

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW



<http://ddee.pf.com>

Reprinted from Vol. 6, No. 12 | December 2006

COURTS & PROCEDURE

Extreme Makeover:

The Effect of the New Federal Rules on E-Discovery

By Paul H. Luehr and Jenna K. Perrin

In reality TV shows, a “makeover” features a person whose initial appearance is always comfortably out-of-date. The experts apply their touches, sometimes small (dabbing on blush) and sometimes bold (whacking off inches of hair), but the overall effect of the makeover is always dramatic, altering the subject’s overall appearance, attitude, and even daily life.

The Federal Rules of Civil Procedure have gone through a similar transformative process. They were trusted, comfortable, and out-of-date until this spring when the Supreme Court approved changes proposed by the Judicial Conference Committee. In production for almost five years, the new proposed amendments focus on electronic discovery. Some changes are bold; others are subtle. Taken together, however, the effect of the new rules is dramatic and may change the daily mechanics of discovery and the overall face of litigation forever.

Background

The Federal Rules are just catching up with modern technology, but digital evidence is actually nothing new. Lawyers, paralegals, and litigation support staff have dealt with e-mail, electronic memos, digital letters, and computer spreadsheets for over a decade. In fact, “electronic discovery” is now so commonplace that attorneys often refer to it as just plain “discovery” and must use a retronym — “paper discovery” — to refer to old-fashioned discovery that involves only hard copy documents.¹

The Judicial Conference Committee on Rules of Practice and Procedure, and its Advisory Committee on Civil Rules (“Advisory Committee”), revised the Federal Rules of Civil Procedure to respond to recurring issues in electronic discovery.² The Supreme Court approved the proposed rule changes on April 12, 2006, and barring any action by Congress, the new Rules take effect on December 1, 2006.³

Although the new Rules merely purport to codify the way courts have handled these issues in previous cases, in fact the new Rules create a new landscape. The attorneys who will

thrive in this new environment are: 1) in-house and outside counsel who appreciate the variety of data implicated in most litigation, 2) attorneys who take steps — even before litigation has ensued — to understand what data is stored where, and for what periods of time within an organization, 3) attorneys who quickly seek technical information about the forms and locations of their data, and 4) attorneys who call on IT staff and experts early in a case to help identify, preserve, collect, process, produce, and generally assess the value and accessibility of their digital evidence.

For a number of years, courts have struggled with electronic discovery issues under procedural rules largely written to cover paper documents. The courts’ struggle has arisen from the fact that electronic documents vary significantly from their paper cousins. Bankers’ boxes bursting from an evidence room may impress an old-time litigator, but in terms of volume, they are no match for even one modest hard drive. A 40 gigabyte (40 GB) hard drive typically found within a modern laptop is physically smaller than a deck of cards, but it can hold rooms full of evidence — the equivalent of 20 million type-written pages.⁴

Apart from its sheer volume, digital information comes in a variety of forms that affect litigation. In paper discovery, document productions vary in quantity and possibly quality, but apart from an occasional 11” by 14” page, usually not in form. In contrast, electronic documents not only appear as numerous file types, but they also come loaded with “meta-data” that describe information “behind” each document.

In many ways, applying the old Federal Rules of Civil Procedure to modern discovery was like trying to fit a round peg into a square hole. Recognizing this, the Committee on Rules of Practice and Procedure (the Standing Committee) began considering rule changes as early as 2001. The Standing Committee typically considers proposals to changes in the rules after the proposals have been filtered through appropriate Advisory Committees.

In this instance, the Advisory Committee on Civil Rules analyzed electronic discovery in depth, held conferences, and

received input from experts, the judicial community, and practitioners. After the amendments were drafted and approved by the Standing Committee in August 2004, they were published and distributed for comment.

In 2005, three public hearings were held. The written and testimonial comments of numerous witnesses were then considered during the final drafting of the Rules.

Under the proposal approved by the Supreme Court, the basic framework and philosophy behind the Federal Rules remains intact, but the new Rules include explicit reference to electronically stored information in every aspect of the operative discovery rules. The most fundamental changes affecting electronic discovery are: 1) requirements to meet and confer with opposing counsel over data issues early in litigation, 2) requirements to identify even relatively hard-to-reach information early in a case, 3) provisions allowing for the testing and sampling of voluminous data, 4) requirements governing how data should be produced, 5) procedures to handle inadvertent disclosure of privileged and work product material, and 6) new spoliation rules governing sanctions for routine destruction or deletion of electronically stored information. Each of these new requirements is addressed below.

Rule 26(f) Conference of Parties; Planning for Discovery.

... the parties must as soon as practicable ... confer to ... *discuss any issues relating to preserving discoverable information*, and to develop a proposal discovery plan that indicates the parties' views and proposals concerning ...:

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

The new rules emphasize that parties to a lawsuit should meet and settle some important and fundamental discovery issues at the onset of litigation, purportedly to save litigants and the courts time and money. Under new Rule 26(f), the parties are required to meet "as soon as practicable" but at least 21 days before a discovery scheduling conference with the court.⁵

At this pre-conference meeting, the parties should discuss several electronic data issues with an eye toward presenting solutions and language to the court for inclusion in a Rule 16(b) scheduling order.

Specifically, the new Rules mandate that parties address at least four major issues: 1) where potentially relevant information exists and how accessible it is, 2) how preservation efforts will be affected by the nature of electronic data and computer operations, 3) how different data should ultimately be produced to each side, and 4) how counsel should handle inadvertent disclosure of privileged material or attorney work product material.

In order to meet their obligations under new Rule 26(f), attorneys will need to enter the pre-scheduling conference with a thorough understanding of their client's data storage practices and the relative accessibility of any potentially relevant data. Counsel should already know how a client's computer systems are laid out in order to meet the dictates of cases like *Zubulake v. UBS Warburg*,⁶ which require that an attorney issue a litigation hold to "key players" and "take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."⁷

Engaging Your Technical Experts and IT

New Rule 26(f) codifies this holding and in practical terms will require both in-house and outside counsel to get to know a company's IT staff early in the course of litigation. In larger cases, attorneys will find it prudent to hire translators who can "talk tech," namely technical consultants and e-discovery experts who can interact with IT staff and assist in identifying key data, ensuring the proper preservation and collection of discovery information. These experts will become important, not only when executing a discovery plan, but also when litigating a discovery dispute. Discovery experts will offer key testimony about the discovery steps taken by a party, the costs and burdens of retrieving data from specific storage areas, and the business or computer routines that may result in lost data.

Whether a case is large or small, a variety of IT staff will need to be interviewed early and possibly disclosed during discovery.⁸ These individuals include: network administrators who understand the standard build of an employee's computer and know where relevant electronic documents appear within individual or shared network folders; e-mail administrators who are familiar with mailbox size limits, auto-delete functions, and archiving protocols; backup specialists who know about disaster recovery and archiving procedures, tape locations, and rotation cycles; and database administrators who know how key transactional information (e.g., customer names, sales data, complaints, etc.) is captured and stored.

Equally important, attorneys and their experts will need to promptly interview key players who possess data related to new or foreseeable litigation. Not only will these individuals possess knowledge germane to the merits of the case, but for e-discovery purposes, they might also be able to confirm whether and how much data actually exists in specific locations described by company policies and procedures, and by IT staff.

Rule 26(a) Required Disclosures; Methods to Discover Additional Matter.

(1) **Initial Disclosures** ... a party must, without awaiting a discovery request, provide to other parties:

(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;

(2) Limitations.

(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. . .*

Attorneys will need to know where their clients' computer data reside because, in addition to the traditional disclosure of names of all individuals likely to have discoverable information, the new Rule 26(a) will require disclosure of the category and location of all relevant "documents and electronically stored information." This includes information that will be difficult to reach.

A quick reading of the new "Limitations" section of Rule 26(a)(2)(B) may lull some attorneys and their clients into a false sense of security, since the Rule encourages litigants to seek out the most accessible data first and exempts from discovery information that is "not reasonably accessible."⁹ In fact, this section should put most attorneys — especially corporate counsel — on high alert since it promises to provoke new, multi-million dollar fights between litigators (and their experts) over the relative accessibility of different data sources.

Most importantly, new Rule 26(a)(2)(B) imposes a new burden on litigants, namely that they identify data that they believe is "not reasonably" accessible. This requirement stands in contrast to the current practice of many attorneys who simply ignore hard-to-reach data or address the issue only when confronted by a motion to compel. The Advisory Committee claims that its proposed amendment is "modest" but admits that it is breaking new ground with this requirement and its "two-tiered" approach to electronic discovery.¹⁰ The Committee states:

Parties sophisticated in electronic discovery first look in the reasonably accessible places that are likely to produce responsive information. . . . But in an improvement over the present practice, in which the parties simply do not produce inaccessible electronically stored information, the amendment requires the responding party to identify the sources of information that were not searched, clarifying and focusing the issue for the requesting party.¹¹

The standard used to determine whether a data source is

"reasonably accessible" will still turn on the traditional question of whether discovery would impose an "undue burden or cost" on the producing party.¹² The Advisory Committee, however, provides some additional guidance regarding what data sources might not be reasonably accessible and lists the following: deleted data that may remain in fragmented form (requiring computer forensics to restore it); backup tapes; legacy data (from antiquated computer systems); and certain databases.¹³ These are merely suggestions in the Committee Notes, and litigants must still "provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources."¹⁴

In practical terms, this means that attorneys will need to get to work earlier to identify different sources of data by media type (e.g., backup tape, desktop hard drive, shared network drive, external USB hard drive, CD/DVD, etc.), physical and/or network location, program or file types, and data size. Attorneys may also need to identify the relevant date(s) and potential users covered within each data source.

To glean this type of information, attorneys should work with the client's IT staff and experts to be able to respond to fundamental questions, such as: What individuals or classes of employees have potentially relevant data? Where do they work? Where do they keep their work files — on their C:\ drives or on the network? How many backup tapes does IT have? Can we identify what data is on a tape by time period or employee name? How many hard drives do we need to image? Do we have the hard drives of former employees? Is any of the hard drive data encrypted? How many databases are relevant? Where are they located? Is all the data live on a particular server or part of a database archive? Is relevant data in a format that is not keyword searchable and in need of forensic processing?

Many attorneys might not like what they learn and be shocked to discover that their client is sitting on years of data and thousands of backup tapes. Yet, only through this type of inquiry can attorneys make the required disclosures under Rule 26 and estimate the cost of pursuing data that is not reasonably accessible.

Preservation Duties

Note that, even if a party initially identifies a source of information as "not reasonably accessible," that does not in any way mitigate the party's duty to preserve hard-to-reach data.¹⁵ Why? The court still may "order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C)."¹⁶ The limitations remain the same under Rule 26(b)(2)(C) as they were prior to the amendments and balance the benefits of the proposed discovery versus the costs of acquiring the data, taking into account various factors such as the needs of the case, the importance of the potential data in resolving key issues in the litigation, and the resources of the parties.¹⁷

The Advisory Committee notes that additional "good cause" considerations may include: 1) the specificity of the

request, 2) the quantity of data from alternate sources, 3) the failure to have produced more accessible data, 4) the likelihood of finding responsive information, 5) the importance and usefulness of the data, 6) the importance of issues at stake in the litigation, and 7) the parties' resources.¹⁸ Although not cited by the Committee, this is a reworked balancing test from e-discovery cases like *Rowe Entertainment* and *Zubulake*, which courts have used to shape discovery and make cost-shifting decisions.¹⁹

Courts may use the foregoing factors to "specify conditions for . . . discovery" and limit the amount or types of information to be produced or accessed.²⁰ In addition, the court may impose cost-shifting as a condition of discovery and thereby assess all or part of the cost of producing less accessible data on the requesting party.²¹

Cost-shifting can be especially important in lawsuits alleging ongoing illegal activity. In those instances, little data can be deleted on a going-forward basis. As a result, e-mail, documents, and backup tapes may simply pile up, raising the discovery costs and litigation stakes for all parties. See, "To Recycle or Not to Recycle, That Is the Hot Backup Tape Question."²²

Rule 34. Production of Documents, Electronically Stored Information, and Things . . .

(a) Scope. Any party may serve on any other party a request

(1) . . . to inspect, copy, *test*, or *sample* any designated documents or *electronically stored information*.

An important cost-control measure expressly included in the new Rules is sampling. Due to the immense amount of electronic data that many litigants accumulate, courts are already turning to this procedure and are likely to do so more often in the future.²³ Sampling may not only help determine whether disputed information is at all relevant to a case, but it also may help determine whether and to what extent the parties should share the costs of pursuing data that is not otherwise reasonably accessible. The preference for sampling large amounts of data is built into new Rule 34(a)(1). Traditionally, the Rules allowed parties to "inspect" designated documents, but new Rule 34(a)(1) now allows the parties to "test, or sample . . . electronically stored information" as well.²⁴

Sampling can take many forms. For example, a court may order the sampling of a few employees' data before requiring production across an entire business unit. A court also may require keyword testing on a limited set of e-mail accounts before allowing discovery across thousands of similar mailboxes.

Most often, though, the courts will likely use sampling to address nettlesome issues surrounding backup tapes. For

example, in a 2003 employment case directed at the U.S. Department of Justice, a D.C. federal district court ordered that the agency restore a sampling of the tapes and report on the costs and results.²⁵ The court then limited discovery to only those backup tapes covering the time periods related to the alleged employment incidents.²⁶

Rule 34. Production of Documents, Electronically Stored Information, and Things . . .

(b) Procedure. . . .

The [discovery] request may specify the form or forms in which electronically stored information is to be produced. . . . 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. . . .

(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.

In addition to the sheer volume of data that can be stored electronically, the available forms of electronic data are numerous. Just a few of the possibilities include Word documents, Excel spreadsheets, TIFF files, PDF files, database files, AutoCAD files (architecture drawings), e-mail files, and web logs.

Under new Rule 34(b), a requesting party can specify the form in which it wants discovery data, and in fact, this is a required topic for discussion at the pre-conference meeting under new Rule 26(f) described above. The responding party can object to the requested form and state its reasons for objecting. If there is no agreement as to form, new Rule 37(a)(2)(B) requires that the parties meet and attempt to solve the problem before either side can file a motion.

If the form is not specified or if the parties still do not agree, then a "default" form applies: the form in which the data is "ordinarily maintained."²⁷ If that form is not usable by anyone, then a party must produce the data in another "reasonably usable" form. Understanding the importance of keyword searching in modern discovery, the Advisory Committee further indicated in a Note that a party cannot take a searchable document and convert it into a format that is no longer searchable if that makes "it more difficult or burdensome for the requesting party to use the information efficiently in litigation."²⁸

New Rule 34(b) may re-enforce the growing tendency of courts to favor production of electronic documents in their native format because that is how they are “ordinarily maintained.”²⁹ The new Rule may be especially important in contract cases, patent litigation, civil fraud actions, and other litigation where the provenance of a document is key, and metadata from the native document best indicates when it was created, last modified, last accessed, last printed, and by whom.

Ultimately, new Rule 34(b) may create a tension between the review and production phases of discovery. On the one hand, litigation support managers may find it easier to read, mark, and redact documents in a uniform, non-native (.tiff or .pdf) format during the review phase. This is especially true if related hard-copy documents have already been converted to standard .tiff or .pdf formats and placed in a law firm’s document viewer like Concordance or Summation.

On the other hand, opposing parties may demand production of relevant electronic documents in native format (.doc, .wpd, .xls, .ppt) precisely because they want to view the full metadata that was available to the producing party. As review and production needs collide, law firms and their experts may have to process many documents twice, and attorneys will need to pay particular attention to vital but normally hidden information that could exist within the metadata of native documents produced to the other side. Such information could include a document’s “Track[ed] Changes,” dates, and last 10 authors.

Rule 26(b)(5) Claims of Privilege or Protection of Trial-Preparation Materials.

...

(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.*

While metadata from a native document can be important to the merits of a case, the existence of metadata along with the sheer volume of electronic data increases the risk that parties will inadvertently disclose privileged or work product information during electronic discovery. New

Rule 26(b)(5)(B) attempts to address this issue, at least procedurally. In fact, the new Rule does little to alter the litigation landscape, and attorneys will still need to conduct rigorous privilege reviews.

When a party realizes that privileged or work-product data has been disclosed in error, new Rule 26(b)(5)(B) requires notice to the other party that identifies the potentially covered information and states the reason for asserting the privilege. The responding party is then required to promptly “return, sequester or destroy” the information, and in any case, cannot use the information until the matter has been resolved.³⁰ If the information has already been disclosed to a third party, the responding party must take “reasonable steps to retrieve it.”³¹

In drafting this rule, the Advisory Committee specifically avoided substantive issues regarding privilege waivers and purposefully removed language referring to “reasonable time limits” and a party’s “intent to disclose.”³² Instead, the Advisory Committee merely streamlined the notification process and encouraged the parties to agree to specific “clawback” or “sneak-peek” procedures as part of their early Rule 26(f) discussions.³³

The Fourth Circuit has already criticized the new Rule for its lack of substance in *Hopson v. The City of Baltimore and the Baltimore City Police Department*.³⁴ There, the Court stated that “absent a definitive ruling on the waiver issue, no prudent party would agree to follow the procedures recommended in the proposed rule.”³⁵

The question of privilege waivers is further complicated by the fact that jurisdictions differ greatly on the issue. Courts apply tests ranging from a “strict accountability” standard to a “lenient ‘to err is human’ approach.”³⁶ Courts also consider a variety of factors, including the precautions taken to avoid the waiver, the volume of the discovery versus the extent of the specific discovery at issue, the time it takes a party to recognize its inadvertent disclosure, and the steps it takes to remedy the situation.³⁷

In short, as cautioned by the *Hopson* court, attorneys should continue to take reasonable steps to protect privileged or work-product material by reviewing it before producing it.³⁸ Even in jurisdictions that apply the most lenient waiver test, “the producing party still must show that reasonable measures were taken to screen for privileged review.”³⁹

In light of continued attention to waiver issues, technical experts will play ever larger roles in sorting through voluminous privileged and non-privileged information. This was demonstrated in the *Rowe* case where plaintiffs hired an agreed-upon expert to image specific hard drives and isolate pertinent e-mails on those hard drives.⁴⁰ Based on a set of search criteria established by both parties, the expert searched the hard drives and then had the plaintiff’s attorney review the documents on an “attorney eyes only basis.”⁴¹ Plaintiff’s counsel selected the documents that they considered relevant and material to the litigation and in turn, defendant’s counsel reviewed those documents in order to assert privilege and confidentiality claims.⁴² The Court approved this process,

noting that just because a document has been viewed by counsel or the expert, privilege had not been waived.⁴³

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.*

Among the Advisory Committee's proposed Rules, none received more public comment than new Rule 37(f), which prohibits sanctions for certain "lost" information due to routine computer operations.⁴⁴ This provision probably received the most public attention because the "oops" factor looms so large in cases involving electronic data, and sanctions for electronic discovery mistakes can be severe, ranging from hefty fines to case dismissals.

Mistakes surrounding automatic computer functions can be particularly devastating. Failing to flick off one auto-delete switch can result in the loss of thousands of e-mails, and the automatic rotation of a few backup tapes can eliminate weeks or months of corporate data.

The Advisory Committee struggled with its own recommendations for Rule 37(f) and ultimately split the difference between its original proposals. The Committee had issued two versions of the Rule, asking for comment on whether sanctions for routine deletions should be imposed based on mere "negligence" or "intentional and reckless" actions.⁴⁵ In the end, the Advisory Committee rejected both standards in favor of an intermediate "good faith" test.⁴⁶

Litigants and companies can demonstrate "good faith" in their preservation efforts by intervening "to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation."⁴⁷ Additionally, courts can consider, as a factor in the good faith analysis, whether a party took affirmative steps to comply with a court order regarding preservation of certain electronically stored information. Although Rule 37(f)'s first draft expressly denied protection to parties who violated a court order,⁴⁸ the Advisory Committee omitted that provision in its final proposed rule. The Committee feared that litigants would engage in "gotcha" tactics and overburden the courts by applying for preservation orders in every case, then sitting back and waiting for violations to occur.

As a practical matter, new Rule 37(f) may help attorneys focus the attention of their IT and operational colleagues on early preservation issues. See, "Rough Waters Ahead: No Smooth Sailing and No Safe Harbor: E-discovery and the New Federal Rules of Civil Procedure."⁴⁹ The proposed Rule highlights the fact that it will only shield parties from sanctions if they act quickly to preserve broad swaths of

information. Noting the interplay between proposed Rules 37(f) and 26(b)(2), the Advisory Committee emphasizes that "good faith may [even] require preservation of information on sources a party believes are not reasonably accessible. . . ."⁵⁰ Where routine operations are involved, this means that counsel will need to do a lot more than e-mail a general company-wide litigation hold. To capture the full benefit of Rule 37(f) protections, attorneys will need to roll up their sleeves and monitor compliance with that hold. They will need to consult with IT staff and technical experts to ensure that a litigation hold has actually reached the server room and that the continuation or cessation of routine computer functions conforms, not only to stated policies and procedures, but also to "good faith" discovery obligations.

Finishing Your Own Makeover

The common theme throughout the new Rules is that attorneys must acquire a solid, working understanding of their clients' electronically stored information, systems, and networks. At first, both in-house and outside counsel may feel insecure operating under the new Rules. Embracing the power of technology, however, attorneys can move beyond their yellow notepads, learn some computer jargon, reach out to their technical experts and staff, and complete their own needed makeovers. Then they can approach discovery conferences, document demands, data production, and general litigation with confidence under the new Federal Rules.

Mr. Luehr is Managing Director and Deputy General Counsel at the Minneapolis, MN office of Stroz Friedberg, LLC, a national computer forensics and electronic discovery firm. He specializes in cybercrime response, insider investigations, and complex e-discovery. He is a former federal prosecutor and Computer Crimes Coordinator for the District of Minnesota and brought cases against Internet fraud, child pornography, and hacking and initially oversaw the post-9/11 search of terrorist Zacarias Moussaoui's laptop. Mr. Luehr was previously an Asst. Director of the Federal Trade Commission and chaired the FTC's Internet Coordinating Committee. He is a frequent speaker and has lectured before national trade groups, the National Academy of Sciences, the FBI, the U.S. Dept. of Justice, and abroad as a U.S. State Department Speaker.

Ms. Perrin is Counsel and a Discovery Consultant at the Minneapolis, MN office of Stroz Friedberg, LLC. A certified electronic discovery specialist, Ms. Perrin advises attorneys and in-house counsel on complex matters involving paper and electronic document preservation and production, and she consults with Fortune 100 corporations about best practices related to data retention. She also oversees computer forensic investigations, including those into trade secret theft. Ms. Perrin's broad legal experience ranges from managing a small town firm to supervising discovery in national class-action litigation.