and implementation obviously involves technical, if not scientific knowledge.”<sup>48</sup>

## C. WAIVER OF PRIVILEGE THROUGH INADVERTENT DISCLOSURE

The sheer volume of ESI, and the sensitivity and costs of search protocols, makes privilege review even more uncertain than it was when counsel was faced with reviewing hundreds of thousands of paper documents. Preventing privileged information from slipping through the cracks becomes exponentially more difficult when a voluminous amount of ESI is involved. Lawyers have a fixed amount of

<sup>46</sup> The Sedona Conference®, *The Sedona Conference® Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189, 208 (2007).

<sup>47</sup> *Id.* at 217-23.

<sup>48</sup> *Victor Stanley*, 250 F.R.D. at 260 (concluding that the defendants waived any privilege or work-product protection for the disclosed documents and allowing the plaintiff to use the documents as evidence in the case to the extent otherwise admissible).







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 is 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. The strict liability approach holds that any inadvertent disclosure is a waiver of the privilege, while an “intent-required” approach waives the privilege only when the producing party knowingly makes the disclosure. In between these two is the so-called “balancing approach,” which balances several factors to decide whether there has been a waiver, including the impact the finding of waiver will have on both parties. As one commentator has put it, these approaches “are inconsistent and inconsistently applied – both at the federal and state levels.”<sup>49</sup> 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.<sup>50</sup> This uncertainty may in turn invite forum shopping among parties who recognize early on that significant electronic discovery is likely.

Federal Rule of Evidence 502 was enacted in 2008 in an attempt to settle this conceptual uncertainty. Rule 502(b) adopts a different kind of middle approach that does not involve balancing. Under this Rule, the party seeking to avoid a finding of waiver must show each of the following:

- (1) the disclosure is inadvertent;
- (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
- (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).<sup>51</sup>

Because federal Rule 502 is still relatively new and untested, and because the approaches taken in the states continue to be profoundly inconsistent, this issue will remain a difficult one for state court judges and litigants. ESI is so pervasive that

<sup>49</sup> 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).

<sup>50</sup> See *Victor Stanley*, 250 F.R.D. at 259 (“[C]ourts have taken three different approaches when deciding whether the inadvertent production to an adversary of attorney client privileged or work-product protected materials constitutes a waiver.”).

<sup>51</sup> FED. R. EVID. 502(b).

sooner or later almost every producer of it (that is, all of us) will face the problem of inadvertent disclosure. As these issues get litigated, perhaps Rule 502 will help catalyze a move toward standardization.

Until then, this issue will continue to bedevil trial lawyers and their clients. Lawyers need the flexibility to retrieve an inadvertently produced document, but also 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 resolve these concerns, more and more lawyers are reaching agreements among themselves and their clients (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 that 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.

Some states have also addressed these private solutions to the dilemma of inadvertent disclosure, often mirroring the federal approach. But several states have taken different tacks. For example, Texas's "claw back" rule gives the producing party only ten days to request return of a document after the party learns of the inadvertent production.<sup>52</sup>

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

---

<sup>52</sup> See TEX. R. CIV. P. 193.3.





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 his or 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, particularly acute with ESI, is the *scope* of a waiver by inadvertent disclosure. Under Rule 502(a), privilege is generally only waived as to the particular communication disclosed, and not as to the entire subject matter of the communication. A broader subject matter waiver “is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary.”<sup>53</sup> Many states follow this rule, but several still treat the inadvertent production of any piece of privileged information as a waiver of the privilege for all information regarding that subject matter. Given the sheer volume of ESI, and the virtual inevitability of an inadvertent disclosure, this kind of broad application of subject matter waiver seems to make less and less sense.

---

53 FED. R. EVID. 502(a) explanatory note.



The 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 and specific responsibilities with respect to e-discovery issues: (1) to facilitate early resolution of some e-discovery issues; (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 use of ESI in motions practice and at trial.

## A. ISSUES TO BE RESOLVED EARLY: 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 1990s, 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.*,<sup>54</sup> 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.<sup>55</sup> Some, like the U.S. District Court for the District of Maryland, have implemented extensive protocols for the discovery of ESI.<sup>56</sup> 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 electronic data may be saved and available

<sup>54</sup> *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002).

<sup>55</sup> 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.

<sup>56</sup> Suggested Protocol for Discovery of Electronically Stored Information (“ESI”), <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf> (last visited May 9, 2007).

## 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.*





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.”<sup>57</sup> 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.<sup>58</sup> 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 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 2006 Amendments, and that there was no need “to reinvent the wheel.” Commentators and groups have made a significant push for states to adopt the federal rules in the interest of promoting uniformity across courts, and a majority of the states have done so, in whole or in part.<sup>59</sup>

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, solutions exist 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.

---

57 THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (Mar. 2003).

58 See THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: SECOND EDITION BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (June 2007).

59 See Allman, *supra* note 6, at 6.

The Sedona Conference® has also been a leading force in summarizing and analyzing the myriad of different approaches to e-discovery taken by the various states, in statutes, rule-making, and case law. Their resources, listed in the appendix, are a must for any lawyer trying to navigate ESI issues across several states.

## 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. In the world of ESI, where the costs of maintaining, reviewing, and producing information can be astronomical, our comfortably broad definition of what is discoverable may need some practical re-tuning. If it is not readily apparent why certain electronically stored information should be produced, challenge the requesting party to explain why its production is necessary. It may well be that e-mails from ten years ago, or a legacy database which would require expensive restoration, is 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."<sup>60</sup>

---

<sup>60</sup> PAUL & NEARON, *supra* note 15, at 115.







- **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. As a result of your experiences in other ESI cases, you may actually know more about certain applicable technology than the lawyers and parties currently before you. Encourage them to use the technology to their advantage.
- **TO THE EXTENT POSSIBLE, LET THE PARTIES WORK OUT THEIR OWN AGREEMENTS.** There are several different ways to address the return of inadvertently produced documents, the form of production, or the allocation of cost. The parties, in consultation with their experts, are in the best position to tailor the right solution for their case. Even if your state or jurisdiction establishes rules or guidelines, you may want to allow the parties to contract around them. Your approach should be an encouraging push at the beginning stages of litigation, without pushing in any particular direction.
- **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.
- **RULE QUICKLY ON ESI DISPUTES.** The old bromide that it is better for litigants that discovery disputes be resolved quickly than that they be resolved correctly, applies with exaggerated force to ESI. Any uncertainties over issues like data preservation or the effects of inadvertent disclosure will increase the already daunting costs of e-discovery.
- **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 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 in a meaningful way to judge and jury alike.

Electronic discovery continues to pose 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 traditional case management skills to an electronic age. One of the keys to managing e-discovery is early intervention in the case, and consistent oversight 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 1930s, 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. As judges, you must remember that delay in addressing e-discovery issues may cause enormous expense to at least one party. On 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 1930s, when the current discovery structure emerged, have courts been in such an excellent position to suggest meaningful improvements to the discovery process.*



# APPENDIX A:

## E-DISCOVERY RESOURCES

### KEY CASES

---

*Lipco Elec. Corp. v. ASG Consulting Corp.*, No. 8775/01, 2004 WL 1949062, at \*1 (N.Y. Sup. Ct. Aug. 18, 2004) (holding the party seeking discovery should incur the costs incurred in production of discovery material)

*McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001) (discussing the costs and burdens of reproducing backup tapes and cost-shifting)

*Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F. Supp. 2d 456 (S.D.N.Y. 2010) (holding investors' duty to preserve ESI was triggered by the filing of the complaint and spoliation instruction and monetary sanctions were warranted against those investors whose failure to preserve evidence amounted to gross negligence or negligence)

*Rowe Ent., Inc. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002) (discussing the costs and burdens of producing ESI and cost-shifting factors)

*Toshiba Am. Elec. Components, Inc. v. Superior Ct.*, 21 Cal. Rptr.3d 532 (Cal. App. 2005) (holding the state's civil rules to require the requesting party 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")

*Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 259 (D. Md. 2008) (discussing whether inadvertent production to an adversary of attorney client privileged or work-product protected materials constitutes a waiver)

*Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake I*) (establishing a seven-factor test to determine cost-shifting for electronic data discovery)

*Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (*Zubulake III*) (applying the seven-factor cost-shifting test previously laid out in *Zubulake I*)

### GENERAL E-DISCOVERY RESOURCES

---

The 2006 Amendments to the Federal Rules of Civil Procedure, collected at 234 F.R.D. 219 (2006)

Thomas Y. Allman, *State E-Discovery Today: An Update on Rulemaking in Light of the 2006 Federal Amendments*, (THE SEDONA CONFERENCE® April 11, 2011)

Thomas Y. Allman, *Managing E-Discovery After the 2006 and 2008 Amendments: The Second Wave*, 804 PLI/LIT 129, 164 (2009)



Thomas Y. Allman, *E-Discovery in Federal and State Courts: The Impact of the 2006 Federal Amendments* (June 1, 2012)

MICHAEL R. ARKFELD, *ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE* (3d ed. 2011)

William P. Barnette, *Ghost in the Machine: Zubulake Revisited and Other Emerging E-Discovery Issues Under the Amended Federal Rules*, 18 RICH. J.L. & TECH. 11, 67 (2012)

*Bit Rot: The World is Losing its Ability to Reconstruct History*, THE ECONOMIST 16-17 (April 28, 2012), <http://www.economist.com/node/21553445>

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

Robert D. Brownstone, *Preserve or Perish; Destroy or Drown—eDiscovery Morphs Into Electronic Information Management*, 8 N.C.J.L. & TECH. 1, 2 (2006)

ADAM I. COHEN & DAVID J. LENDER, *ELECTRONIC DISCOVERY: LAW & PRACTICE* (2d ed. 2011)

CONFERENCE OF CHIEF JUSTICES, *GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION* (2006), available at <http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf>

Jason Fliegel & Robert Entwisle, *Electronic Discovery in Large Organizations*, 15 RICH. J.L. & TECH. 7 (2009)

PAUL W. GRIMM ET AL., *DISCOVERY PROBLEMS AND THEIR SOLUTIONS* (2d ed. 2010)

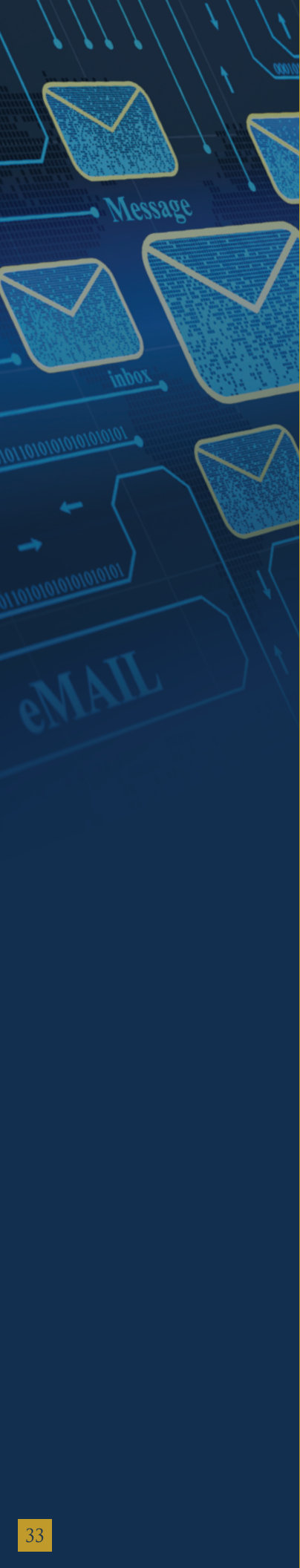
JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND THE INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM FINAL REPORT (Rev. Apr. 15, 2009)

James M. Johnston Jr. & Philip A. Whistler, *E-Discovery: A Critical Litigation Issue for Franchisors and Franchisees*, 26 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)

BARBARA J. ROTHSTEIN ET AL., *MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES* 16 (Federal Judicial Center 2007), *available at* [http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/\\$file/eldscpkt.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf)

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

THE SEDONA CONFERENCE®, *THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE* (September 2005)

The Sedona Conference®, *The Sedona Conference® Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189 (2007)

The Sedona Conference®, *The Sedona Conference® Cooperation Proclamation*, 10 SEDONA CONF. J. 331, 333 (2009 Supp.)

THE SEDONA CONFERENCE®, *Selected State Court Decisions Involving Electronic Discovery* (Kenneth J. Withers, ed., Apr. 25, 2011)

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

## KEY RESOURCES ON COST OF E-DISCOVERY

---

Robert E. Altman & Benjamin Lewis, *Cost-Shifting in ESI Discovery Disputes: A Five Factor Test to Promote Consistency and Set Party Expectations*, 36 N. KY. L. REV. 569 (2009)

Jenna M. Bedsole, *Controlling Costs in E-Discovery*, 72 Ala. Law. 134 (2011)

David Degnan, *Accounting for the Costs of Electronic Discovery*, 12 Minn. J. L. Sci. & Tech. 151 (2011)

NICHOLAS M. PACE & LAURA ZAKARAS, *WHERE THE MONEY GOES: UNDERSTANDING LITIGANT EXPENDITURES FOR PRODUCING ELECTRONIC DISCOVERY* (2012)

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)

Vlad Vainberg, *When Should Discovery Come with a Bill? Assessing Cost Shifting for Electronic Discovery*, 158 U. PA. L. REV. 1523 (2010)

## KEY RESOURCES ON SPOILIATION

---

J. Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1 (2006)

*The Philip D. Reed Lecture Series: Panel Discussion: Sanctions in Electronic Discovery Cases: Views From the Judges*, 78 FORDHAM L. REV. 1, 30-31 (2009)

Shira Scheindlin & Kanchana Wangkeo, *Electronic Discovery in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71 (2004)

Bradley T. Tennis, *Cost-shifting in Electronic Discovery*, 119 YALE L.J. 1113 (2010)

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

Dan H. Willoughby, Jr. et. al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 DUKE L.J. 789 (2010)

## KEY RESOURCES ON PRIVILEGE ISSUES

---

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)

Robert L. Haig, *Attorney-Client Privilege and Work Product Protection*, 795 PLI/ LIT 89 (2009) (“Naturally, the lack of one uniform set of attorney-client privilege rules leads to inconsistency in application, making it difficult to establish procedures that will protect in-house counsel and corporate communications in every jurisdiction.”)

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)





# APPENDIX B:

## GLOSSARY

**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 or work product protected 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 off-site 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 exists on a computer system even though it has 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.

## **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 than 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.

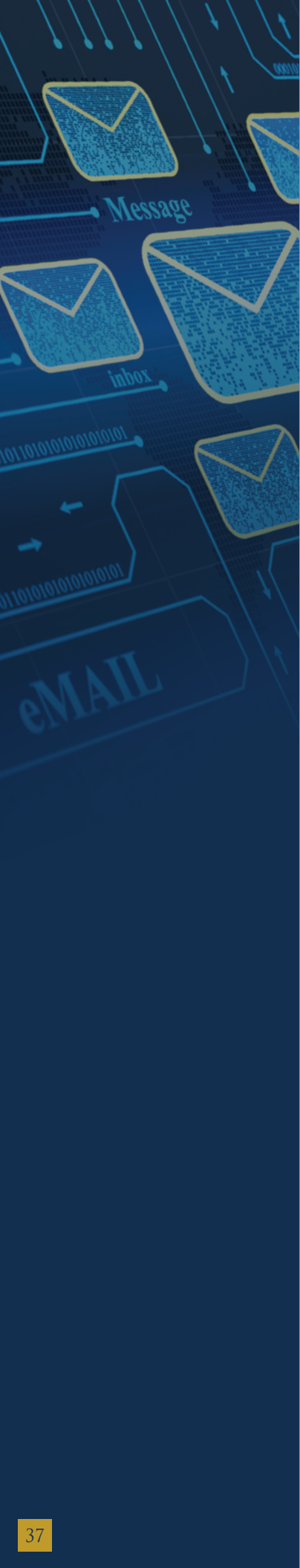
**TEMPORARY FILE** – a file that is designed to store information for a short time, and typically deleted automatically by a computer after use.

**TIFF FILE** – a TIFF is created from native files and works 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 allows 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.

**RESTORATION** – the process of regenerating data that has been lost or corrupted.

**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.

**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.

**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://iaals.du.edu>.





Message

connection

inbox

connection

eMAIL





INSTITUTE *for the* ADVANCEMENT  
*of the* AMERICAN LEGAL SYSTEM



Institute for the Advancement of the American Legal System

University of Denver

John Moyer Hall, 2060 South Gaylord Way

Denver, CO 80208

Phone: 303.871.6600 <http://iaals.du.edu>