

## Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure

Kenneth J. Withers



---

Recommended Citation: Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 7 SEDONA CONF. J. 1 (2006).

Copyright 2006, The Sedona Conference  
Copyright 2006, Kenneth J. Withers

For this and additional publications see:  
<https://thesedonaconference.org/publications>

# ELECTRONICALLY STORED INFORMATION: THE DECEMBER 2006 AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE

---

*Kenneth J. Withers*<sup>1</sup>  
*The Sedona Conference*  
*Sedona, AZ*

## I. INTRODUCTION: JUST ANOTHER DAY IN ELECTRONIC DISCOVERY COURT

Earlier in 2006, in a federal court in New York City, a rather ordinary discovery dispute in a rather ordinary case was decided by a highly capable United States Magistrate Judge. The case was brought by a securities analyst who lost his job after being implicated in an alleged stock manipulation scheme. He was suing two of the companies he regularly analyzed for defamation and tortious interference. The discovery dispute centered on three issues related to the topic of this article -- a motion for an order preserving documents potentially subject to discovery, a discovery "questionnaire" proposed by the plaintiff, and the method by which the defendant would locate responsive documents.

Neither the case nor any of the discovery issues are particularly unusual in our federal courts. What is significant about this case, *Treppel v. Biovail Corp.*,<sup>2</sup> and the Memorandum and Order issued by Judge John Francis, is that it foreshadows the expanded role federal judges will have in resolving discovery disputes after December 1, 2006, when amendments to the Federal Rules of Civil Procedure are anticipated to go into effect nationwide.

Judge Francis faced three electronic discovery questions in the case. First, the plaintiff moved for a preservation order covering email and other electronically stored information. The judge noted that the defendants may have been "shortsighted" in rejecting an offer by the plaintiff for a stipulated preservation order, stating that while preservation orders are not automatic, they are increasingly routine in electronic discovery cases. He then took up the question of when preservation orders for electronic records are warranted and reviewed the various standards courts have used to consider such orders. He rejected the notion that preservation orders must meet the test of injunctive relief, and opted instead for a balancing test taking into consideration the danger of destruction, the content of the endangered records, and the burden of appropriate preservation measures. After consideration of all the factors, he rejected the plaintiff's motion as premature, and in the alternative adopted a questionnaire proposed by the plaintiff to ascertain information about the defendant's electronic records management system.

On the second issue, the defendant objected to the plaintiff's questionnaire, which sought information about the defendant's electronic document retention policies and procedures, as being thinly-disguised interrogatories exceeding the presumptive 25-interrogatory limit imposed by rule.<sup>3</sup> The judge agreed with that characterization, but ordered them to be answered as special or

---

<sup>1</sup> ©2006 Kenneth J. Withers. Before assuming the position of Managing Director of The Sedona Conference, Kenneth J. Withers was on the staff of the Federal Judicial Center (FJC) from September 1999 through December 2005, first as a Research Associate and later as a Senior Education Attorney. During his tenure at the FJC, he was assigned to support the Civil Rules Advisory Committee's work in the area of electronic discovery. The views expressed in the article are entirely his own, and do not necessarily reflect the views of the Federal Judicial Center, the Civil Rules Advisory Committee, or The Sedona Conference.

<sup>2</sup> 233 F.R.D. 363 (S.D.N.Y. 2006).

<sup>3</sup> FED. R. CIV. P. 33(a).

supplemental interrogatories, over the presumptive 25-interrogatory limit, based on his power to grant “leave to serve additional interrogatories... consistent with the principles of Rule 26(b)(2).”<sup>4</sup>

On the third issue, the defendant suggested that before producing electronic information, it enter into a stipulation with the plaintiff defining the scope of electronic discovery by identifying electronic information sources and agreeing upon a set of search terms to be used in an electronic search. The plaintiff refused to enter into a stipulation, taking the position that the use of search terms has no application in standard discovery of accessible electronic records. Judge Francis disagreed, citing case law precedent and *The Sedona Principles* for the proposition that a defined search strategy, including the use of search terms, is appropriate in electronic discovery. Nevertheless, he stated, the refusal of the plaintiff to enter into a stipulation establishing a search methodology -- a “missed opportunity” -- did not relieve the defendant from the duty to respond to the plaintiff’s discovery request, and he ordered the use of selected search terms as an “interim step” at this stage of discovery.<sup>5</sup>

This opinion, which probably strikes the reader as matter-of-fact, sensible, and routine, would have been extraordinary a scant six years ago, when the last major revision of the discovery rules went into effect in federal courts. At that time, in December 2000, there was some recognition among practitioners, judges, and legal scholars that “digital is different,” but little agreement as to what exactly the differences were between the discovery of conventional, paper-based records and correspondence, and discovery of the new digitally created, managed, and stored information. The prevailing view among judges was that whatever differences there may be, the current rules of civil procedure could accommodate them. The handful of reported decisions on electronic discovery disputes analogized the situation to conventional discovery disputes.

On December 1, 2006, a new package of amendments to the Federal Rules of Civil Procedure will likely go into effect. These amendments address the myriad issues associated with the discovery and production of information in digital form--what the amendments call “electronically stored information.” The amendments are the result of five years of study by the Advisory Committee on Civil Rules and an extraordinarily broad, open, and inclusive rulemaking process. They recognize some fundamental differences between paper-based document discovery and the discovery of electronically stored information, and they continue a trend that has become quite pronounced since the 1980’s of expanding the role of judges in actively managing discovery to sharpen its focus, relieve its burdens, and reduce costs on litigants and the judicial system.

This article concentrates on the increased profile of the judge in managing discovery, a role which demands that the judge have a familiarity with the technical aspects of electronic discovery as well as a willingness to use the tools of case management, as demonstrated by Judge Francis in *Treppel v. Biouvail*. Part Two of this article discusses the distinctions between electronically stored information and information stored in conventional documentary form that justify different treatment in the amended rules and shows how judges dealt with these distinctions in the years leading up to the proposed rules. Part Three lays out the amendments themselves, as approved by the Committee on Rules of Practice and Procedure and the Judicial Conference, and currently awaiting submission to Congress by the Supreme Court in May of this year. Part Four discusses recent decisions in federal courts citing, interpreting, and applying the proposed rules as “persuasive authority,” several months before they are anticipated to go into effect.

## II. THE DISTINCTIVE CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

The proposed 2006 package of amendments to the Federal Rules of Civil Procedure were promulgated to address the discovery and production of “electronically stored information.” While neither the amendments nor the accompanying Committee Notes explicitly define that phrase, it is

<sup>4</sup> *Treppel*, 233 F.R.D. at 373 (quoting FED. R. CIV. P. 33(a)).

<sup>5</sup> *Id.* at 374 (citing *The Sedona Principles; Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Principle 11 (2003)).

<sup>6</sup> *Id.* at 374-75.

understood to mean information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. Electronically stored information is distinguished from information derived from “conventional” media, such as writing or images on paper, photographic images, analog recordings, and microfilm.

The distinctions between electronically stored information and conventional information are not based on the sophistication of the technology needed to create, present, or understand the information. After all, the creation and presentation of analog sound recordings or big-screen movies requires technology arguably as sophisticated as computers. The distinctions are in the unique ways digital information is created, modified, communicated, stored, and disposed of by computer systems.<sup>7</sup> The distinctions are also in the ways that computer systems themselves have evolved and are continuing to evolve.

## A. Volume

Perhaps the most significant aspect of electronically stored information, and certainly the most obvious to litigants, attorneys, and judges who have dealt with it, is its sheer volume. While volume is not the only distinction between conventional, paper-based information and every other form that has come before, it is the most striking. Almost 800 megabytes of recorded information is produced per person each year, 92% of which is in magnetically stored form, on computers or computer storage media. To visualize this amount of information, it would take about 30 feet of books to store the equivalent of 800 MB of information on paper.<sup>8</sup> This volume has several causes.

### 1. Replication

The primary cause of the tremendous volume of electronically stored information is that computer systems seldom “move” digital information from one place to another, in the same physical sense that paper media is moved from a desk to a file cabinet, mailbox, or warehouse. Instead, electronically stored information is replicated on media in various physical locations. “Sending” an email message, for example, initiates an electronic process by which a pattern of positively and negatively charged electrons on one computer hard drive is replicated on several other computer hard drives, perhaps around the world, until it reaches the destination hard drive and is rendered as an image on the recipient’s screen. It is also likely to be replicated on several locations on both the sender’s and recipient’s hard drive, as well as on network email servers and their backup media. One message becomes several, a process repeated billions of times daily.

### 2. Electronic communications

Another major contributor to the volume of electronically stored information is the way we use computers increasingly as our primary communication tools, effectively replacing the telephone, postal service, and even face-to-face meetings and private conversation. “Conventional” pre-computer communication methods seldom resulted in the creation of a transcript or recording. However, each time we use instant messaging, Voice Over Internet Protocol, collaboration software, or web-based meeting technology, we create a digital file, subject to the same replication as the email in the example above.

### 3. Digital information defies deletion

Much has been written about the “Delete” key, which does nothing of the sort.<sup>9</sup> By now, all computer users should be aware that the action of “deleting” an electronic file does little more than change the name and eliminate reference to it in the operating system’s list of active files, a situation aptly

---

7 The phrase “computer system” as used here refers to hardware, software, media, peripheral devices, communications infrastructure, and other elements involved in the activities mentioned.

8 See Peter Lyman and Hal R. Varian, *How Much Information?* 2003, at <http://www.sims.berkeley.edu/how-much-info-2003> (last visited Mar. 26, 2006).

9 See, e.g. Hon. James M. Rosenbaum, *In Defense of the Delete Key*, 3 GREEN BAG 2D 393 (2000).

described by computer forensics expert Joan Feldman as a “witness protection program for bad documents.”<sup>10</sup> Not only can the deleted file be easily recovered, but the action of pressing the “delete” key does nothing for the dozens, scores, or hundreds of replicants existing elsewhere on the system, on the network, or on backup media. This fact helps us catch criminals and fraudsters, of course-- but it also frustrates well-intentioned efforts to effectively dispose of outdated, superceded, or surplus electronically stored information.

#### **4. Non-apparent and ancillary electronically stored information**

Not only is there more electronically stored information, but the fact that the information is stored in electronic form gives rise to the creation of ancillary electronic information needed to manage the primary electronic information. Operating system and application software require that electronic files be labeled in order to be stored, retrieved, viewed, managed, and communicated, necessitating the creation of a second level of electronic information commonly referred to as “metadata.” Application software itself provides additional information necessary for the complete understanding and proper manipulation of electronic files, much like the way grammar gives meaning to strings of words in language. Many common business applications, particularly word processing, routinely save each version of an electronic file as it is modified and edited over time, to allow comparison of versions or recovery of past versions. Operating system software generates its own electronic information to manage the files and the interaction of the various elements of the computer system-- input devices such as keyboards and scanners; output devices such as monitors, printers and fax machines; and communication with other computers through networks. The data created to operate the computer system adds to the total amount of electronically stored information.

#### **5. Legacy data**

The fact that access to electronically stored information, and a complete understanding of that information, depends entirely on availability of the appropriate operating system and application software gives rise to another distinction between electronically stored information and information found on conventional media. Off-the-shelf operating system and application software commonly used by business, government, and private individuals is updated at an ever-increasing pace. In a technological environment that is changing constantly, operating system and application software become outdated and unavailable after only a few years. Similarly, the physical media on which digital information is stored, and the hardware needed to retrieve that information, are constantly changing to accommodate advances in technology.<sup>11</sup> Vast quantities of electronically stored information become inaccessible every day, as computer systems are updated without adequate provision for the migration of the data. This “legacy data” does not disappear. It adds to the total volume of electronically stored information.

#### **6. Backup media**

A variant of the legacy data problem, and one that many corporations and government agencies see as the most vexing problem of electronic discovery, is caused by the common procedure of replicating electronically stored information in wholesale fashion at regular intervals for the purpose of restoring the information in the event of catastrophic computer system failure. While this is a laudable procedure for short-term operational purposes, the long-term implications may be catastrophic.

Because the organizational structure of electronically stored information presented to us on our desktops is an artificial construct based on the operating system and metadata, the electronic files on the disaster recovery backup media need not, and generally are not, found in any humanly discernable order. Disaster recovery backup systems are not designed to accommodate the retrieval of individual electronic files, but for wholesale restoration of entire electronic information collections. Retrieving individual files, or files with particular characteristics such as date or author, requires either

<sup>10</sup> Joan Feldman, “Technology Experts Panel,” Presentation Before the Advisory Committee on Civil Rules at Hastings College of Law, San Francisco CA., (March 27, 2000).

<sup>11</sup> When addressing audiences on electronic discovery, I often ask for a show of hands of all those who still have 5-inch floppy disks at their home or office. Invariably a few do, and I then ask what they plan to do if they need the information from those floppy disks. Few have an answer.

complete restoration of the entire collection to an operating system environment similar to that from which it came, or the application of highly specialized search and retrieval software only now becoming available to corporations and law firms.

For reasons known only to Information Technology (IT) staff members and psychologists, backup media are kept for much longer than necessary to meeting disaster recovery needs. Daily backups containing only incremental changes from the day before are kept for a week or more. Weekly backups are kept for months, and monthly backups are kept for years. Many daily backups are retained until the computer system administrators need to recycle the media or they run out of storage space. Boxes of forgotten backups gather dust in storerooms and warehouses, long after the hardware and software needed to retrieve and restore the information have disappeared.<sup>12</sup>

All this digital information—primary files, copies, versions, metadata, the system data, legacy data, backup data—is potentially discoverable in litigation, if it is relevant and not privileged. While the sheer volume of digital information may be enough reason to make a distinction between digital information and information found in conventional documentary form, the same attributes of digital information that create volume also create other problems.

## B. Accessibility

While most paper-based information can be read and understood by reasonably well educated human beings, all electronically stored information must be rendered intelligible by the use of technology - computers, operating systems, and application software. To the extent that the appropriate technology is readily available to render the electronically stored information intelligible, it is considered “accessible.” However, much of the electronically stored information that may be subject to discovery is not easily rendered intelligible with the computers, operating systems, and application software available in every-day business and personal environments. This electronically stored information may be considered “not reasonably accessible” due to the cost and burden associated with rendering it intelligible.

The classic case illustrating both the volume and accessibility problems that distinguish electronic discovery is *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*<sup>13</sup> (commonly referred to as the “*Morgan Stanley*” case). The litigation had its genesis in the sale of the Coleman camping and outdoor sports equipment company to Sunbeam in 1998, in which financier Ronald Perelman exchanged his controlling interest in Coleman for Sunbeam stock, valued at \$650 million at the time by investment banking house Morgan Stanley. Shortly after the sale, the value of Perelman’s stock plummeted amidst allegations of financial improprieties at Sunbeam. Perelman’s holding company filed suit in Florida state courts against Morgan Stanley, charging misrepresentation and fraud. During discovery, Morgan Stanley repeatedly missed electronic document production deadlines as it struggled to locate, secure, analyze, and produce relevant files from thousands of backup tapes squirreled away in various storerooms and warehouses across the country. Its problems were magnified by belated certifications that its production was complete, later withdrawn as erroneous, and a contemporaneous, if unrelated, investigation by the Securities and Exchange Commission for its failure to retain email files, in violation of SEC regulations. In a pair of scathing decisions, Judge Elizabeth Maass sanctioned Morgan Stanley by issuing adverse-inference jury instructions, reversing the burden of proof on the plaintiff’s fraud charges, and revoking the pro hoc vice license of Morgan Stanley’s trial counsel two weeks before trial was to begin. At the close of trial, the jury awarded the plaintiff \$600 million in compensatory and \$850 million in punitive damages.

The volume of potentially responsive data in the Morgan Stanley case was staggering, but the fatal problem was the inaccessibility of the data, which was stored on disaster recovery backup tapes numbering in the thousands in facilities scattered across the country. Not only was much of the data physically inaccessible, but even when it could be located, the nature of the storage media

---

<sup>12</sup> See, e.g., *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, 2005 WL 679071 (Fla. Cir. Ct., 15th Cir. Mar. 1, 2005); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley, Inc.*, 2005 WL 674885 (Fla. Cir. Ct., 15th Cir. Mar. 23, 2005).

<sup>13</sup> *Id.*

prevented analysis to determine whether they contained relevant information, or whether any relevant data could be recovered within the time and budget constraints that Morgan Stanley and its attorneys were operating under. According to the trial judge, instead of informing the court and opposing party of the problem, Morgan Stanley and its attorneys repeatedly misrepresented the situation. It should be stated that the majority of the backup tapes were never analyzed for relevance, and may not have been relevant to subject matter of the litigation. But by failing to overcome the accessibility problem, Morgan Stanley created a situation in which the very existence of the backup tapes themselves became relevant to the fraud allegations. The jurors were instructed that because of Morgan Stanley's actions, they could infer the information on the backup tapes would be adverse to Morgan Stanley's interests.

Morgan Stanley represents an extreme, but not isolated,<sup>14</sup> situation. Far more common are the cases in which a relatively small number of backup tapes are involved and counsel on both sides are fully aware of the problem. But the problem is the same-- for a variety of reasons, electronic data is commonly stored in formats that prevent meaningful content analysis. Considerable expense and burden may be involved in making the data accessible before it can be determined whether it is relevant to the lawsuit. This is fundamentally different from the "undue burden" consideration of existing Fed. R. Civ. P. 26(B)(2), which assumes that the discovery being sought is relevant, and the benefits and burdens of production being weighed are known or can reasonably be estimated. When dealing with electronic information stored on inaccessible media or in inaccessible formats, the benefits and burdens are far more speculative.

This question was squarely presented in *McPeck v. Ashcroft*,<sup>15</sup> an otherwise ordinary employment discrimination suit against the Department of Justice. The plaintiff demanded production of electronic information alleged to be stored on scores of backup tapes. Instead of putting the defendant to the expense of restoring the entire collection before making a relevance determination (or threatening the plaintiff with the cost), the judge ordered a random sampling of a few of the tapes to determine both the cost of restoration and the rough statistical likelihood that relevant information could be found from those sources.

Faced with requesting parties who state with all sincerity, "your honor, we don't know what we don't know," judges have come up with several ways to manage the scope of discovery in the face of the accessibility problem. In *Byers v. Illinois State Police*,<sup>16</sup> another employment discrimination suit against a government agency, the plaintiff requested that the defendant search a collection of backup media going back eight years to locate relevant email messages. However, the plaintiff failed to make a credible threshold showing that relevant email messages were likely to be found, making the cost-benefit analysis of Fed. R. Civ. P. 26(b)(2) meaningless. Without such a threshold showing, the requesting party would have to bear the cost of rendering the backup media accessible.

"Inaccessibility" is not synonymous with either "backup media" or "requesting party loses." Data stored on outmoded computer systems may also be inaccessible, requiring considerable expense and effort to render the data accessible before a determination of relevance can be made. In *Xpedior Creditor Trust v. Credit Suisse First Boston (USA), Inc.*,<sup>17</sup> a putative securities class action case, the plaintiff sought electronic information stored on two decommissioned computer systems. The defendant sought a protective order shifting the cost of data restoration to the plaintiff. This gave the court the opportunity to use cost-shifting analysis to manage the scope of discovery. However, instead of the simple benefit-and-burden test of Fed. R. Civ. P. 26(b)(2), the court adopted the more nuanced seven-factor test of *Zubulake v. UBS Warburg LLC*,<sup>18</sup> The court determined after detailed consideration of all seven Zubulake factors that although the data on the legacy computer systems was "inaccessible" without incurring costs, those costs should remain with the responding party.

14 See, e.g., *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002) (in which backup tapes were all collected and conceded to contain relevant information, but the respondent was found to have engaged in "purposeful sluggishness" in failing to make the information accessible, a factor which the Second Circuit determined to be grounds for potential sanctions).

15 202 F.R.D. 31 (D.D.C. 2001).

16 53 Fed. R. Serv. 3d 740 (N.D. Ill. 2002).

17 58 Fed. R. Serv. 3d 855 (S.D.N.Y. 2003).

18 217 F.R.D. 309 (S.D.N.Y. 2003), discussed *infra* at part II.C.



In *Super Film of America, Inc. v. UCB Films, Inc.*,<sup>19</sup> a contract dispute over the sale of \$115,000 worth of transparent film, the defendant sought discovery of e-mail, documents, databases, and spreadsheets which the plaintiff claimed were beyond its “knowledge or expertise” to retrieve and produce. The plaintiff offered to make computers available to the defendant to retrieve the requested data itself. The defendant objected to the offer as an unreasonable attempt to shift discovery costs to the requesting party. The court rejected the plaintiff’s unsupported and conclusory assertion of burden and ordered the plaintiff to produce the requested data. However, in *Compuware Corp. v. Moody’s Investors Services, Inc.*,<sup>20</sup> the defendant in this unfair trade practices case requested that the plaintiff produce “[a]ll documents, including but not limited to internal memoranda, internal e-mails, and correspondence with [IBM] or any other entity or person, referring or relating to actual or contemplated conduct by IBM.” After initially objecting that the request was overbroad, the plaintiff responded by producing compact disks containing the electronically stored information in its original file format. Now arguing that the production was overbroad, the defendant asked the judge to narrow the scope of its own request and order the plaintiff to index the documents on the CDs and designate those that were relevant to the subject matter of the dispute. The court denied the request, demonstrating that in the world of electronic discovery, a party must be careful what it asks for, as it may get it.

### C. Custodianship issues

In the conventional, paper-based world of business and government, custodianship of records and correspondence was usually clear. Corporate officers, government official, secretaries, file clerks, archivists, and warehouse managers generally understood what they had and what their responsibilities were as custodians of documents. If they did not, the consequences were also generally clear. In the world of electronically stored information, without physical artifacts (“documents”) being created, organized, stored, and moved, custodianship is not nearly as clear. Since the mechanics of document discovery traditionally has been tied closely with the identification of document custodians, the loss of clear lines of custody generates problems with the discovery, preservation, and production of electronically stored information.

With electronically stored information, there are several levels of custodianship. At the primary level are people who work with the data directly—the employees of a company or government agency, for instance, who write and receive electronic communications; create or edit electronic “documents” such as word processing files, graphics, or spreadsheets; or who enter and retrieve data from enterprise databases. These people are familiar with the content of the electronically stored information, but might not know anything about computers, and when asked to physically retrieve information outside the scope of their daily routine, would be entirely lost. Most consumers and home computer users would also fall into this category of custodian.

At the next tier of custodianship are the systems analysts and business process engineers who are generally familiar with the types of data being generated, received, stored, and manipulated, and who are familiar in an abstract sense with the relationships between the different files or stores of information, such as the structure of computer directories or databases. While they are the custodians of the information management system, they usually know little or nothing about the specific content of the information, or where the information is found in a physical sense.

At another tier of custodianship are the IT staff people, who are the physical custodians of the active electronically stored information - the computers, the servers, the backup systems, the near-line media, etc. These custodians are essential to discovery, as they actually run the computer operation. However, they generally know nothing about the informational content of the system, and seldom are familiar with the electronic business processes. Their job is to make sure the computer hardware and software are working efficiently and securely.

---

19 219 F.R.D. 649 (D. Kan. 2004).

20 2004 WL 2931401 (E.D. Mich. Dec.15, 2004).



Another tier of custodianship is becoming more prevalent in electronic discovery, and it is in many ways unique to the discovery of electronically stored information. These are outsource contractors and others who serve a variety of functions associated with a party's information management, but who are not themselves parties. For consumers and home users, these custodians could be the Internet Service Providers (ISPs) such as America Online who provide essential connectivity and computer services, but are also holders of the consumers email, traffic records, and other important data. For businesses, these custodians could be computer service bureaus, Application Service Providers (ASPs) or foreign corporations who provide services ranging from off-site data storage, to computer-based customer service, to complete IT Department functionality.

Few consumers, corporations, or government agencies have any formal lines of communication between these various tiers of custodians to allow for efficient identification, preservation, and production of electronically stored information in discovery. In most organizations, these various tiers operate in complete ignorance of each other. Several cases illustrate the problems that this common situation creates.

Perhaps the most famous case illustrating this situation is *Zubulake v. UBS Warburg*,<sup>21</sup> in which Judge Shira Scheindlin quoted a line from the classic film *Cool Hand Luke*: "What we've got here is a failure to communicate."<sup>22</sup> The failure in *Zubulake* was that the defendant's attorneys attempted to locate important responsive emails by asking the most obvious custodian, the employee who wrote and received them. That employee stated that the emails in question had been "archived," which the attorneys understood as meaning that they had been captured by the formal email archiving function of the electronic business process, maintained by the IT staff, and were therefore safe from destruction. In reality, the employee had meant that she simply moved them into a virtual file folder on her hard drive, where they were later destroyed. That miscommunication between custodians as to what an "archive" meant may have contributed to costing the defendant millions of dollars in the subsequent settlement after judgment for punitive damages.

Illustrating a common problem with third party custodians, in *Keir v. Unumprovident Corp.*,<sup>23</sup> an ERISA class action suit, the parties agreed to a data preservation order after several conferences. The order was very narrowly drawn and concentrated on preserving six days of email records on the defendant's backup media and hard drives. However, the defendant's upper management did not communicate the order to its IT staff for nearly two weeks, and most of its data-management functions had been outsourced to IBM, which failed to implement the required preservation. Although the court found that the defendant's failure to preserve the data was unintentional, it criticized the defendant's poor compliance with the preservation order. The court recommended that further action be taken to determine the feasibility of retrieving the lost data to which the plaintiffs were prejudiced, in order for the court to fashion an appropriate remedy.

Occasionally the problem of third party custodians is insurmountable. In *Procter & Gamble Co. v. Haugen*,<sup>24</sup> an unfair trade practices case with a long history and many reported decisions related to electronic discovery, the 10th Circuit reversed the trial court's dismissal of the plaintiff's Lanham Act claims, based on the plaintiff's failure to produce a database maintained by a non-party contractor. The trial court's order compelling production failed to take into account the logistical difficulties of doing so, which would have involved the purchase of a mainframe computer or paying the non-party an estimated \$30 million to maintain an archived version of the database. The circuit court held that the violation of the order was not willful and the prejudice to the defendant was not clearly established, and vacated the trial court's sanction.

---

21 229 F.R.D. 422 (S.D.N.Y. 2004).

22 *Id.* at 424.

23 2003 WL 21997747 (S.D.N.Y. 2003).

24 427 F.3d 727 (10th Cir. 2005).

#### D. Cost paradigm shift

In the “good old days” of paper-based document discovery, the rules of civil procedure, interpreted in light of the common law rule that each party bears its own costs,<sup>25</sup> operated to even out the cost of discovery. For the producing party, the costs were locating responsive documents, assembling them in either request or business order, and presenting them to the requesting party for inspection and copying. The requesting party bore the cost of analyzing the documents and the significant cost (in the early days of photocopying technology) of copying and transporting them. If anything, this served to tilt the cost paradigm in favor of producing parties. That paradigm began to crumble in the late 1970’s and early 1980’s as the cost of wholesale photocopying decreased significantly. However, the conventional cost paradigm disintegrated entirely with the advent of electronic discovery. Electronically stored information, if kept in electronic form and not reduced to paper printouts, can be very inexpensive to search through and sort using simple, readily available technologies such as word or “string” searching. The cost of copying and transporting electronically stored information is virtually nil. The costs for the producing side, however, have increased dramatically, in part as a function of volume, but more as a function of inaccessibility and the custodianship confusion. Organizations without state-of-the-art electronic information management program in place, which classify information and routinely cull outdated or duplicative data, face enormous (often self-inflicted) costs and burdens. Commentators posited that savvy requesting parties could force settlement of cases simply by threatening electronic discovery.<sup>26</sup>

Early electronic discovery cases that considered the allocation of costs tended to hold to the conventional cost bearing paradigm.<sup>27</sup> However, it soon became apparent that the assumptions underlying the conventional cost paradigm did not apply in the electronic discovery context, and judges began to use their powers under Fed. R. Civ. P. 26(b)(2). In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*,<sup>28</sup> plaintiff minority talent agencies alleging racial discrimination in bookings requested e-mail from the defendants’ backup media. The four defendants objected, citing the high costs estimated by electronic discovery consultants to restore the backup media to accessible form and the legal costs associated with screening the e-mails for relevance and privilege. Balancing eight factors derived from the case law, the court required the plaintiffs to pay for the recovery and production of the defendants’ extensive e-mail backups, except for the cost of screening for relevance and privilege. The eight “*Rowe* factors” articulated by the court were:

1. the specificity of the discovery request;
2. the likelihood of discovering material data;
3. the availability of those data from other sources;
4. the purposes for which the responding party maintains those data;
5. the relative benefits to the parties of obtaining those data;
6. the total costs associated with production;
7. the relative ability and incentive for each party to control its own costs; and
8. the resources available to each party.

While the *Rowe* factors were hailed as the “gold standard” of cost allocation adjudication when they were announced, they were quickly superceded by a modified seven-factor test articulated in the first reported decision in *Zubulake v. UBS Warburg LLC* (“*Zubulake I*”).<sup>29</sup> In this sex discrimination suit against a financial services company, the plaintiff requested email beyond the approximately 100 printed pages produced by the defendants. She presented substantial evidence that more responsive email existed, most likely on backup tapes and optical storage media created and maintained to meet SEC records-retention requirements. The defendants objected to producing e-mail from these sources, which they estimated would cost \$175,000 exclusive of attorney review time. Judge Scheindlin held that the plaintiff’s request was clearly relevant to her claims, but both parties raised the question of who would pay for the discovery and urged the court to apply the *Rowe* factors.

25 *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978).

26 See, e.g., Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561 (2002).

27 See, e.g., *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 WL 360526 (N.D. Ill. June 15, 1995).

28 205 F.R.D. 421 (S.D.N.Y. 2002).

29 217 F.R.D. 309 (S.D.N.Y. 2003).

The judge held that for data kept in an accessible format, the conventional rules of discovery apply--the responding party should pay the costs of producing responsive data. A court should consider cost shifting only when electronically stored information is not reasonably accessible, such as data stored on disaster recovery backup tapes. In conducting the cost-shifting analysis to be applied to discovery of the data deemed "not reasonably accessible," the judge rejected the *Rowe* factors and substituted a seven-factor test. The "Zubulake factors" are, in order of importance or weight:

1. the extent to which the request is tailored to discover relevant data;
2. the availability of those data from other sources;
3. the total cost of production, relative to the amount in controversy;
4. the total cost of production, relative to the resources available to each party;
5. the relative ability and incentive for each party to control its own costs;
6. the importance of the issues at stake in the litigation; and
7. the relative benefits to the parties in obtaining those data.

While the *Zubulake* factors have withstood the test of time, they have not been accepted universally by federal district courts across the country. In *Wiginton v. CB Richard Ellis Inc.* ("Wiginton II"),<sup>30</sup> a class action lawsuit alleging sexual harassment and a hostile work environment, the plaintiffs requested a search through the defendant's email backup tapes for pornographic images and sexually suggestive messages. By agreement, the plaintiffs' computer discovery expert was provided with 94 selected backup tapes and with a set of search terms to use. The expert identified between 142 and 567 arguably responsive documents at a cost of \$249,000. The plaintiffs filed a motion for costs. Considering the cost-shifting factors from both *Rowe* and *Zubulake*, the court opted to modify the *Zubulake* factors to emphasize the proportionality test of Fed. R. Civ. P. 26(b)(2)(iii). The factors the *Wiginton* court considered were

1. the likelihood of discovering critical information;
2. the availability of such information from other sources;
3. the amount in controversy as compared to the total cost of production;
4. the parties' resources as compared to the total cost of production;
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;
7. the importance of the requested discovery in resolving the issues at stake in the litigation; and
8. the relative benefits to the parties of obtaining the information.

The judge found that while most of the factors weighed in favor of cost shifting, the plaintiff had not entirely overcome the presumption that each party bears its own costs. The judge ordered that the plaintiffs should bear 75% of the costs and the defendant only 25%.

Cost-shifting is not the only tool judges have to control electronic discovery costs. Judges have the power to supervise discovery to reduce costs, either directly or through the appointment of special masters. In *Medtronic Sofamor Danek, Inc. v. Michelson*,<sup>31</sup> an intellectual property case involving spinal fusion technology, the defendant sought discovery of information from 996 computer backup tapes and 300 megabytes of data on the desktop computers of the plaintiff's employees. The plaintiff objected that the proposed discovery would be unduly costly and burdensome. The court agreed and applied the *Rowe* factors to determine that the defendant should shoulder most of the costs of the proposed discovery. The court then ordered a detailed protocol for the parties to follow in conducting discovery of the backup tapes and hard drives. Finally, the court granted the defendant's request that a special master be appointed under Fed. R. Civ. P. 53, with the costs to be borne equally by the parties.

<sup>30</sup> 229 F.R.D 568 (N.D. Ill. 2004).

<sup>31</sup> 56 Fed. R. Serv. 3d 1159 (W.D. Tenn. 2003).

## E. Privilege screening

Of all the costs associated with electronic discovery, screening electronically stored information for privilege before production is emerging as the greatest. While other costs can be mitigated by the use of technology or by shifting costs to the requesting party, no technology has yet to be developed that can make privilege decisions, and there is considerable authority for the proposition that privilege screening costs cannot be shifted to an opposing party.<sup>32</sup>

The tremendous cost of privilege screening is a function of the volume of electronically stored information that may need to be screened, but also the nature of that information, particularly email. Email is informal in nature and tends to be circulated widely, creating many copies and versions of the same message with different senders and recipients. In addition, email messages tend to be strung together in “threads,” making it difficult to parse out the privileged messages from the non-privileged ones.<sup>33</sup> Perhaps the most significant contributor to the cost of privilege screening, however, is fear. In many jurisdictions, the inadvertent production of a document over which a privilege objection should have been raised serves to waive that privilege as applied to that document, or possibly over that category or documents or then subject matter of the document. Even if the jurisdiction in which the litigation is taking place does not recognize this “privilege waiver” doctrine, there is fear that the inadvertent production of a privileged document in one litigation may serve as a waiver in other jurisdictions in which the party has litigation. This uncertainty results in extremely cautious behavior on the part of counsel, which drives costs up.

Judges have come up with creative solutions to reducing the cost of privilege screening. In *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*,<sup>34</sup> a lawsuit for breach of contract, the plaintiff made a motion to compel the defendant to reproduce e-mails from its backup tapes. Applying *Rowe*, the court offered the defendant two options for proceeding with discovery of e-mail from the backup tapes. Under the first option, the requesting party would pay the cost of hiring an expert to recover the defendant’s emails and would perform an initial review to identify those that it considered responsive. The defendant would then review those designated documents to determine whether any were privileged, at which point it could object to their actual production. This method of reducing privilege screening costs is sometimes referred to as a “quick peek” agreement. The second option was more conventional. The defendant would review, at its own cost, all the documents recovered by the expert and produce only the responsive, non-privileged documents to the plaintiff.

## F. Choice in the form of production

For decades, the production of paper documents in discovery assumed only one physical form: paper. That paper was allowed to be organized in either of two ways: in business record order or labeled to correspond to the categories of the document request.<sup>35</sup> Occasionally one would come across documents stored in a non-paper format, such as microfilm, but usually those would be printed out on paper for the purposes of discovery or document production. Even after 1970, when the Federal Rules of Civil Procedure were amended to include discovery of “data compilations” stored in electronic format, the assumption reflected in the accompanying Committee Notes was that data compilations would be produced as computer printouts. In those days, computers were owned and operated only by the largest and most sophisticated banks, insurance companies, academic institutions and government agencies. Production of electronically stored information in electronic form would have been useless. As computers became mass produced and ubiquitous, running standardized operating systems and off-the-shelf application software, the exchange of electronically stored information in a variety of forms became possible. While still common in smaller, routine cases, large scale document production in paper form is now considered expensive and burdensome.

However, as the possibilities developed for production of information in a variety of forms, so did disputes over the form of production. These disputes often become the playing field for

<sup>32</sup> See *Computer Assocs. Int'l, Inc. v. Quest Software, Inc.*, 56 Fed. R. Serv. 3d (West) 401 (N.D. Ill. 2003).

<sup>33</sup> See, e.g., *In re Universal Serv. Fund Billing Practices Litig.*, 232 F.R.D. 669 (D. Kan. 2005).

<sup>34</sup> 52 Fed. R. Serv. 3d 168 (E.D. La. 2002).

<sup>35</sup> FED. R. CIV. P. 34(b).

litigation gamesmanship, as each party maneuvers to minimize their discovery obligations and place obstacles in their opponent's discovery path. The early cases considering the form of production for electronically stored information focused on the issue of whether, after a responding party had produced information in paper form, the requesting party could compel production of the same information in electronic form.

This was the posture of the discovery dispute in *McNally Tunneling Corp. v. City of Evanston*,<sup>36</sup> a lawsuit for breach of contract, in which the plaintiff moved to compel delivery of electronic documents the defendant had already produced in hard copy. The court noted that case law was split on whether a party is entitled to discovery in electronic form as well as paper form, citing *Williams v. Owens-Illinois*,<sup>37</sup> which denied a request for computerized data to supplement paper production, and *Anti-Monopoly, Inc. v. Hasbro, Inc.*,<sup>38</sup> which held that a party is entitled to both hard-copy and computerized data. The motion was denied, as it was not supported by any controlling case law, and the defendant failed to demonstrate that it was entitled to both a hard copy and an electronic version of the responsive material.

Other courts focused on the language of Fed. R. Civ. P. 34(b), which appeared to offer only two choices in the form of production, and conversion of electronically stored information into another form was not one of them. In *In re Honeywell International, Inc.*,<sup>39</sup> a putative securities class action, the plaintiffs served a subpoena on non-party PriceWaterhouseCoopers (PWC), the defendant's auditor. PWC produced 63,500 pages of financial work papers in hard-copy form. The plaintiff moved to compel the production in electronic form, claiming that the data as produced were neither in business record order nor labeled to correspond to the categories of the request, as required by Fed. R. Civ. P. 34 and corresponding provisions of Fed. R. Civ. P. 45. PWC opposed the motion to compel because it had produced the information sought in paper form and recreating it electronically would cost \$30,000. The court acknowledged that PWC had produced paper versions but stated it was "insufficient because they were not produced as kept in the usual course of business." The court required that PWC produce the data in electronic form and said that PWC could avoid the \$30,000 expense by also producing the proprietary software to access the data. The court noted that the plaintiffs were not competitors and a confidentiality order was already in place, so PWC's trade-secret interests in the electronic form would be adequately protected.

Some courts have tackled form-of-production gamesmanship head on. In *In re Bristol-Myers Squibb*,<sup>40</sup> a securities fraud suit, the parties had agreed early in litigation to paper production and a per-page price for photocopying. However, the defendant did not disclose that the documents had been scanned, were being "blown back" to paper form at a cost below that of photocopying, and were available in electronic form for considerably less money. The court held the parties to the agreement to produce paper, but at the lower cost of the "blow backs," and ordered that the electronic versions also be produced, at the nominal cost of duplicating compact disks. The court rejected the defendant's argument that the plaintiff contribute to the cost of scanning the documents, as that action was taken unilaterally by the defendant, who, for its own purposes, didn't inform the plaintiff. Finally, the court lamented that the parties did not take the "meet and confer" obligations of Fed. R. Civ. P. 26(f) seriously in light of electronic discovery.

In the past few years, the focus of form-of-production disputes has shifted from paper v. electronic form, to far more nuanced disputes about the particular form of electronic production. Most electronic document productions, until recently, mimicked paper document productions. The electronic files were "imaged," that is, converted from their native file format into a static image, usually in Tagged Image File Format ("TIFF") or Portable Document Format ("PDF"). These formats are essentially the same as photocopies of the electronic document as it would appear on a screen or in a paper printout. These images have some of the advantages of portability and cost-savings of other electronic documents, and they also have the advantages of being static artifacts—they

---

36 2001 WL 1568879 (N.D. Ill. Dec. 10, 2001).

37 665 F.2d 918 (9th Cir. 1982).

38 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995).

39 230 F.R.D. 293 (S.D.N.Y. 2003).

40 205 F.R.D. 437 (D.N.J. 2002).

can be Bates stamped, categorized and gathered into virtual file folders, and even readily printed out for those who insist on handling paper. But they are also different from the electronic file in its native format, such as a word processing document, database, or spreadsheet. The files in native formats are dynamic, and behave the way they do in the active business environment, which may be significant to understanding their function and content. They also contain non-apparent information, such as metadata (embedded records of the creation and management of the document), editorial comments and changes (which may be kept in the native file format for later revision), and functions (such as the mathematical formulas that determine the relationship of cells in a spreadsheet or records in a database). The form of production is more than a question of convenience or cost—it becomes a question of relevance and “best evidence,” as it applies to electronically stored information.

Some courts have proactively ordered production in electronic form, and particularly in native format, as a discovery cost management device. In *In re Verisign, Inc.*,<sup>41</sup> a class action securities suit, the defendants were ordered by the magistrate judge to produce all documents in electronic form. The order further stated that the production of electronic images would not be sufficient, and that electronic records must include metadata as well as be searchable in electronic form. The defendants objected that the order required them to produce irrelevant material and to convert TIFF images already prepared for production into some other form. In reviewing the magistrate judge’s order, the district judge interpreted it as essentially an order to produce in native format, but found that the order was within the magistrate judge’s discretion, being neither clearly erroneous nor contrary to law.

### G. Preservation and the routine destruction of digital information

Perhaps the most vexing issues in electronic discovery, and the issues that grab the most headlines, are the issue of data preservation and its flip side, spoliation. It can be said, with a fair amount of truth, that it is nearly impossible to destroy electronically stored information, particularly in a networked environment. The data can be recovered using expensive forensic methodologies or located elsewhere using expensive and expansive supplemental discovery. Intentional efforts by litigants to “destroy” electronically stored information are usually detected and pose few analytical problems—intentional spoliation of evidence is not a new phenomenon, and intentional spoliation in the electronic discovery context simply introduces new methods.<sup>42</sup>

However, electronically stored information can easily be rendered inaccessible through negligence, unfamiliarity of custodians with computer technology, or routine operations of computers and networks. The simple act of opening a file on a computer changes the information in the “date last accessed” field of that file’s metadata, creates or overwrites various system files, and may change substantive information in the file itself. Computers are configured to run routine maintenance and “clean up” functions that will change or overwrite electronically stored information. Networks are configured to eliminate files that have not been accessed for a reasonable period of time, or automatically delete the oldest emails in a user’s email box. Disaster recovery backup tapes regularly create electronically stored information by copying it from the computer hard drives, and regularly are recycled, thus destroying that information. Halting these routine operations in response to a “legal hold” may be difficult, impossible, unduly costly or unduly burdensome.

Nevertheless, the duty to preserve potential evidence is essential to the courts’ truth-seeking function, and the routine operations of computer systems cannot be allowed to obstruct justice. Somewhere a balance must be struck between the ideal of data preservation and the realities of technology. The courts must consider that balance at two very different points in discovery—at the very outset, when the duty and scope of preservation needs to be defined, and later, in the context of an accusation of spoliation and a motion for sanctions under Fed. R. Civ. P. 37 or the court’s inherent authority.

41 2004 WL 2445243 (N.D. Cal. Mar. 10, 2004).

42 See, e.g., *Kucala Enters., Ltd. v. Auto Wax Co., Inc.*, 56 Fed. R. Serv. 3d 487 (N.D. Ill. 2003) (in which the plaintiff purchased and used disk-wiping software called “Evidence Eliminator” the night before his computer was to be turned over to the defendant for inspection).



On the front end, the duty of preservation has consistently been held to attach when a person knows of or reasonably anticipates litigation involving identifiable parties and identifiable facts. The scope of that duty encompasses potential evidence related to those identifiable facts, which may shift as the litigation develops.<sup>43</sup> The duty exists independently of any “preservation demand letter” issued by the opposing side, although that may provide notice.<sup>44</sup> It also exists independently of any court order, so that a preservation order is only necessary to clarify the obligations in a particular case or to protect evidence from some real and immediate threat.<sup>45</sup> That said, parties contemplating electronic discovery will often negotiate and agree to a stipulation data preservation plan, in part to make sure the opposing side understands its obligations, and in part to limit the party’s own potential liability.

The failure to have a clear idea of the scope of preservation, and a clear plan to institute a “litigation hold” that encompasses electronically stored information, can have dire consequences. The *Zubulake* series of decisions, culminating in “*Zubulake V*,”<sup>46</sup> chronicle the efforts, and ultimate failure, of one team of lawyers attempting to define and fulfill the duty of preservation in an otherwise routine employment discrimination case. In this opinion, Judge Scheindlin considered the plaintiff’s motion for sanctions against the defendant UBS Warburg for deleting e-mails the plaintiff claimed would support her allegations of sex discrimination. The court found that, contrary to instructions from both outside counsel and in-house lawyers, certain UBS Warburg employees deleted relevant e-mails. The duty to monitor client behavior fell squarely on the shoulders of outside counsel, which failed “both in terms of its duty to locate relevant information and in its duty to preserve and timely produce that information.” The judge held that an adverse-inference jury instruction and an award of costs were appropriate, based on the apparent willful misconduct of certain UBS employees in destroying the e-mails. In addition, UBS Warburg failed to preserve backup tapes on which copies of the destroyed e-mails might have been found. While that failure was mere negligence and was not in itself sanctionable conduct, had the backup tapes been preserved, the sanction for the intentional destruction of the email would likely have been far less severe.

A similar client supervision situation developed in *United States v. Philip Morris USA Inc.*<sup>47</sup> A blanket data-preservation order was entered early in this national tobacco products litigation. However, the defendant continued for at least two years its routine practice of deleting e-mail messages more than sixty days old. After discovering this apparent violation of the order, counsel for the defendant delayed informing the court about it for an additional four months. The United States moved for sanctions against the defendant. The court found that eleven of the company’s highest placed officers and supervisors violated not only the court order, but also the company’s stated policy for electronic records retention. The court fined the defendant \$250,000 per employee, for a total of \$2,750,000, and precluded the defendant from calling any of the eleven employees as witnesses at trial.

Counsel, of course, may find themselves to be cogs in a much larger machine operated by the client, over which they may have little control. The questions arises as to what extent, if any, the clients routine electronic records management policies and procedures may continue during discovery, or be relied upon to justify routine destruction of electronically stored information.

In *Renda Marine, Inc. v. United States*,<sup>48</sup> a contract dispute filed by a marine dredging contractor against the U.S. Army Corps of Engineers, the plaintiff moved to compel production of backup tapes and for permission to access the contracting officer’s computer hard drive. The policy of the corps was that after an email was read, it was either deleted or moved to a personal folder immediately. The court found that this practice continued after the defendant had been put on notice that litigation might be pending, thereby breaching a duty to preserve documents. Thus, the court granted the plaintiff’s motion to compel the defendant to produce the backup tapes at its own expense and to provide access to the contracting officer’s computer hard drive.

43 *Stevenson v. Union Pac. R.R. Co.*, 354 F.3d 739 (8th Cir. 2003).

44 *Wiginton v. Ellis*, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) [hereinafter *Wiginton I*]

45 *Treppel v. Biovail Corp.*, 233 F.R.D. 363 (S.D.N.Y. 2006).

46 229 F.R.D. 422 (S.D.N.Y. 2004).

47 327 F. Supp. 2d 21 (D.D.C. 2004).

48 58 Fed. Cl. 57 (Fed. Cl. 2003).



While the analysis of the duty of preservation at the beginning of litigation and throughout the discovery process focuses on the intent and behavior of the parties and counsel, the analysis of the appropriate sanction for spoliation adds the important element of prejudice to the opposing party. Not all destruction of potentially discoverable evidence leads to the severest of sanctions. In *In re Cheyenne Software, Inc., Securities Litigation*,<sup>49</sup> a securities litigation lawsuit, the court held that routine recycling of computer storage media must be halted during discovery when that is the most reasonable means of preserving available data. But the court refused to give an adverse jury instruction, because the plaintiff had not proved prejudice—instead the court ordered the defendant to pay \$15,000 in fees and fines.

Of course, the severity of a sanction is in the eye of the beholder. In *MasterCard International, Inc. v. Moulton*,<sup>50</sup> a trademark infringement suit against a website featuring a “fairly tasteless parody” of MasterCard’s “Priceless” ad campaign, the defendants failed to take any measures to preserve e-mails until five months after the suit was filed, despite knowledge of the lawsuit and a discovery request. The plaintiff moved for spoliation sanctions. The court found that the defendant did not act in bad faith in deleting the e-mails, but that such actions were “grossly negligent.” As simple negligence is the threshold of culpability, sanctions were therefore appropriate. The court denied the plaintiff’s request to have key issues in the case “deemed conclusively established,” because plaintiff did not make a compelling case as to likely significance of the e-mails. The court concluded that the appropriate sanction was an adverse-inference jury instruction.

### III. OVERVIEW OF THE 2006 AMENDMENTS

#### A. History

In October 1999, a few weeks after a package of amendments to the Federal Rules of Civil Procedure dealing with discovery had been passed by the Judicial Conference of the United States and was destined for implementation the following year, the Advisory Committee on Civil Rules met in Kennebunkport, Maine. Rather than congratulating themselves on a job well done and disbanding the Discovery Subcommittee, they decided to take up an issue raised, but not addressed, in the public comment period of their recently-completed rulemaking effort. This issue was electronic discovery.

In a letter to the Judicial Conference prior to the October meeting reporting on the activities of the Advisory Committee, Committee Chairman Judge Paul V. Niemeyer said

[T]he committee recognizes that electronic storage and retrieval of information are changing the opportunities for discovery and the dangers of excessive discovery. Anecdotes abound. The committee is just beginning to study the need to devise mechanisms that will ensure continued access to useful information without overwhelming the parties by burdens far beyond anything justified by the interests of litigation.<sup>51</sup>

Thus, the Advisory Committee embarked on a five year project to answer three fundamental questions. The first question was, what are the differences between conventional and electronic discovery? The second question was, do these differences create problems that can or need to be addressed through changes in the Rules of Civil Procedure? And finally, if there are problems that rulemaking can or should address, what rules can be crafted to serve that purpose? The answers to these questions were far from obvious at the start, and well into the rulemaking process there were many who questioned the need for any rulemaking in this area at all.<sup>52</sup>

---

49 1997 WL 714891 (E.D.N.Y. Aug. 18, 1997).

50 2004 WL 1393992 (S.D.N.Y. June 22, 2004).

51 Letter from Paul V. Niemeyer to the Chief Justice of the United States and Member of the Judicial Conference of the United States, September 1, 1999, reprinted in the meeting materials of the Advisory Committee on Civil Rules, October 14-15, 1999.

52 See, e.g., F. Paul Bland, Jr., Arthur H. Bryant, and Vicky Ni, *Comment of the Trial Lawyers for Public Justice and the TLPJ Foundation* (Feb. 14, 2005), available at <http://www.uscourts.gov/rules/e-discovery/04-CV-239.pdf> (last visited Mar. 29, 2006); Ertie Ward, *Comment of Prof. Ertie Ward* (Feb. 15, 2005), available at <http://www.uscourts.gov/rules/e-discovery/04-CV-240.pdf> (last visited Mar. 29, 2006). Links to all 253 written comments submitted during the official public comment period are available at <http://www.uscourts.gov/rules/e-discovery.html> (last visited Mar. 29, 2006).

On behalf of the Advisory Committee, its Discovery Subcommittee began to answer the questions by going to the experts. During 2000, it convened two “mini-conferences” on electronic discovery, one at Hastings College of Law in San Francisco on March 27, and the second at the Brooklyn Law School in New York City on October 27. Each of these one-day conferences featured presentations by about a dozen technologists, lawyers, litigation support professionals, and judges given to a small audience of Advisory Committee members and invited guests. These conferences were dynamic, informal, and unfortunately not recorded for posterity.<sup>53</sup> They provided the committee members with explanations of the technologies involved, a glimpse into the day-to-day realities of electronic discovery, and views “from the trenches” on many aspects of electronic discovery, both beneficial and problematic.

The following year the Federal Judicial Center conducted a study of electronic discovery disputes coming before federal magistrate judges. Using questionnaires, reviews of case dockets, and interviews with several magistrate judges and the attorneys who appeared before them in electronic discovery disputes, the FJC researchers found that while electronic discovery disputes were not frequent, they were widespread both geographically and across the federal docket, although they usually involved individual plaintiffs and corporate or government defendants, most commonly in employment-related cases, and were resolved by judges applying novel case management techniques within the existing rules framework.<sup>54</sup>

In September 2002 and again in September 2003, the Discovery Subcommittee’s Special Reporter, Prof. Richard L. Marcus of Hastings College of Law, distributed open letters to approximately 200 people nationwide who had expressed interest in and knowledge of the discovery rulemaking process by their appearance at past rulemaking activities or their past contribution of comments on proposed rules. These two communications, dubbed the “Dear Fans” letters, sought their informal input on a series of questions or “trial” rules before the Advisory Committee would begin drafting formal proposals. More than 60 replies were received.<sup>55</sup>

On February 20-21, 2004, the Advisory Committee sponsored a large and more formal conference at Fordham Law School in New York City. This conference was recorded, and complete transcripts are available.<sup>56</sup> A 53-page report outlining proposed rules amendments was presented and discussed by the Advisory Committee at its next meeting,<sup>57</sup> which became the basis of a formal submission of proposed rules amendments to the Standing Committee on Rules of Practice and Procedure.<sup>58</sup> After some modification, these proposals were approved by the Standing Committee for public comment.<sup>59</sup>

Comments from the public were slow to come in at first, but picked up considerably before the February 15, 2005 cutoff date.<sup>60</sup> In addition to taking written comments, the Advisory Committee held hearings on the proposed amendments in San Francisco, Dallas, and Washington DC.<sup>61</sup> The public comment process resulted in some significant revisions to the proposed

53 Summaries of the proceedings of the two “mini-conferences” were prepared for the Advisory Committee by its Special Reporter, Prof. Richard L. Marcus, and published in the meeting materials of the Advisory Committee on Civil Rules dated April 10-11, 2000 and April 23-24, 2001.

54 Molly Treadway Johnson, Kenneth J. Withers, and Meghan A. Dunn, *A Qualitative Study of Issues Raised By the Discovery of Computer-Based Information in Civil Litigation* (Federal Judicial Center, Sept. 13, 2002), available at [http://www.fjc.gov/public/pdf.nsf/lookup/elecdi10.pdf/\\$file/elecdi10.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/elecdi10.pdf/$file/elecdi10.pdf) (last visited Mar. 29, 2006).

55 The letters and replies have been collected and posted by this author at <http://www.kenwithers.com/rulemaking/civilrules> (last visited Mar. 29, 2006).

56 Judicial Conference Advisory Committee On The Federal Rules Of Civil Procedure, *Conference On Electronic Discovery, Morning Session* (Feb. 20, 2004), available at <http://www.kenwithers.com/rulemaking/civilrules/fordham022004am.pdf> (last visited Mar. 29, 2006); *Afternoon Session* (Feb. 20, 2004), available at <http://www.kenwithers.com/rulemaking/civilrules/fordham022004pm.pdf> (last visited Mar. 29, 2006); *Morning Session* (Feb. 21, 2004), available at <http://www.kenwithers.com/rulemaking/civilrules/fordham022104am.pdf> (last visited Mar. 29, 2006).

57 Myles V. Lynk and Richard L. Marcus, *E-Discovery Proposals for Discussion at the April 2004 Meeting*, (Apr. 5, 2004), available at <http://www.kenwithers.com/rulemaking/civilrules/marcus040604.pdf> (last visited Mar. 29, 2006).

58 Hon. Lee H. Rosenthal, *Report of the Civil Rules Advisory Committee* (May 17, 2004), available at <http://www.kenwithers.com/rulemaking/civilrules/report051704.pdf> (last visited Mar. 29, 2006).

59 Hon. Lee H. Rosenthal, *Report of the Civil Rules Advisory Committee* (May 17, 2004, rev. Aug. 3, 2004), available at <http://www.uscourts.gov/rules/comment2005/CVAug04.pdf> (last visited Mar. 29, 2006).

60 Links to all 253 written comments submitted during the official public comment period are available at <http://www.uscourts.gov/rules/e-discovery.html> (last visited Mar. 29, 2006).

61 *Public Hearing on Proposed Amendments to the Federal Rules of Civil Procedure*, San Francisco (Jan. 12, 2005), available at <http://www.uscourts.gov/rules/e-discovery/0112frcp.pdf> (last visited Mar. 29, 2006); Dallas (Jan. 28, 2005), available at <http://www.uscourts.gov/rules/e-discovery/DallasHearing12805.pdf> (last visited Mar. 29, 2006); Washington D.C. (Feb. 11, 2005), available at <http://www.uscourts.gov/rules/e-discovery/CVHearingFeb2005.pdf> (last visited Mar. 29, 2006).

amendments, which were presented to the Standing Committee in June 2005 and approved by the Judicial Conference on September 20, 2005.<sup>62</sup>

The following overview presents the amendments in a practical, conceptual framework, starting with the definition of discoverable electronically stored information in Rule 34, and going through the amendments in the order they would likely surface in electronic discovery procedure.<sup>63</sup>

## B. Redefining “Document Discovery” in Rule 34

Since 1937, discovery has been thought of as the process of gathering information from three primary sources: depositions, answers to interrogatories, and the inspection of “documents and things.”<sup>64</sup> Rule 34 addresses discovery of documents, which are defined to include “writings, drawings, graphs, charts, photographs, and other data compilations...”<sup>65</sup> These are all tangible things. The inadvertently visionary amendment of 1970, which added the phrase “data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably useable form” did little to change that mindset. The emphasis was still on the production of the data compilation as a tangible thing, and only secondarily on the information which could be obtained from it.

In this round of rulemaking, quite a bit of effort was put into updating the quaint language of 1970 to include digital information as we understood it at the turn of the millennium. But the focus of much of the discussion was still on the production of tangible objects. Meetings were devoted to the question of whether we should expand Rule 34’s “laundry list” of objects subject to production to include tapes, floppy disks, and hard drives. While members of the Advisory Committee were discussing this question, I-Pods and thumb drives came on the market and floppy disks virtually disappeared. It became apparent that by the time the committee finished any such list, it would have to amend it to keep up with ever-changing digital technology.

Broader thinking that would transcend current technology was needed, but there was resistance based on a perceived need to limit electronic discovery by concentrating on forms that could easily be rendered as tangible objects, as close as possible to paper documents. One Advisory Committee member, a sophisticated business litigator, expressed shock at the news that practitioners were asking for, and receiving, the metadata associated with discoverable electronic “documents.” She took the position that only “documents,” meaning the part of the files visible in printouts or screen images, were discoverable. This was symptomatic of the widespread confusion between the “scope” of document discovery set out in Rule 34(a), which is supposed to track the scope of discovery in general expressed in Rule 26(b), and the “procedure” for document production set out in Rule 34(b). It took a while for the Advisory Committee to come to the elegant conclusion that Rule 34(a) was about discovering information which happened to be recorded on tangible media, not tangible media that happened to contain information.

While it was clear that digital information could no longer be treated in Rule 34 as a subset of documents, there was little support for completely rewriting Rule 34(a) to eliminate all references to tangible media, although the suggestion was made. Instead, the language was updated slightly<sup>66</sup> and the “data compilations” language which has served so well since 1970 was preserved. But the phrase “electronically stored information” was added on an equal footing with “documents,” both in the title of the new rule and in the text. Here is the amended Rule 34(a):

62 *Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure*, at 86-194 (Sept. 2005), available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> (last visited Mar. 29, 2006).

63 The reader will note that the remaining portion of this section is written in the first person and is not supported by the exhaustive footnotes that might be found in a more objective historical account, because it is a memoir of the discussion that took place. It may reflect the author’s personal recollection and interpretation of events, and may vary with the recollection and interpretation of the other participants. The author has not consulted the other participants while composing the following overview, and therefore assumes sole responsibility for any inaccuracies or misinterpretations.

64 FED. R. CIV. P. 30, 33, 34.

65 FED. R. CIV. P. 34.

66 *E.g.*, the term “phonorecords” does not appear in the amended Rule 34(a), having been replaced by “sound recordings.”

**Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes**

(a) **Scope.** Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information - including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained - translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).<sup>67</sup>

**C. Early Attention to Electronic Discovery Issues**

Almost every survey, research project, or round of commentary conducted on electronic discovery between 1999 and 2004 produced the same fundamental finding-- many of the problems associated with electronic discovery can be worked out between opposing parties who meet and confer early in the litigation, before discovery formally begins, and who continue to communicate with each other and the court throughout discovery. The traditional discovery avoidance tactic of "hiding the ball," when applied to electronic discovery, results in increased cost and delay, and needless disputes. Early attempts at local electronic discovery rulemaking in the federal district courts centered on this concept. Building on the initial disclosure requirement of Fed. R. Civ. P. 26(a)(1) and the pre-discovery conference requirement of Fed. R. Civ. P. 26(f), provisions which went into effect in 2000 as a result of the previous round of discovery rulemaking, federal courts in Arkansas and Wyoming adopted local rules requiring disclosure of electronic records and discussion of electronic discovery plans before formal discovery can begin.<sup>68</sup> The District of New Jersey took the concept a few steps further, requiring not only disclosure and conference, but also that counsel on both sides know what they are talking about, by requiring that counsel investigate the client's information system and identify a person with knowledge of the information system to assist with computer-based discovery.<sup>69</sup> The federal district courts in Delaware and Kansas took a slightly different path. Instead of adopting local rules, these district courts formulated standards or guidelines for attorneys to follow when conducting electronic discovery. These have the effect of standing orders and are far more detailed than the local rules of Arkansas, Wyoming and New Jersey.<sup>70</sup>

The emergence of these local rules, standards, and guidelines affected the deliberations of the Civil Rules Advisory Committee in two ways. First, these local experiments or models provided objective experience on which the Advisory Committee could draw. Second, they served as a clear indication that federal rulemaking was necessary, if for no other reason than to prevent any further divergence from the ideal of a national, uniform set of civil procedure rules in effect in all federal courts.

The change proposed to Rule 26 to require early disclosure of electronically stored information is really quite minor--simply the insertion of the phrase "electronically stored information" in Rule 26(a)(1)(B):

<sup>67</sup> The quoted language is based on the Report of the Civil Rules Advisory Committee dated May 27, 2005 and revised July 25, 2005 (published in the *Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure* (Sept. 2005) p. 86-194, available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> (last visited Mar. 29, 2006)). This is the source for all citations to the rule amendments in this article. The reader is cautioned, however, that the exact text of the rule amendments is still subject to technical, typographical, or grammatical changes before submission to Congress by the Supreme Court. Until then, for the most up-to-date and authoritative version of the rule amendments, readers should consult the "Pending Rules Amendments" web page of the U.S. Courts at <http://www.uscourts.gov/rules/newrules6.html>.

<sup>68</sup> Eastern and Western Districts of Arkansas, Local Rule 26.1, available at <http://www.ark.uscourts.gov/rules/r26-1.html> (last visited Mar. 31, 2006); District of Wyoming, Local Rule 26.1(e), at <http://www.ck10.uscourts.gov/Wyoming/district/pdfforms/localrules-cv.pdf> (last visited Mar. 31, 2006).

<sup>69</sup> District of New Jersey, L. Civ. R. 26.1(d), available at <http://pacet.njd.uscourts.gov/rules/05-0901-Rules.pdf> (last visited Mar. 31, 2006).

<sup>70</sup> District of Delaware, *Default Standard for Discovery of Electronic Documents*, available at <http://www.ded.uscourts.gov/Announce/Policies/Policy01.htm> (last visited Mar. 31, 2006); District of Kansas, *Electronic Discovery Guidelines*, available at <http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf> (last visited Mar. 31, 2006).

**Rule 26. General Provisions Governing Discovery; Duty of Disclosure**

[...]

**(a) Required Disclosures; Methods to Discover Additional Matter.**

(1) Initial disclosures. Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

[...]

The changes proposed to Rule 26 to incorporate electronically stored information into the initial discovery conference of the parties is more complicated. Here, the Advisory Committee intended to have the parties tackle, head-on, three of the difficulties most likely to arrive in electronic discovery—the preservation of potentially discoverable information, the form of production, and the assertion of privilege:

**Rule 26. General Provisions Governing Discovery; Duty of Disclosure**

[...]

**(f) Conference of Parties; Planning for Discovery.** Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

(1) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;

(2) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;

(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(4) any issues relating to claims of privilege or of protection as trial-preparation material, including - if the parties agree on a procedure to assert such claims after production - whether to ask the court to include their agreement in an order;

(5) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and

(6) any other orders that should be entered by the court under Rule 26(c) or under Rule 16(b) and (c).

[...]

Form 35 is a seldom-used appendix to the Rules. It is intended to serve as a model for a joint report of the parties to the court on the outcome of the Rule 26(f) conference, and the basis for the Rule 16(b) pretrial conference with the judge. It is proposed to be amended in line with Rule 26(f):

**Form 35. Report of Parties' Planning Meeting**

[...]

3. Discovery Plan. The parties jointly propose to the court the following discovery plan: [Use separate paragraphs or subparagraphs as necessary if parties disagree.]

Discovery will be needed on the following subjects: (brief description of subjects on which discovery will be needed)

Disclosure or discovery of electronically stored information should be handled as follows: (brief description of parties' proposals)

The parties have agreed to an order regarding claims of privilege or protection as trial-preparation material asserted after production, as follows: (brief description of provisions of proposed order)

All discovery commenced in time to be completed by (date). [Discovery on (issue for early discovery) to be completed by (date).]

[...]

The agenda for the Rule 16(b) pretrial conference is proposed to be amended to accommodate the new topics for discussion at the Rule 26(f) conference. Here, one problem identified with the discovery of electronically stored information is highlighted for judicial consideration, because it is the one most likely to require judicial action: any agreement between the parties on the assertion of privilege over information produced in discovery. The concern extends beyond electronic discovery into conventional discovery as well, but it appears here for the first time:

**Rule 16. Pretrial Conferences; Scheduling; Management**

[...]

**(b) Scheduling and Planning.** Except in categories of actions exempted by district court rule as inappropriate, the district judge, or a magistrate judge when authorized by district court rule, shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties and any unrepresented parties by a scheduling conference, telephone, mail, or other suitable means, enter a scheduling order that limits the time

(1) to join other parties and to amend the pleadings;

(2) to file motions; and

(3) to complete discovery.

The scheduling order may also include

(4) modifications of the times for disclosures under Rules 26(a) and 26(e)(1) and of the extent of discovery to be permitted;

(5) provisions for disclosure or discovery of electronically stored information;

(6) any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production;

(7) the date or dates for conferences before trial, a final pretrial conference, and trial; and

(8) any other matters appropriate in the circumstances of the case.

The order shall issue as soon as practicable but in any event within 90 days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant. A schedule shall not be modified except upon a showing of good cause and by leave of the district judge or, when authorized by local rule, by a magistrate judge.

[...]

**D. The "Two Tier" Approach to the Accessibility of Electronically Stored Information**

While the "meet and confer" requirements of the proposed amendments are non-controversial, the so-called "two tier" approach to defining the scope of electronic discovery has been highly controversial. The "two tiers" refer to two levels of accessibility of information, and apply only to electronically stored information. The first tier is electronically stored information that is "accessible," meaning that it can be obtained and reviewed for relevance without extraordinary cost or technical



difficulty. Active online data that is routinely accessed in the ordinary course of business is the most obvious example, but it can also include off-line data stored on disks or tapes, or archival data that is indexed and maintained on media and in formats that allow for access when needed.

While we may informally refer to “accessible data,” the emphasis is really on the data source—the media and formats in which the data is kept. This subtle distinction becomes more important when we consider the second tier of discovery of electronically stored information—data from sources that are “not reasonably accessible.” We concentrate on the characteristics of the data source, as opposed to the data, because the difficulties presented by a data source that is “not reasonably accessible” prevent us from knowing anything about the data itself. Most importantly, the medium or the format prevents us from knowing whether the data itself is relevant to the litigation. Costs must be incurred and burdens borne before that threshold determination of relevance can reasonably be made.

The distinction between data sources that are “accessible,” as opposed to those that are “not reasonably accessible,” was first clearly articulated in *Zubulake v. UBS Warburg LLC* (“*Zubulake I*”)<sup>71</sup> and applied to the question of when cost shifting is an appropriate consideration in electronic discovery. The court held that the presumption that the each party bears its own costs in discovery applied with full force in electronic discovery when the information being sought comes from reasonably accessible sources. Only when the information being sought comes from sources that are not reasonably accessible may cost shifting be considered, and then only with the application of a seven-factor test.

As applied in proposed Rule 26(b)(2), the accessibility of any data source is not primarily a cost-shifting factor. Accessibility is applied to determine the presumptive scope of discovery of electronically stored information. The fundamental principle is that if electronically stored information resides on a source that is not reasonably accessible, such that the relevance of the information to either the claims and defenses or the general subject matter of the litigation cannot be determined without incurring “undue” costs and burdens<sup>72</sup> then that electronically stored information is presumptively outside the scope of discovery.

That presumption may be challenged, for instance by the presentation of circumstantial evidence indicating that the data source contains relevant data (such as deposition testimony reasonably identifying a mysterious backup tape), or that the cost of searching sources that are not reasonably accessible for important missing data is justified, or that the source is more reasonably accessible than represented. In the first two examples, the cost shifting analysis from *Zubulake I* may come back into the picture if discovery is ordered.

Critics point to this provision of the amended Rules and state that this represents a restriction in the scope of discovery itself, fundamentally different from the consideration of a protective order over otherwise discoverable information.<sup>73</sup> Supporters of the amended Rules essentially agree.<sup>74</sup> Practitioners testified before the Advisory Committee that the “two tier” approach was already the *de facto* standard in electronic discovery. Responding parties routinely only produced electronically stored information in discovery from accessible sources, and only investigated sources that were not reasonably accessible when necessary. The silver lining for the critics of this rule is that responding parties will be required to identify the sources of electronically stored information that they are not considering to be within the scope of discovery because they are not reasonably accessible. Under the informal practice, requesting parties were left to guess or had to engage in costly ancillary discovery to get a complete picture of the electronic discovery landscape.

---

71 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

72 Here the proposed Rule has an explicit reference to current Rule 26(b)(2), which will be renamed Rule 26(c), and the “proportionality” test applied to consideration of a protective order, thus grafting a well-developed body of law onto an entirely new concept.

73 See e.g., F. Paul Bland, Arthur H. Bryant, and Vicky Ni, *Comments of the Trial Lawyers for Public Justice and TLPJ Foundation* (Feb. 15, 2004), at 21, available at <http://www.uscourts.gov/rules/e-discovery/04-CV-239.pdf> (last visited Mar. 31, 2006).

74 See, e.g., Prof. Arthur Miller’s letter to the Advisory Committee dated February 10, 2004, at <http://www.uscourts.gov/rules/e-discovery/04-CV-219.pdf> (last visited Mar. 31, 2006).



In one respect, the Advisory Committee had to act to prevent a potential unintended consequence of the “two tier” approach. Several commentators, including myself,<sup>75</sup> noted when the “two tier” approach was first offered, placing sources that are “not reasonably accessible” outside the presumptive scope of discovery raised the question as to whether those sources were now also outside the scope of the duty of preservation, particularly in light of early drafts of Rule 37(f) regarding spoliation. The Advisory Committee did not want create a federal rule on preservation, expressly or implicitly, and included a strong comment in the Committee Note following Rule 26(b)(2): “A party’s identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence.”

Here is the language of the amended Rule 26(b)(2):

**Rule 26. General Provisions Governing Discovery; Duty of Disclosure**

[...]

**(b) Discovery Scope and Limits.** Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

[...]

**(2) Limitations.**

(A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

(B) 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.

(C) The frequency or extent of the use of discovery methods otherwise permitted under these rules...

[...]

**E. Privilege Screening and Inadvertent Production of Privileged Information**

If the Civil Rules Advisory Committee wanted to avoid creating a federal rule of preservation, expressly or implicitly, in Rule 26(b)(2), the Committee wanted even more to avoid creating a federal rule of privilege waiver, expressly or implicitly, in Rule 26(b)(5). Not only could that invade the territory of the Evidence Rules Advisory Committee, but it could also be viewed as establishing or modifying substantive law under the guise of a adopting procedural rule.

However, something had to be done to reign in the cost of screening electronically stored information (and conventional documentation for that matter) for privilege before production. As the volume and complexity of data sets increases, so does the danger that attorney reviewers will inadvertently produce a document over which there was a legitimate claim of privilege. Depending on the law of the particular jurisdiction, that inadvertent production could be viewed as a waiver of the privilege for that document, they type of document, or all such documents related to that subject of the litigation. Even if no waiver is found under the law of one jurisdiction, a litigant in parallel litigation in another jurisdiction may raise the claim of waiver and attempt to discover the document - or all documents of that type, or all documents related to that subject of the litigation. The stakes, therefore, can be very high. To avoid inadvertent waiver of privilege, hours and hours of attorney time is spent reviewing data collections, item by item, often two or three times. Electronic discovery holds out the promise - or illusion - that technological tools can be applied to reduce the cost of this task.

<sup>75</sup> Kenneth J. Withers, *Two Tiers and a Safe Harbor: Federal Rulemakers Grapple with Electronic Discovery*, 51 FED. LAW. 29, 31 (Fall 2004).

Key word searches, filters, and even Artificial Intelligence could be employed to take the attorney out of all but the final or most critical stages of the review process. But since these tools are still in the development and testing stages, they are considered too risky to be put into a game on which so much is riding.

To reduce the risks and therefore the costs of privilege screening, practitioners have entered into agreements with opposing counsel to better manage the production process and contain the potential damage caused by error. One such agreement is called a “claw back,” under which counsel on both sides agree to surrender any documents they receive from the other if a privilege claim is asserted in a timely manner after production, and if there is a disagreement, to place the document on a privilege log for review by the judge at an appropriate time. While a claw back agreement may reduce tension in litigation, it might not actually reduce costs. If the issue of privilege waiver comes before the judge, one of the considerations will likely be the degree of care taken by the producing party to avoid such an error. Therefore producing parties will still exercise a high degree of care in the screening process, at a high cost. Perhaps more frightening is the prospect that while the “claw back” agreement may be useful and constructive between the parties, it does not bind non-parties, who may claim in parallel litigation in another court, perhaps operating under a stricter standard, that any privilege claimed over the documents “clawed back” had been waived by the fact of production.

A second type of agreement is the “quick peek.” Under this agreement, the parties can dramatically reduce the scope and cost of privilege review, and the scope and cost of discovery itself. The parties agree to an “open file” review of each other’s data collections prior to formal discovery, reserving all rights to assert privilege when responding to the actual document request. After the review, the parties designate the files or data sources that they believe are most relevant to their case, and submit a formal Rule 34 request listing those items. The producing party then has a much narrower task of privilege review, focusing on just those files or data sources before responding to the request.

The “open peek” agreement, while very tempting, demands the highest degree of trust between opposing counsel, and is open to attack from the parallel litigant in another jurisdiction, who may claim that the very existence of such an agreement is evidence that the parties willingly and knowingly waived privilege by opening their files to opposing counsel.

Knowing full well the dangers of these agreements, but desiring to encourage them whenever possible, the Advisory Committee worked on two levels. The primary level was to make strong suggestions in Rule 26(f) and 16(b) that the parties and the judge should consider this option. The second level was to adopt the essentials of a “claw back” agreement as the default procedure in the event there was no formal agreement, thereby bolstering the argument that a procedure imposed by rule cannot be a willing waiver. But the Advisory Committee took great pains to word the rule, and the accompanying Committee Note, to disclaim any intention or ability to determine by rule the outcome of a privilege claim dispute arising from the inadvertent production.

**Rule 26. General Provisions Governing Discovery; Duty of Disclosure**

[...]

**(b) Discovery Scope and Limits.** Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

[...]

**(5) Claims of Privilege or Protection of Trial Preparation Materials.**

**(A) Information withheld.** When a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.

**(B) Information produced.** If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.  
[...]

## F. The Form or Forms of Production

Form-of-production disputes are becoming more frequent in discovery as more choices in the form of production become available to parties. In the context of electronic discovery the form of production becomes much more than a question of cost, convenience, or logistics. The forms in which electronically stored information can be produced become strategic decisions for both requesting and responding parties, as each form conveys different information and allows different levels of analysis, as well as logistical advantages and disadvantages. In addition, different types of electronically stored information logically require different forms of production. Databases and spreadsheets, for instance, are not conducive to being reduced to static images, as opposed to drawings or basic text.

The Advisory Committee tackled this issue, like the privilege waiver issue, on two levels. In the first instance, the revision to Rule 26(f) encourages the parties to discuss the form or forms of production of electronically stored information before any formal document request is issued. But should the parties not reach agreement, Rule 34(b) is amended to provide a default procedure for the production of electronically stored information. Under Rule 34(b), the requesting party is encouraged to state a preferred form of production as part of the request. The responding party has the right to object to the proposed form for stated reasons. If the parties cannot come to an agreement at this stage, the requesting party has resort to a motion to compel under Rule 37. Presumably, although it is not stated in the Rule, the responding party has recourse to a protective order under existing Rule 26(b)(2), which will be renumbered Rule 26(c).

Absent any stated preferences in the request, agreement of the parties, or order of the court, the default forms of production for electronically stored information are meant to be parallel to the default forms of production for conventional document discovery- “a form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable.” The first default option has been interpreted by many commentators, especially technologists, as being Rulespeak for “native file format.” This is not necessarily the case, particularly with archival data, but it has already spawned a cottage industry of consultants and technologists who are becoming expert in handling this volatile and problematic form of production. The second default option is, of course, open to interpretation, particularly whether the phrase “reasonably useable” refers to the logics of handling documents and data during discovery, or whether it refers to the usability of the information available in the chosen form.

Here is the language of the amended Rule 34(b):

### **Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes**

[...]

**(b) Procedure.** The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced.

Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).

The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. If objection is made to the requested form or forms for producing electronically stored information -- or if no form was specified in the request -- the responding party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless the parties otherwise agree, or the court otherwise orders,

(i) a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request; and

(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable; and

(iii) a party need not produce the same electronically stored information in more than one form.

[...]

### **G. Answering Rule 33(d) Interrogatories with Electronically Stored Business Records**

Rule 33(d) is a time-honored method of cost shifting in discovery, when the costs for either party will be roughly the same, by allowing (or insisting) that the requesting party analyze records to answer interrogatories. The amendment to Rule 33(d) merely recognizes the current reality that Rule 33(d) can apply to electronically stored information as well as conventional paper business records. Disputes can arise, however, over the elements that need to go into the determination that the cost of record analysis is roughly the same for either party. Does that include the overhead costs of maintaining the necessary computer hardware and software? Does that include the cost of training personnel? When those costs are figured in, plus the potential business disruption, security compromise, and privilege issues involved in having a party opponent occupying the client's IT department, cautious counsel will likely skip over this option and simply have the client produce the data.

#### **Rule 33. Interrogatories to Parties**

[...]

**(d) Option to Produce Business Records.** Where the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information, of the party upon whom the interrogatory has been served or from an examination, audit or inspection of such business records, including a compilation, abstract or summary thereof, and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries. A specification shall be in sufficient detail to permit the

interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.  
[...]

## H. Discovery of Electronically Stored Information from Non-Parties

Non-parties to litigation have an increasingly important role in discovery. For individuals and small businesses, non-parties may hold their own electronically stored information or that of their opponent. Few individuals or small business own and operate their own computer networks, and most depend instead on Internet Service Providers, Application Service Providers, employers, and schools to provide the resources for their personal data management. As a consequence, these non-parties are being asked increasingly to respond to subpoenas for electronically stored data or information about a party's computer use. Although not parties, they face the same questions of preservation, cost, privilege, and form-of-production as parties. Receipt of a subpoena should be an invitation to a dialog with the requesting party about the scope of the request, protective measures, and costs. Courts are generally solicitous towards non-parties, as they are instructed by rule to relieve non-parties from "substantial" costs related to the production of records, a much lower threshold than the "undue burden" standard of current Rule 26(b)(2), which will be renumbered Rule 26(c). The case law in the electronic discovery sphere already recognizes the different approach taken by Rule 45 in protecting responding parties.<sup>76</sup>

Rule 45 is amended extensively to bring it in line with the amendments to Rules 26 through 34.

### Rule 45. Subpoena

#### (a) Form; Issuance.

(1) Every subpoena shall

[...]

(C) command each person to whom it is directed to attend and give testimony or to produce and permit inspection, copying, testing, or sampling of designated books, documents, electronically stored information, or tangible things in the possession, custody or control of that person, or to permit inspection of premises, at a time and place therein specified; and

[...]

A command to produce evidence or to permit inspection, copying, testing, or sampling may be joined with a command to appear at trial or hearing or at deposition, or may be issued separately. A subpoena may specify the form or forms in which electronically stored information is to be produced.

[...]

#### (c) Protection of Persons Subject to Subpoenas.

[...]

(2) (A) A person commanded to produce and permit inspection, copying, testing, or sampling of designated electronically stored information, books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection, copying, testing, or sampling may, within 14 days after service of the subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to producing any or all of the designated materials or inspection of the premises-or to producing electronically stored information in the form or forms requested. [...]

[...]

<sup>76</sup> See, e.g., *U.S. v Amerigroup*, 2005 WL 3111972 (N.D. Ill. Oct. 21, 2005).

**(d) Duties in Responding to Subpoena.**

[...]

(1) (A) [...]

(B) If a subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable

(C) The person responding to a subpoena need not produce the same electronically stored information in more than one form.

(D) A person responding to a subpoena need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought 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 such discovery.

(2) (A) [...]

(B) If information is produced in response to a subpoena that is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The person who produced the information must preserve the information until the claim is resolved.

[...]

**I. Restrictions on Judicial Power to Sanction Parties for Failing to Produce Electronically Stored Information**

The final rule we discuss in this article rivals the “two tier” provisions of Rule 26 in controversy. Rule 37(f), which is entirely new, purports to place restrictions on a judge’s discretion in issuing sanctions for the failure to produce electronically stored information. The Advisory Committee took a long and winding road to reach the final language of Rule 37(f), which came as a surprise to many who were following the public comments on the rules package from August 2004 through February 2005. The rule quoted below bears little resemblance to the proposed rule published in 2004 that was the subject of so much comment and analysis. Perhaps more importantly, it bears little resemblance to the model rule advocated by corporate defense attorneys early in the Advisory Committee’s five-year study of electronic discovery. It can be said that Rule 37(f) really isn’t a rule at all, but more a framework for analysis, restating the law of sanctions in the spoliation context.

The proposal for a rule restricting the use of sanctioning power for the loss of electronically stored data subject to discovery was initially dubbed the “safe harbor” proposal, and centered on culpability. Absent a finding of gross negligence or intentional misconduct, the various proposals ventured, no sanction for the loss of data should be levied. This proposal was grounded in the fear of many in corporate America (and in the government sector) that electronic information systems were far too large and complex to manage with the degree of certainty needed to fulfill the duty of preservation, and that no party should face sanctions arising out of circumstances beyond their control.

The fundamental problem with the various early proposals is that they appeared to be a solution in search of a problem. Sanctions analysis had always incorporated the concept that “the

punishment must fit the crime,” and in the area of sanctions for the loss of electronically stored information, there was no evidence that “case killer” sanctions (an adverse inference jury instruction, striking of a pleading or defense, dismissal or default) had ever been levied by a federal judge without a finding, express or implied, on culpability amounting to gross negligence or intentional misconduct.<sup>77</sup> The “sanctions” that the early proposals would restrict were those discovery orders that were far less severe and designed to place the parties in the position they would have been but for the loss of the electronically stored information, generally some form of supplemental discovery at the expense of the party who lost the data. In addition, the early proposals ignored what had heretofore been an important element in the judge’s analysis- the degree of prejudice to the requesting party’s case due to the non-producing party’s loss of the data.

After floating several different formulation of a “safe harbor” rule, including taking the somewhat unusual step of publishing two alternative proposed rules simultaneously for public comment, the Advisory Committee finally came up with language that most everyone could agree on. But it fell far short of that the original proponents had wanted, and the Advisory Committee Chair, Judge Lee Rosenthal, emphasized on several occasions that this could no longer be called a “safe harbor.” Jonathan Redgrave, chair of the Steering Committee of The Sedona Conference Working Group on Electronic Retention and Production, the authors of *The Sedona Principles*, likened the rule instead to a lighthouse-a guide to assist the skillful sailor through dangerous waters at night.

Consider the language approved by the Standing Committee and the Judicial Conference:

**Rule 37. Failure to Make Disclosures or Cooperate in Discovery; Sanctions**

[...]

**(f) Electronically stored information.** 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.

[...]

This short rule contains several puzzles to be worked out by judges on a case by case basis.

“Absent exceptional circumstances...” Perhaps this is an attempt to restore the factor of prejudice to the requesting party’s case.

“... a court may not impose sanctions under these rules...” A judge has inherent authority or contempt powers outside these rules, of course.

“... on a party...” This phrase explicitly excludes the non-party served with a subpoena duces tecum for electronically stored information under Rule 45.

“...for failing to provide electronically stored information lost as a result of the routine, good-faith operation...” What is a routine, good-faith operation?

“... of an electronic information system.” What is an electronic information system? Does it include the human beings who run it?

Although not yet in force, Rule 37(f), coupled with the *Zubulake* series of opinions, is already generating a significant amount of activity on the part of lawyers, business people, and government officials to attempt to define and establish electronic information systems governed by routine, good-faith policies and procedures, including the all-important “legal hold” over electronically stored information relevant to current or reasonably anticipated litigation. One need only look at the notices in the legal press to come to the conclusion that the sun never sets on an electronic discovery/electronic records management conference taking place somewhere in the world, which is a good thing. Even if Rule 37(f) ultimately proves to be problematic in application, at least it will have accomplished that.

<sup>77</sup> Hon. Shira A. Scheindlin and Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. TECH. L. REV. 71, 85 (2004).



#### IV. EPILOGUE: THE 2006 AMENDMENTS AS “PERSUASIVE AUTHORITY”

In the nature of an epilogue to this article, or a prologue for what is to come, five cases are presented below, each of which cites one provision or another of the amended rules, many months before they are to come into effect. The amended rules are, of course, binding on no one yet, but are cited in these cases as persuasive authority. This is a tribute to the Civil Rules Advisory Committee and all who worked for five long years studying the issue of electronic discovery.

##### A. Placing Practical Limits on the Duty of Preservation: Reasonable Foreseeability

*Convolve, Inc. v. Compaq Computer Corp.*,<sup>78</sup> the first reported decision to cite a rule from the amendments package, was a patent infringement suit involving disk drive technology. The plaintiff moved for an adverse inference jury instruction, alleging spoliation of e-mail messages and laboratory test results by the defendant. In considering the circumstances surrounding the destruction of the e-mail messages, the court noted that the duty to preserve potentially discoverable e-mail had clearly arisen, since the messages were composed and sent after litigation had commenced. However, the court found that the plaintiff had failed to establish that the e-mail messages in question had been destroyed intentionally, or that the e-mail messages had any significant bearing on the facts of the case. Therefore sanctions were not justified. Regarding the laboratory test results, the court found that the “results” consisted of visual observations of waves displayed on an oscilloscope as disk drives were subjected to variable electrical currents. Since these “results” were ephemeral, “the preservation of the wave form in a tangible state would have required heroic efforts far beyond those consistent with [the defendant’s] regular course of business.” Citing the recently published proposed amendment to Fed. R. Civ. P. 37, the court held that absent a violation of a preservation order, no sanction was warranted.

##### B. Is Metadata Within the Scope of Rule 34?

*Williams v. Sprint/United Management Co.*<sup>79</sup> is an employment class action suit alleging age discrimination in layoffs. The defendant produced Excel spreadsheets showing reduction-in-force calculations in a static image format, which eliminated the mathematical formulae behind the spreadsheets, text that exceeded cell size, and metadata. Referring to *The Sedona Principles* as well as proposed Rule 34(b), the judge determined that the defendant should have preserved and produced the spreadsheets “as they are kept in the ordinary course of business” -- that is, in native format -- or taken other measures to preserve and produce non-apparent information contained within the electronic files, as it was reasonable to assume that the calculations, text, and metadata would be relevant and material to the claims raised in the lawsuit.

##### C. What Are the Court’s Powers to Order the Form of Production and Allocate Costs?

*In re Priceline.com, Inc. Securities Litigation*.<sup>80</sup> is a securities class action case in which the court set out a detailed order regarding the forms of production for a variety of electronic information sources, stating the defendants “shall produce responsive information...in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.” The court noted, however, that exceptions may apply if native file production would be necessary to view the information contained in the file. The directives required backup tape restoration to be performed on “a measured basis, with cost-shifting determinations made at each step of the process.” The court declared it would apply the analysis outlined in the proposed amendments to Fed.R.Civ.P. 26(b)(2).

78 223 F.R.D. 162 (S.D.N.Y. 2004).

79 230 F.R.D. 640 (D.Kan. 2005).

80 233 F.R.D. 88 (D.Conn. 2005).

#### D. Can the Court Order the Parties to Enter Into a “Claw Back” Agreement?

In *Hopson v. The Mayor and City Council of Baltimore*,<sup>81</sup> a putative class action lawsuit alleging race discrimination in the Baltimore fire department, discovery was bogged down over a number of procedural issues, one of which was the time and cost of reviewing the defendant’s voluminous document collection for privilege prior to production. Citing the proposed amendments to Fed. R. Civ. P. 26(b)(5), the magistrate judge encouraged the parties to enter into a “claw back” agreement. Recognizing that “claw back” agreements raise difficult issues of privilege waiver, the judge stated that the agreement would be framed as a court order, bolstering the argument that no waiver was taking place and offering some privilege protection against parties in parallel or future litigation. However, the court noted, such an order would not relieve the parties of the duty to perform a reasonably thorough privilege review, as time and resources allow, nor would it act as an iron clad protection against a “privilege waiver” claim being raised in another jurisdiction, particularly one that takes a strict view of waiver.

### V. CONCLUSION

These five cases begin to apply the 2006 amendments to the Federal Rules of Civil Procedure and answer a few of the many questions raised elsewhere in this article. But by citing and discussing the rules, the judges in these cases acknowledge that the amended rules, the Advisory Committee Notes, the reports and memoranda, the public comments, the conference proceedings, *The Sedona Principles*, and the rest of the “legislative history” constitute a formidable body of learning in this fascinating and complex area of the law. We have learned much in the past five years, and what is more, we have generated a wealth of original material for future legal scholars. As time goes on and technology changes, we will undoubtedly look back and think how innocent and naïve we were. But I hope that the labors of the Civil Rules Advisory Committee, its many advisors and antagonists, the people who came to the meetings and the people who wrote comments, will be recognized as an extraordinary example of open and democratic rulemaking.

---

81 232 F.R.D. 238 (D. Md. 2005)