Background
There are several practical reasons why disputes regarding electronic evidence are on the increase. First, electronically stored information has become ubiquitous. Some have estimated that upwards 95 percent of all information is now created or at least stored electronically. Second, electronic evidence is pervasive in other ways that seemingly promote more disputes – it is more difficult to eliminate than paper documents; has content that changes over time even without human intervention; and includes information that is not readily apparent to one viewing a given file (often in the form of meta-data that provides information regarding the storage, modification and retrieval of the electronic file).

Recognizing the ever-increasing importance of electronic evidence, the Federal judiciary in the United States recently adopted new procedural rules. These rules are designed to anticipate problems with electronic discovery and avoid the drawn-out disputes that have occurred previously in many cases. Avoiding such disputes is important because they dramatically increase the transaction costs associated with litigating a case; often leave not only the parties, but the court, lacking critical evidence, thereby affecting the integrity of the decision making process; and frequently delay the ultimate resolution of the case. As was stated in United Medical Supply Co., Inc. v. United States,' 4

'Aside perhaps from perjury, no act serves to threaten the integrity of the judicial process more than the spoliation of evidence. Our adversarial process is designed to tolerate human failings – erring judges can be reversed, uncooperative counsel can be shepherded, and recalcitrant witnesses compelled to testify. But, when critical documents go missing, judges and litigants alike descend into a world of ad hocery and half measures – and our civil justice system suffers.'

Key provisions in the U.S. Federal Rules of Civil Procedure insofar as they relate to electronic discovery

Civil litigation in the Federal courts of the United States is generally governed by the Federal Rules of Civil Procedure. Those rules are promulgated under the Rules Enabling Act, which authorizes the U.S. Supreme Court to prescribe 'general rules of practice and procedure and rules of evidence for cases in the United States district courts . . . and courts of appeals.' These rules permit discovery as to 'any matter, not privilege, that is relevant to the claim or defense of any party.' Generally speaking, Federal courts are required to limit all forms of discovery when the burden or expense of the proposed discovery outweighs its likely benefit. U.S. District courts have local rules or guidelines that may impose additional duties, including duties relating to electronic discovery. Many States have rules or general orders that contains electronic discovery provisions which parallel those of the Federal rules.

What are some of the key provisions of these Federal

1. This article is adapted from an outline used by Judge Allegra to make his presentation to the International Conference on Digital Evidence developed by Stephen Mason and run by MIS Training in London, June 2008.
Rules, insofar as they relate to electronic discovery? To begin with, Rule 16 of the Federal Rules of Civil Procedure anticipates that the court will conduct one or more pretrial conferences to discuss the management of the case. Rule 16(b)(1) requires the district court to issue a scheduling order for the case. Rule 16(b)(4) permits U.S. district courts to include in that scheduling order ‘provisions for disclosure or discovery of electronically stored information.’ Rule 16(b)(6) further provides that such orders may include any agreements reached by the parties for handling the production of privileged documents. According to the Advisory Committee Notes (which notes are generated by the drafters of the rules), Rule 16 ‘is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur.’ These notes further indicate that the parties might agree to various arrangements to handle privileged materials.

Rule 26 of the Federal Rules of Civil Procedure includes special provisions that govern the discovery of electronic evidence. Rule 26(a) requires parties to include certain information about electronically stored information in their initial disclosures (those materials exchanged by the parties prior to formal discovery). Specifically, the rule provides that a party must, without awaiting a discovery request, provide to other parties ‘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.’

Rule 26(b)(2)(B) provides that, absent a court order, ‘[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.’ The producing party must, if challenged, demonstrate that the information truly is ‘not reasonably accessible;’ if it makes such a showing, the requesting party may obtain the production only if it can show ‘good cause.’ Rule 26(b)(2)(C) requires a court to weigh the potential benefit or importance of all requested information – including electronically stored information – against the burden of having to produce the information. Rule 26(b)(2)(C)(i) indicates that discovery may be limited if ‘the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.’ Rule 26(f) requires that, in advance of the scheduling conference to be held under Rule 16, the parties ‘meet and confer’ to address various issues regarding discovery and to develop a discovery plan. Rule 26(f)(2) indicates that while conferring, the parties may discuss ‘any issues about preserving discoverable information.’

Rule 26(f)(3)(C) indicates that the proposed discovery plan should discuss the parties’ views on ‘any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.’ Rule 26(f)(3)(D) indicates that the same plan should discuss the parties’ views on ‘any issues about claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert these claims after production – whether to ask the court to include their agreement in an order.’

Rule 34 of the Federal Rules of Civil Procedure governs the production of electronically stored information. Rule 34(a)(1) makes clear that the discovery provisions of the rule apply to any ‘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 either directly or, if necessary, after translation by the responding party into a reasonably usable form.’ The Advisory Committee Notes explain that references in all of the rules to ‘electronically stored information’ should be understood to invoke the expansive definition employed in this rule. Rule 34(a)(1) further makes it clear that the parties may request an opportunity to test or sample materials sought under the discovery rules before copying them.

Rule 34(b)(1)(C) indicates that the request for document may ‘specify the form or forms in which electronically stored information is to be produced.’ The rule envisages that the requesting party may specify different forms of products for different types of electronically stored information. Rule 34(b)(2)(D) indicates that the party responding to the request may ‘state an objection to a requested form for producing electronically stored information;’ if such an objection is lodged, the responding party ‘must state the form or forms it intends to use.’ Rule 34(b)(2)(E) indicates that ‘[u]nless otherwise stipulated or ordered by the court’:

(i) A party must produce documents as they are kept in the usual course of business or must organize
The loss or destruction of evidence engenders distrust and can totally destroy the potential for developing a good working relationship with one’s opposing counsel – the sort of relationship that is essential to managing electronic discovery.

and label them to correspond to the categories in the request;
(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
(iii) A party need not produce the same electronically stored information in more than one form.

Rule 33 of the Federal Rules of Civil Procedure, which involves interrogatories to parties, includes provisions designed to parallel the electronic discovery provisions of Rule 34.

Finally, Rule 37 of the Federal Rules of Civil Procedure authorizes the imposition of sanctions when a litigant or an attorney fails to comply with discovery rules or orders. Sanctions may be imposed under Rule 37(b), upon the failure of a party to comply with an order, or under Rule 37(d), upon a complete failure to comply with a discovery request. Rule 37(e) indicates that ‘[a]bsent 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.’

The Advisory Committee Notes explaining Rule 37(e) clarify that ‘[g]ood faith in the routine operation of an information system may involve a party’s intervention 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,’ adding that ‘a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve.’

Common pitfalls that lead to electronic discovery disputes in the United States – and how to avoid them

Failing initially to take proper steps to preserve electronic information

In the United States, the duty to preserve evidence attaches whenever a party knows or should know that evidence may be relevant to anticipated litigation. This duty clearly extends to electronically stored information.

While the existence of this duty to preserve is common knowledge among U.S. lawyers, litigants and their attorneys often move too slowly to protect documents, initially take steps that prove inadequate in protecting documents, or fail to identify all the documents that need to be protected. Often, this results in the spoliation of electronic evidence, frequently as the result of periodic in-house destruction policies that should have been modified or suspended once litigation was anticipated.

Nothing fans the fires of discovery disputes more than the spoliation of documents. As stated in the Advisory Committee Notes to Rule 26, ‘[f]ailure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes.’ The loss or destruction of evidence engenders distrust and can totally destroy the potential for developing a good working relationship with one’s opposing counsel – the sort of relationship that is essential to managing electronic discovery. Such conduct provides the predicate for the court to enter a ‘document preservation order,’ potentially leading to heavy-handed court-supervision of the retention and storage of electronic information. Spoliation also can lead the court to impose significant sanctions under either Rule 37 of the Federal Rules of Civil Procedure or the court’s inherent authority. Such sanctions may be financial.

* For example, see Barsoum v. NYC Housing Authority, 202 F.R.D. 396, 399 (S.D.N.Y. 2001) (construing this Federal rule).
* Silverstri v. General Motors Corporation, 271 F.3d 583, 591 (4th Cir. 2001); Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998); The Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 135 (2004).
* For generally, The Pueblo of Laguna v. United States, 60 Fed. Cl. at 138-39 (noting that the prior spoliation of evidence gravitates in favour of a document preservation order being entered).
(such as fines or the imposition of attorney’s fees) or take the form of limitations on the issues and types of evidence that may be presented at trial.\footnote{United Medical Supply Co., Inc. v. United States, 77 Fed. Cl. 257 (2007).} As noted above, Rules 16 and 26 of the Federal Rules of Civil Procedure anticipate that many problems involving electronic discovery will be raised and resolved at the preliminary status conference. However, many litigants arrive at that conference unprepared to discuss seriously many of the issues involving the discovery of electronically stored information. This lack of preparation often stems from counsel’s lack of knowledge concerning: technology, in general, and electronically-stored information, in particular; how various forms of electronically-stored information might potentially relate to proof of facts in the case; key technical attributes of their client’s electronically stored information (for instance, format, ease of accessibility); and key attributes of their opponent’s electronically stored information. The use of technical consultants, as well as legal consultants specializing in electronic discovery, may serve to assist counsel in improving their knowledge. At a minimum, technical support is often required to ensure that counsel ask their clients and opposing parties the right questions.

Thereafter, continuously verify that the steps to protect electronically information are being properly implemented. As noted by the Sedona Conference, “[d]ecisions regarding the preservation of electronically stored information should be a team effort, often involving counsel (both inside and outside), information systems professionals, end-user representatives, records and information management personnel, and, potentially, other individuals with knowledge of the relevant electronic information systems and how data is used, such as information security personnel.”

If the case has been filed, notify opposing counsel and the court immediately if it becomes known that documents were destroyed before steps could be undertaken to preserve them.

Larger organizations that are often in litigation should have proper records and information management policies and programs in place that not only provide for reasonable practices regarding the retention and destruction of electronically stored information, but also detail the specific steps that should be taken once litigation regarding a particular matter is anticipated.\footnote{Sedona Principles at 29.}

In general, where destruction occurs, courts will be less likely to penalize reasonable efforts to preserve documents that were undertaken in good faith. This conclusion is reinforced by Rule 37(e) of the Federal Rules, which, as mentioned prevents courts from sanctioning a party that undertakes certain good-faith efforts to preserve electronically stored information.

Failing to maximize the value of the preliminary status conference

As noted above, Rules 16 and 26 of the Federal Rules of Civil Procedure anticipate that many problems involving electronic discovery will be raised and resolved at the preliminary status conference. However, many litigants arrive at that conference unprepared to discuss seriously many of the issues involving the discovery of electronically stored information. This lack of preparation often stems from counsel’s lack of knowledge concerning: technology, in general, and electronically-stored information, in particular; how various forms of electronically-stored information might potentially relate to proof of facts in the case; key technical attributes of their client’s electronically stored information (for instance, format, ease of accessibility); and key attributes of their opponent’s electronically stored information. The use of technical consultants, as well as legal consultants specializing in electronic discovery, may serve to assist counsel in improving their knowledge. At a minimum, technical support is often required to ensure that counsel ask their clients and opposing parties the right questions.

The disclosures made under Rule 26(a)(1) of the Federal Rules of Civil Procedure should provide baseline information regarding the nature of an opposing party’s computer systems, as well as the software applications used to operate those systems. Nonetheless, Rule 26(f) of the Federal Rules means what it says when it requires parties to ‘meet and confer’ about electronic discovery matters. Yet, ‘[a]ll too often, attorneys view [this] obligation . . . as a perfunctory exercise.’ Instead, as described on pages 4-5 in the FJC Pocket Guide, prior to the preliminary conference, the parties should inquire into: whether there will be discovery of [electronically stored information]; what information each party has in electronic form and where that information resides; whether the information to be discovered has been deleted or is available only on backup tapes or legacy systems; the anticipated schedule for production and the format and media of that production; the difficulty and cost of producing the information and reallocation of costs, if appropriate; and the responsibilities of each party to preserve [electronically stored information].

Armed with proper information, many discovery
disputes can be avoided by reaching agreement with the opposing counsel on several key points and having the court adopt those agreements as part of its preliminary order. In this regard, consider developing:

- a plan that specifically addresses the client’s preservation obligations, explicitly listing what needs to be preserved (and how) and what does not;

- a phased discovery plan that focuses first on the production of relevant data from the most accessible sources and postpones the production of data from the least accessible sources until it becomes clear that data is needed;

- an agreement to exchange samples of relevant data, so that discovery requests can be developed with a specific eye as to what might be produced. The use of such samples, in particular, should allow both parties to determine what they truly need and limit the unnecessary production of meta-data; or

- an agreement to employ a common litigation support platform that both parties can use, so as to lessen problems associated with the form of production. In agreeing to such a platform, keep in mind the eventual need to present evidence to the court.

If, despite good faith efforts, it proves impossible to reach agreement on any of the above points, consider moving the court for a carefully-tailored protective order. If, despite good faith efforts, it proves impossible to reach agreement on any of the above points, consider moving the court for a carefully-tailored protective order

**Failing to develop, and format properly, discovery requests and objections**

Many electronic discovery disputes find their genesis in poorly-formatted electronic discovery requests, overbroad objections, or both. Frequently, discovery requests seek more data than is needed, including metadata that is wholly unnecessary (e.g., over which internal servers and e-mail traveled on its way to the internet). Be aware that some e-mail systems generate upwards of 140 items of metadata for each message. In many instances, the requesters are unaware of what compliance with their requests entails or will yield – this frequently occurs when attorneys attempt to use boilerplate definitions that sweep up all electronic mail, databases, word processing files, and such like. In many instances, overbroad requests yield so much information as to render the production useless to the requesting party. And, if a dispute arises, such overbroad requests are rarely enforced.\(^4\) Requests involving electronically stored information may also be overbroad if they do not adequately specify the form of production. Rule 34(b)(2) potentially supplies two defaults in this regard, allowing such information to be produced in either the form ‘in which it is ordinarily maintained’ or a form that is ‘reasonably usable.’

Overbroad requests are often met with equally-overbroad objections. Most U.S. courts expect that objections to production will be made with particularity – enough detail so that the requesting party can reexamine whether it really needs the information and so that the court can resolve any continuing disputes.\(^7\) Rule 26(B)(2)(B) requires the recipient of such requests to distinguish between information that is reasonably accessible and that which is not. Further, under Rule 34(b), if the request does not specify the form of production or the responding party objects to the form requested, it must identify the form or forms it intends to use.

Both blanket requests and blanket objections invite judicial intervention, often with the result that neither party gets what it wants. While judicial resolution of disputes involving overbroad requests or objections sometimes takes the form of giving each party a bit of what they want, courts, at other times, react to such disputes by either completely disallowing the electronic discovery request or completely rejecting the objection and ordering full production. As Scheindlin J stated in *Zubulake*, *[S]pecifity is surely the touchstone of any good discovery request, requiring a party to frame a request broadly enough to obtain relevant evidence, yet narrowly enough to control costs.*\(^8\)

Discovery requests and objections should not be crafted without first knowing the computer systems involved. Counsel should take full advantage of the test and sampling provisions in the Federal rules, such as Rule 34(a) and any agreements crafted thereunder to tailor their requests and objections the realities of how given data is maintained.\(^8\) In particular, efforts should be made to avoid requesting more than one copy of the same data (e.g., the active data as well as recovery backup tapes), unless data integrity or

---

\(^4\) For which, see *Wright v. AmSouth Bancorporation*, 320 F.3d 1198, 1205 (11th Cir. 2003).  
\(^\text{1}\) Conclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail.*

\(^\text{2}\) *Zubulake v. UBS Warburg, LLC,* 217 F.R.D. at 321.  
\(^\text{3}\) *McPeek v. Ashcroft,* 202 F.R.D. 31 (D.D.C. 2001);  
McPeek v. Ashcroft, 212 F.R.D. 33 (D.D.C. 2003);  
Hagemeyer N. Am., Inc. v. Gateway Data Sciences Corp., 222 F.R.D. 594 (E.D. Wis. 2004) (all supporting the use of sampling to tailor the scope of further discovery).
authenticity issues are at issue. A narrowly-tailored request is more likely to produce relevant information and to reduce the transactional costs associated with obtaining and organizing the materials requested. And if a dispute does arise, the court likely will more favorably look upon narrowly-tailored requests and objections.

Even if the requests or objections are initially overbroad, the parties should still seek to compromise their positions before bringing their dispute to the court. Indeed, Rules 37(a)(1) and 37(a)(2)(B) of the Federal Rules of Civil Procedure indicates that a motion to compel discovery 'must include a certification that the movant has in good faith conferred or attempted to confer with the person or party failing to make disclosure or discovery in an effort to obtain it without court action.' This requirement is often strictly enforced.22

Failing to anticipate adequately privilege issues

Rule 26(b)(1) of the Federal Rules of Civil Procedure provides that a party may obtain discovery of any matter that: (i) 'is not privileged' and (ii) 'is relevant to the claim or defense of any party.'23 While there are as many as a dozen privileges under U.S. law, two of the most commonly-asserted privileges are the attorney-client privilege and the work product doctrine.

The attorney-client privilege, which has its roots in Roman law, 'protects the confidentiality of communications between attorney and client made for the purpose of obtaining legal advice.'24 The privilege encourages 'full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice.'25

In the United States, the work-product doctrine can be traced to the U.S. Supreme Court's opinion in Hickman v. Taylor, 329 U.S. 495, 510 (1947), in which the Court rejected 'an attempt, without purported necessity or justification, to secure written statements, private memoranda and personal recollections prepared or formed by an adverse party's counsel in the course of his legal duties.' That doctrine has now been incorporated into Rule 26(b)(3) of the Federal Rules of Civil Procedure which states that documents 'prepared in anticipation of litigation or for trial' are discoverable only upon a showing of ‘substantial need’ for the materials and 'undue hardship' if they are not produced. These privileges may be waived if information is disclosed to any opposing party, even if the production of privileged information is inadvertent. In some circumstances, the waiver affects not only the document produced, but also every document involving the same subject matter.26

Disputes often arise when electronic documents are inadvertently produced giving rise to claims that a given privilege has been waived. Disputes also arise when the party seeking to assert the privilege does not provide an accurate privilege log or makes blanket claims of privilege that are plainly inappropriate. The enormous costs and delays that can be associated with reviewing documents and generating an accurate privilege log only serve to heighten the likelihood of disputes arising. Privilege reviews can require the producing party to review not only the basic electronic documents, but also the underlying metadata. Some disputes are driven by debates over who should bear particular costs associated with searching and providing data.27

There are various ways to minimize disputes over privileges (or at least minimize the cost and delay associated with such disputes). Consider entering into an agreement that allows for the initial examination of the requested materials without waiving any privilege or protection – sometimes known as a ‘quick peek’ agreement. Under this arrangement, a party first provides documents to the opposing party under the agreement. The receiving party uses the results of its preliminarily review of those documents to designate the documents that it actually wishes to be produced. The responding party then responds in the usual course, screening only those documents that are formally requested and asserting privileges under Rule 26(b)(5)(A). Alternatively, consider entering into a ‘clawback’ agreement that minimizes both parties privilege risks, for which see Fed. R. Civ. P. 26(b)(5). As described in the Advisory Committee Notes to the Federal Rules, under such arrangements, the parties agree that the production of documents ‘without an intent to waive privilege or protection should not be a waived so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances.’ ‘Quick peek’ and ‘clawback’ agreements

---

22 For example, see Ross v. Citifinancial, Inc., 203 F.R.D. 239, 240 (S.D. Miss. 2001) (“This prerequisite is not an empty formality,” but rather often leads to the “resolution of discovery disputes by counsel without intervention by the Court.”); IA Wright & Miller, Federal Prac. & Proc. § 2285 (2008).
26 In re Keeper of Records (XYZ Corp.), 348 F.3d 16, 22 (1st Cir. 2002); Evergreen Trading, 80 Fed. Cl. at 128-29, 133.
are only a few of the sorts of agreements that might be
devised not only to avoid disputes over privileges, but
also substantially reduce the transaction costs
associated with reviewing documents for privileged
materials. These agreements can be given to the court
to be incorporated into case management orders.

Nonetheless, care must be taken in using and drafting
these agreements. Individuals and entities that are not
parties to the agreement might contend in other
litigation that the production of certain electronic
documents pursuant to such agreements had the effect
of waiving the associated privileges.\footnote{Hopson v. Mayor and City Council of Baltimore, 232 F.R.D. 228, 235 (D. Md. 2005); Sedona Principles at 5A-54.}

Conclusion

In sum, while, in the United States, some disputes
involving electronic discovery are inevitable, others are
easily avoided if the parties proceed in a reasonable
fashion, with good faith, and taking full advantage of
the recent advancements incorporated into the Federal
Rules of Civil Procedure.

© Francis M. Allegra, 2008