ELECTRONIC DISCOVERY PRIMER FOR JUDGES

By David K. Isom*

Abstract

[a.1] More than 99% of information now being created and stored is created and stored electronically. Though many parties and lawyers, for strategic and other reasons, still prefer to convert electronic data to paper for production in litigation, the percentage of document production that is electronic is growing and the reasons for preferring electronic discovery are becoming more obvious and widely known. The technology facilitating electronic discovery is becoming more accessible. The law of electronic discovery is beginning to emerge, but most issues are so unexplored that judges must still develop much important law. In doing so, courts must be guided as much by principles of basic fairness and good case management in light of the emerging technology, as they are guided by precedent. As U.S. Magistrate Judge Paul W. Grimm has said, "Under Rules 26(b)(2) and 26(c), a court is provided abundant resources to tailor discovery requests to avoid unfair burden or expense and yet assure fair disclosure of important information. The options available are limited only by the court's own imagination. . . ."

[a.2] This article is a practical guide for judges to the main electronic discovery issues likely to be presented in the foreseeable future, and a brief discussion of possible solutions.

Table of Contents

---

* David K Isom is a shareholder in Greenberg Traurig LLP's Denver office. He does commercial litigation and electronic discovery consulting, and leads the firm's electronic discovery practice group. The author acknowledges the assistance of United States Magistrate Judge David Nuffer, District of Utah, throughout the conception and development of this article. The author also thanks the following for their insightful suggestions: Diane Block; Macyl Burke; Bob Gomes; Honorable Ronald Hedges; Matthew R. Howell; Andy Johnson-Laird; Ronald Kilgard; Sharon D. Nelson; Anne Rogers; John Simek; J. Preston Stieff; and United States Magistrate Judge John M. Facciola, United States District Court for the District of Columbia.

I. INTRODUCTION

[I.1] More than 99% of new human information now being created and stored is stored electronically.[1] Most parties and lawyers are more comfortable with traditional paper discovery and still prefer, for strategic and other reasons, to convert electronic data to paper for production in litigation. But electronic discovery is growing and the reasons for preferring electronic discovery are becoming more obvious and widely known.

[I.2] Magistrate Judge John Hughes has urged that "the production of electronic information should be at the forefront of any discussion of issues involving discovery and trial . . . ."[2] Judge Hughes also advised that in future cases, electronic discovery should be discussed from the beginning of a case, e.g. by counsel in Rule 26 conferences, and by counsel and the court in Rule 16 conferences. But, to date, only a few federal district courts (Arkansas, Delaware, Kansas, New Jersey and Wyoming) and state courts[3] (Mississippi and Texas) have local rules, standing orders or guidelines requiring early discussion of electronic discovery in civil litigation.[4]

---

[1] Peter Lyman and Hal R. Varian, *How Much Information 2003?*, at http://www.sims.berkeley.edu/research/projects/how-much-info-2003/ (last visited Oct. 28, 2004) (showing that, of an estimated 5.6 million terabytes of data stored in 2002, 5.18 million terabytes were stored electronically and an additional 420,000 were stored on film). Technically speaking, "electronically stored information," as used in the proposed new federal rules discussed below and in the trade literature, seems to mean "information that is created and stored using an electronic process on a medium other than paper – such as optical media (DVDs or CD-ROMs) and magnetic media (such as hard disks and magnetic tapes) – and that may be retrieved and processed using an electronic medium." The shorter phrase is adequate and obviously preferable.

[2] *In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 444 (D.N.J. 2002).

[3] This article examines electronic discovery in federal courts under the Federal Rules of Civil Procedure. State judges are seeing electronic discovery issues with increasing frequency, and some of the discussion here will apply to state court litigation. Some of the issues addressed here, however, when they arise in state courts, will be governed by state rules and case law that are substantially different from federal rules and case law.

For example, now that Rule 53 regarding special masters has been amended (as discussed below), the federal rules governing the appointment of special masters are quite different than rules in states that have not recently amended their rules relating to special masters. *See, e.g.,* Ronald Kilgard, *Discovery Masters: When They Help – and When They Don't*, 40 ARIZONA ATTORNEY 30 (2004) (hereinafter "Kilgard, *Discovery Masters*") (comparing Arizona's special masters rules to federal rules both before and after the 2003 amendments to Federal Rule 53).

Another example: some states may have rules governing the allocation of discovery costs that are quite different from the federal rules. *See, e.g.*, *Lipco Elec. Corp. v. ASG Consulting Corp.*, 2004 N.Y. Misc. LEXIS 1337, No. 01-8775/01, 2004 WL 1949062, at *4 (N.Y. Sup. Ct. August. 18, 2004) (noting that, unlike federal rules, New York state rules require the party seeking production of data and documents to pay the costs of production).

[4] *See* Honorable Ronald J. Hedges, *Discovery of Digital Information* (Sept. 27, 2004), *at* (continued...)

[I.3] In August 2004, the federal Standing Committee on Rules of Practice and Procedure promulgated proposed amendments to the Federal Rules of Civil Procedure[5] dealing with discovery of electronic documents and data.[6] Though some changes, even significant changes,[7] could be made to the proposed new rules before they are adopted, it seems certain that amendments to the Federal Rules of Civil Procedure will soon be adopted (possibly by early 2006), placing new emphasis on electronic discovery. This article discusses the likely impact of the proposed new rules.

[I.4] Under the proposals, Rule 26(f) of the federal rules[8] would require counsel at the outset of the litigation "to discuss any issues relating to preserving discoverable information . . ."[9] and to develop a discovery plan addressing "any issues relating to disclosure or discovery of electronically stored information, including the form in which it should be produced."[10]

[I.5] Proposed Rule 16(b) would be amended to require the parties and the court, at the pretrial scheduling and management conference, to establish a schedule "for disclosure or discovery of

---

[4] (...continued)
http://www.kenwithers.com/articles/index.html (last visited Oct. 26, 2004).

[5] The proposed rules are available at http://www.uscourts.gov/rules/newrules1.html (last visited Sept. 30, 2004) (hereinafter "Proposed Rules") (pinpoint citations are to the actual Proposed Amendments to the Federal Rules of Civil Procedure, which follow a twenty-page transmittal memorandum).

[6] The proposed amendments are the culmination of five years of consideration. For an excellent article chronicling and analyzing the development of the proposed new federal rules on electronic discovery during which time electronic discovery has grown from rarity, infancy, and obscurity to become the core of much cutting edge civil litigation, see Ken Withers, *Two Tiers and a Safe Harbor: Federal Rulemakers Grapple with E-Discovery* (Aug. 23. 2004), *at* http://www.kenwithers.com/articles/index.html (Aug. 23, 2004).

[7] Two of the proposed new rules are controversial and may undergo some change as a result of comments and criticism that are emerging. These proposals – which appear designed to add some protection against discovery of inaccessible documents and create a safe harbor from rules-based sanctions for some failures to produce documents – are discussed below.

[8] "Federal rules" and "rules" refer to the Federal Rules of Civil Procedure unless otherwise indicated.

[9] Proposed additions to the federal rules are underlined in this article. Proposed deletions are ~~stricken~~.

[10] Proposed Rule 26(f), *supra* note 6, at 8-9.

electronically stored information."[11] Form 35 would be amended to require that the written report of the parties' planning meeting would include a joint proposal as to how "[d]isclosure or discovery of electronically stored information should be handled . . . ."[12]

[I.6] Thus, even in jurisdictions where electronic discovery is still rare, judges and the parties and counsel will be prompted to consider electronic discovery early in all cases.

II. DISCUSSION

[II.1] The remainder of this article deals with the principal electronic discovery issues that judges are likely to face.

A. DEFINING "DOCUMENT" AND "ELECTRONIC INFORMATION"

[II.A.1] The scope of the data subject to discovery under the rules has been clarified by the proposed new rules. Since at least 1970, when the definition of "document" in Rule 34 was amended to include "data compilations," electronic data has been discoverable under Rules 34 and 45 of the Federal Rules of Civil Procedure.[13]

[II.A.2] The proposed new federal rules would make clear that electronic data in its native form is discoverable, and remove any argument that discovery is limited to compilations of that data. The title of Rule 34 would add the phrase "Electronically Stored Information" to the "Documents" and "Things" that are discoverable under Rule 34.[14] The new rules would add that "electronically stored information [and] any designated documents [including] . . . sound recordings, images ~~phonorecords~~ and other data or data compilations in any medium" are discoverable.[15] The Committee Note to new Rule 34(a) emphasizes the breadth of the types of information intended to be within the scope of Rule 34 discovery:

> The definition in Rule 34(a)(1) is expansive, including any type of information that can be stored electronically . . . . The reference to "data or data compilations" includes any database currently in use or developed in the future. The rule covers information stored "in any medium," to encompass future developments in computer technology.

---

[11] Proposed Rule 26(b), *supra* note 6, at 2.

[12] Proposed Rules Form 35, *supra* note 6, at 51.

[13] *See Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002).

[14] Proposed Rules, *supra* note 6, at 24.

[15] *Id.* at 24-25.

> Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.[16]

[II.A.3] Thus, proposed Rule 34 seems broad and flexible enough to embrace future developments in computing, biological, biomedical and chemical technologies.

B. MANAGING ELECTRONIC DISCOVERY

[II.B.1] Because of the diversity of issues surrounding electronic discovery, and because those issues are new for courts, parties, and lawyers, early and continual attention to electronic discovery is essential.

[II.B.2] *In re Bristol-Myers Squibb Securities Litigation*[17] is a cautionary tale in which the putative class action plaintiffs agreed to pay for copying paper documents they had requested from the defendant, obviously aware of what every judge and lawyer now must know: that paper documents come from electronic data. When plaintiffs' counsel realized that electronic data would be more manageable, more helpful and less expensive in the litigation, they sought in electronic form the data that had already been produced on paper.[18] Plaintiffs' counsel also refused to pay for the paper copies that had already been made. Judge Hughes ordered that electronic versions of the documents must be produced, but also ordered plaintiffs to pay the approximately $300,000 that they had agreed to pay for the now-useless paper. Judge Hughes was faced with a problem that often faces judges –

---

[16] Proposed Rules, *supra* note 6, at 28-29. Note that "data" is included in the definition of discoverable "documents" and "information." In some computer literature, useful distinctions are made between "data" and "information," depending primarily upon the use of the information or data, and upon whether the reader or audience can understand the data without translation or conversion. In general, data become information when the reader or user understands the syntax, format and semantics of the data. The distinction between "data" and "information" is not important in the proposed rules because the scope of the rules is broad and because both "data" and "information" are clearly included within scope of the proposed new rules. This article therefore uses "data" and "information" interchangeably.

[17] 205 F.R.D. 437 (D.N.J. 2002).

[18] The new ABA Civil Discovery Standards suggest several ways to avoid what happened here: that the requesting party should specify in the request whether electronic or paper documents are sought; that an electronic production should be presumed if the request does not so specify; that the specific electronic format (*e.g.*, native, searchable, etc.) should be specified in the request; and that ordinarily a party need not produce the same document in more than one format. Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29)(b), *at* http://www.abanet.org/litigation/taskforces/electronic/home.html (under "Amendments to the Civil Discovery Standards" and "Final Revised Standards") (Aug. 2004) (redline version).

how much to intervene to resolve problems created by counsel's inattention or ignorance. Judge Hughes said: "The Court was sorely tempted to place some sort of affirmative burden upon the party creating information in electronic form, for trial preparation purposes, to so advise the adversary before responding to paper document requests. However, in dealing with issues of this nature, the Court believes in what ought to be a familiar maxim: lawyers try cases, not judges."[19]

[II.B.3] The moral is clear: judges and lawyers must be conscious of the risks and benefits of electronic discovery and actively manage electronic discovery from the beginning of the case. The duties of lawyers to raise, negotiate and resolve discovery issues, and the need for courts to manage discovery actively, are more important for electronic discovery than they were for paper discovery. Not only does effective electronic discovery present novel and sometimes difficult technical issues, the cost and complexity of electronic discovery can vary significantly depending upon the issues and evidence, and upon the effectiveness of the court, the lawyers, and the parties.

[II.B.4] As discussed above, the proposed new rules reflect this importance and require counsel and the court explicitly to address electronic discovery from the beginning of the case.

[II.B.5] Judge Hughes' comment also points out the need for measured judicial intervention in electronic discovery. Because judges may deal with more electronic discovery issues than do some counsel, they may see opportunities for – or pitfalls in – electronic discovery where counsel do not. Judges may also assume they have insights into technology that are not truly applicable in the data systems present in another case. In this relatively unexplored area, caution will keep the court in a position of resolving controversies, rather than creating them.

C. PRESERVING DISCOVERABLE INFORMATION: PRESERVATION ORDERS

[II.C.1] People and companies have a duty, without being so ordered by a court, to preserve documents that they reasonably anticipate may be discoverable[20] in foreseeable litigation.[21] Though this duty exists even in the absence of a court order requiring preservation, in some cases a preservation order can be helpful to increase the likelihood that data will be preserved; to define what data must be preserved and what may be destroyed; and to increase culpability and severity of

---

[19] *In re Bristol-Myers*, 205 F.R.D. at 443.

[20] The preservation duty applies to *discoverable*, not just *admissible*, documents and things. In general, preservation orders ought also to aim at discoverable, not just admissible, data. *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 434 (W.D. Pa. 2004).

[21] The violation of this duty – spoliation – is discussed below. *See infra* note 98.

sanctions if evidence is not preserved.[22] This section discusses issues that will confront courts considering whether to enter preservation orders or not.

[II.C.2] Courts certainly have the power to enter preservation orders. *Pueblo of Laguna v. United States*[23] is a helpful recent analysis of the sources of this power and how it ought to be used. There, the plaintiff pueblo sought an order requiring that various federal agencies preserve certain categories of documents relating to the pueblo's claims. The government resisted the order, arguing that an order was unnecessary because the government was already required to preserve the documents by its record retention policies and by statutes and regulations.

[II.C.3] District Judge Francis M. Allegra first held that federal courts have inherent power and power under Rule 16[24] to enter such orders. He then held that two issues govern when that power ought to be exercised: (1) whether the order is "necessary" and (2) whether the order is unduly burdensome. Judge Allegra said:

> To meet the first prong of this test, the proponent ordinarily must show that absent a court order, there is significant risk that relevant evidence will be lost or destroyed - a burden often met by demonstrating that the opposing party has lost or destroyed evidence in the past or has inadequate retention procedures in place.[25]

[II.C.4] The court found that the first prong[26] was satisfied by the government's mishandling and destruction of documents in related Indian litigation.[27] Judge Allegra ordered the government to:

---

[22] If the proposed "safe harbor" provision discussed below is added as Rule 37(f), preservation orders may be requested more often than now, given that a prior preservation order would exempt data from the safe harbor of proposed new Rule 37(f).

[23] No. 02-24 L, 2004 U.S. Claims LEXIS 49, 60 Fed. Cl. 133 (Fed. Cl. Ct. Cl. March 19, 2004)

[24] This conclusion would be bolstered by Proposed Rule 16(b)(5), which would expressly authorize courts to make pretrial orders regarding "disclosure or discovery of electronically stored information . . . ." Proposed Rules, *supra* note 6, at 1-2.

[25] *Pueblo of Laguna*, 2004 U.S. Claims LEXIS 4960 Fed. Cl. at 1387.

[26] The court did not explicate the second prong (burdensomeness) but minimized the burden by restricting the scope of the preservation order. *Id.* at 140-41.

[27] *Cobell v. Norton*, 283 F. Supp. 2d 66, 159-60 (D.D.C. 2003) (discussing failure to prevent destruction of or to take reasonable measures to preserve trust records); *vacated in part*, --F.3d--, 2004 WL 2828059 (D.C. Cir. JanDec. 2108, 2004); *Cobell v. Norton*, 201 F. Supp. 2d 145, 147-48 (D.D.C. 2002) (concerning record transfers and destruction).

> (i) preserve all the documents, data and tangible things in question (including those subject to the above inspection regime); (ii) index all the documents, data and tangible things reasonably anticipated to be subject to discovery in this case, including those subject to the inspection regime, to ensure some baseline by which to gauge defendant's compliance with this order and the effectiveness of the record retention policies adopted by the agencies; and (iii) report immediately any destruction or loss of records.[28]

[II.C.5] The second prong – burdensomeness – is normally a function of the scope of the information sought to be preserved. "Evidence can take many forms in the world today. Considerations such as storage space, maintenance and storage fees, and physical deterioration of the evidence are just a few of the considerations to be evaluated . . . ."[29] If the request is unduly broad, vague or burdensome, the request should ordinarily be denied.[30]

[II.C.6] These two issues dominate the analysis in all courts that anchor the power to order document preservation in Rules 16, 26, 34 or 45, or in the court's inherent power. A different analysis applies when parties seek a preservation order in the form of a temporary restraining order and preliminary injunction under Rule 65. Courts that have anchored their analysis of preservation orders in Rule 65 have required an additional showing that the seeking party will be harmed irreparably without the order[31] and that the order is in the public interest. Some have required a showing of probability of success on the merits. Especially with the emphasis in the proposed new rules upon the court's power and obligation to manage discovery, it seems unnecessary to resort to Rule 65 preliminary injunction law to decide whether to issue a preservation order.

[II.C.7] Judge Kim R. Gibson of the Western District of Pennsylvania recently examined and compared cases grounding preservation orders in Rule 65 with those that base preservation orders in the court's inherent power or the discovery rules. In a thoughtful opinion,[32] District Judge Gibson concluded that two of the four requirements for a preliminary injunction are inapplicable to the

---

[28] *Pueblo of Laguna*, 2004 U.S. Claims LEXIS 49, at60 Fed. Cl. at 1410.

[29] *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 435-46 (W.D. Pa. 2004).

[30] E.g., *In re African-American Slave Descendants' Litig.*, MDL No. 1491, Lead Case No. 02 C 7764, 2003 U.S. Dist. LEXIS 12016 (N.D. Ill. July 14, 2003) (determining that a request for order to preserve all documents related to the "establishment of the company, in past or present form" is too broad).

[31] *E.g., id.* at *9.

[32] *Capricorn Power*, 220 F.R.D. at 429.

decision whether to issue a preservation order. He held that "a probability of success in the litigation is not an appropriate consideration in the determination whether to order preservation of documents" because this requirement is inconsistent with the scope of discovery defined by Rule 26(b)(1).[33] He also held that the Rule 65 "public interest" requirement is inapplicable to discovery between private litigants.[34]

[II.C.8] When a preservation order is requested, the court might encourage the parties to stipulate to the terms of a preservation order[35] since both parties potentially have something to gain from a stipulated order. The requesting party would obtain the obvious advantage of the preserved evidence. The responding party can benefit by clarifying what must be preserved, and receiving judicial approval of what may be destroyed.

[II.C.9] In considering a preservation order, the court ought to seek to minimize the burden imposed upon a party:

> The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Complete cessation of that activity could paralyze a party's operations. *Cf. Manual for Complex Litigation* (4th) § 11.422 ("A blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations.") . . . The parties' discussion should aim toward specific provisions, balancing the need to preserve relevant evidence with the need to continue routine activities critical to ongoing business.[36]

[II.C.10] Any preservation order must be clear and specific so that the ordered party will know how to comply and so that any violation of the order can be sanctioned. Contempt, for example, may be an appropriate remedy for violation of a preservation order only if the order was sufficiently

---

[33] *Id.* at 433.

[34] *Id.*

[35] Committee Note to Proposed Rule 26(f). Indeed, Proposed Rule 26(f) would require the parties "to discuss any issues relating to preserving discoverable information . . . ." Proposed Rules, *supra* note 6, at 8.

[36] Proposed Rules, *supra* note 6, at 18-19.

clear.[37] Clear orders should include: (1) a clear scope of the data subject to the order; and (2) which, if any, platforms or repositories – such as databases, software, computers, other electronic devices – must be preserved and which may be destroyed.

[II.C.11] The proposed new rules would enhance the court's rules-based power to order preservation of electronic information. As amended, Rule 26(f) would direct the parties to negotiate a discovery plan regarding "any issues relating to disclosure or discovery of electronically stored information . . . ."[38] Proposed Rule 16(b)(5) would expressly authorize scheduling orders that include "provisions for disclosure or discovery of electronically stored information."[39] The Committee Note to Proposed Rule 16(b) explains that the "amendment to Rule 16(b) is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation as such discovery is expected to occur."[40]

D. EXPEDITING ELECTRONIC DISCOVERY

[II.D.1] Parties are seeking expedited discovery of electronic data more frequently than they sought expedited discovery of paper documents. This is probably because of the ease and speed with which vast volumes of electronic data can disappear if not safeguarded. It is likely, therefore, that a judge will need to decide whether to order swift preservation or discovery of electronic data. Decisions that will need to be made quickly must balance the risk of the disappearance of volatile information against the risk that a rash order might harm a party by disrupting business or exposing information that is beyond the legitimate scope of discovery.

[II.D.2] Courts plainly have power to expedite electronic discovery. This power has four sources.

[II.D.3] First, the parties may stipulate to such an order, or one party may simply not oppose the order.[41] Both parties potentially have something to gain from a stipulated order, and ought to be encouraged to negotiate the terms of an order expediting discovery. The party seeking discovery obtains the obvious advantage of extracting evidence before it can be destroyed. The party holding the information can benefit by negotiating a clear and narrow scope of what information is subject to expedited discovery.

---

[37] *See, e.g.*, *Landmark Legal Found. v. Envtl.ironmental Protect.ion Agency*, 272 F. Supp. 2d 70, 74-5 (D.D.C. 2003).

[38] Proposed Rules, *supra* note 6, at 8-9.

[39] *Id.* at 2.

[40] *Id.*

[41] *See, e.g.*, *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002).

[II.D.4] Second, the breach of a preservation order may justify expedited discovery.[42]

[II.D.5] Third, various current rules of civil procedure can support this power. Rule 16(c), for example, can support expedited electronic discovery: it provides that the court "may take appropriate action" with respect to "(6) the control and scheduling of discovery," "(12) the need for adopting special procedures for managing potentially difficult or protracted actions" and any "(16) such matters as may facilitate the just, speedy and inexpensive disposition of the action." In addition, "Federal Rules of Civil Procedure 26(d), 30(a), 33(b), 34(b) and 36 give [a] Court the power to adjust the timing requirements imposed under Rule 26(d) and, if warranted, to expedite the time for responding to the discovery sought."[43]

[II.D.6] The essential standard for determining whether to expedite electronic discovery under these rules is whether some showing has been made that expedited discovery is needed to prevent destruction of evidence. This showing is typically made by evidence of actual or attempted destruction of relevant evidence, or by a showing that, by intent or neglect, relevant evidence is likely to be destroyed in the absence of expedited discovery.

[II.D.7] Fourth, the court under Rule 65 may issue a temporary restraining order and preliminary injunction expediting electronic discovery.[44] As discussed above, satisfying the requirements for a temporary restraining order or preliminary injunction (such as the need to show a probability of success on the merits) is more onerous than the showing needed for expediting discovery under Rules 16 and 26.

E. GETTING HELP: APPOINTING SPECIAL MASTERS AND NEUTRAL EXPERTS

[II.E.1] The court has power under Rule 53 of the Federal Rules of Civil Procedure to appoint a special master for electronic discovery and under Rule 706 of the Federal Rules of Evidence to appoint a neutral expert.[45]

[II.E.2] Appointment of a special master or neutral expert for electronic discovery may seem out of the norm, but such appointment merits renewed consideration. Old Rule 53 was adopted in 1912

---

[42] *E.g.*, *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 141 (Fed. Cl. 2004).

[43] *Physicians Interactive v. Lathian Syst. Inc.*, No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868 WL 23018270, at *4 (E.D. Va. Dec. 5, 2003).

[44] *E.g., id.*

[45] Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 FEDERAL COURTS LAW REVIEW 2 (2000), *at* http://www.fclr.org/2000fedctslrev2.htm.

before discovery as we know it was invented[46] and has become "completely outdated."[47] Rule 53 of the Federal Rules of Civil Procedure was substantially amended effective December 1, 2003. Where old Rule 53 discouraged the appointment of special masters[48] and constricted their powers and duties, new Rule 53 "encourages judges to appoint special masters with much broader functions."[49]

[II.E.3] New Rule 53(a) provides:

> (1) Unless a statute provides otherwise, a court may appoint a master only to:
>
> (A) perform duties consented to by the parties;
>
> (B) hold trial proceedings and make or recommend findings of fact on issues to be decided by the court without a jury if appointment is warranted by
>
> (i) some exceptional condition, or
>
> (ii) the need to perform an accounting or resolve a difficult computation of damages; or
>
> (C) address pretrial and post-trial matters that cannot be addressed effectively and timely by an available district judge or magistrate judge of the district.

[II.E.4] Thus, for managing electronic discovery, a court may appoint a master: (A) to perform functions to which the parties have consented, or (B) to make recommended findings of fact on issues that need not be decided by a jury if warranted by some exceptional condition, or (C) to address pretrial discovery that cannot be addressed effectively and timely by the district judge or magistrate judge. In this last circumstance, the appointed individual is often called a "discovery master."[50]

---

[46] *Kilgard*, *supra* note 4, at *Discovery Masters*, 40 Arizona Attorney at 32.

[47] Symposium, *Judge Jack B. Weinstein, Tort Litigation, and the Public Good*, 12 J.L. & POL'Y, 149, 169 (2003) (comments of Judge Shira Scheindlin).

[48] Old Rule 53(b) warned that "reference to a special master shall be the exception and not the rule." Fed. R. Civ. P. 53(b) (before Dec. 1, 2003). *See Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373-M1V, 2003 WL 21468573, at *31-32 (W.D. Tenn. May 13, 2003).

[49] Symposium, *supra* note 46,12 J.L. & POL'Y at 169-70 (comments of Judge Shira Scheindlin).

[50] Kilgard, *supra* note 4, *Discovery Masters*, 40 Arizona Attorney 30.

[II.E.5] The appointee must be neutral.[51] Moreover, "[i]n appointing a master, the court must consider the fairness of imposing the likely expenses on the parties and must protect against unreasonable expense or delay."[52] Civil Rule 53 and Evidence Rule 706 spell out other details of the qualifications and duties of a neutral or special master.

[II.E.6] The new ABA Civil Discovery Standards suggest that experts such as independent information technology consultants, special masters, referees, and other officers or agents of the court may assist with privilege review, and aid or assist the court generally on technical issues.[53]

F. INSPECTING COMPUTERS AND OTHER THINGS

[II.F.1] Most document requests under Rule 34 request that documents be "produced." Such requests invite the producing party to organize and tender paper documents or electronic information. In response to such a request, electronic information is typically copied to a compact disc in native format or converted to Tagged Image File Format (TIFF) or Adobe Acrobat Portable Document Format (PDF), and the disc produced.

[II.F.2] For electronic discovery, litigants are now sometimes requesting, not just "production," but direct access to inspect computers and other electronic devices. Courts are likely to face the question whether direct access is allowed and under what conditions.

[II.F.3] Current Rule 34(a) clearly allows direct access. Not only does Rule 34(a)(1) authorize a request for "production," but also a request that the other party "permit the party making the request . . . to inspect . . . documents (including . . . data compilations. . .) or to inspect and copy, test, or sample . . . tangible things. . . ." Rule 34(a)(2) authorizes requests "to permit entry upon designated land . . . for the purpose of inspection . . . testing, or sampling . . . any designated object or operation thereon. . . ."

[II.F.4] Most cases that have approved direct access have made no distinction between a request for "production" and a request for "inspection." To the extent that inspection has created undue burden or disruption or security issues, courts have simply imposed safeguards under Rule 26(b)(2) or Rule 26(c) to minimize such burdens.

---

[51] Rule 53(a)(2) provides: "(2) A master must not have a relationship to the parties, counsel, action, or court that would require disqualification of a judge under 28 U.S.C. § 455 unless the parties consent with the court's approval to appointment of a particular person after disclosure of any potential grounds for disqualification." FED. R. CIV. P. 53(a)(2). For electronic discovery, this means, for example, that absent informed consent, an agent of an electronic discovery provider retained by one of the parties cannot act as a master for all the parties.

[52] FED. R. CIV. P. 53(a)(3).

[53] Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29) & (32), *supra* note 17.

[II.F.5] The Eleventh Circuit has taken a controversial position on these issues. In *In re Ford Motor Company*,[54] the Eleventh Circuit granted the extraordinary remedy of mandamus to review an order of the Northern District of Alabama allowing plaintiffs to inspect certain databases in Ford's computers. For reasons not apparent in the opinion, the Eleventh Circuit did not address the Rule 34(a)(1) or 34(a)(2) provisions allowing inspection of tangible things, but only the Rule 34(a)(1) provision for production of documents and data compilations. The court held that "Rule 34(a) does not grant unrestricted direct access to a respondent's database compilations. Instead, Rule 34(a) allows a requesting party to inspect and copy the product -- whether a document, disc, or other device -- resulting from the respondent's translation of the data into a reasonably usable form."[55]

[II.F.6] The court then held that Rule 34(a) might allow "some kind of direct access" to inspect computers upon a showing of improper conduct by the document holder: "While some kind of direct access might be permissible in certain cases, this case has not been shown to be one of those cases. Russell is unentitled to this kind of discovery without -- at the outset -- a factual finding of some non-compliance with discovery rules by Ford."[56]

[II.F.7] Proposed Rule 34(a) would strengthen direct access, and probably would overturn *In re Ford Motor Company*. New Rule 34(a)(1) would add language authorizing a requesting party to "test or sample" any "electronically stored information or any designated documents . . . (including . . . data or data compilations in any medium. . . .)"[57] New Rule 34(b) would state: "The request may specify the form in which electronically stored information is to be produced."[58]

[II.F.8] The Committee Note to the proposed changes to Rule 34 reinforces the intent to allow direct access to inspect computers:

> Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly provides that such discovery is permitted. As with any other form of discovery, issues of burden

---

[54] 345 F.3d 1315 (11th Cir. 2003).

[55] *Id.* at 1316-17.

[56] *Id.* at 1317.

[57] Proposed Rules, *supra* note 6, at 24-25.

[58] *Id.* at 26.

and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c).[59]

G. DISCOVERING NEW SOURCES OF ELECTRONIC INFORMATION

[II.G.1] As if understanding desktops, laptops and palmtops were not hard enough, the next generation of electronic discovery issues will be characterized by the novelty and multiplicity of the types, sources and repositories of information.

[II.G.2] The court, the lawyers, and the parties need to become familiar with these sources. The requesting party needs to understand where important information might be found in order to know what to seek and how to request. The producing party likewise needs to know where information might lurk, both to be complete in production and to avoid spoliation penalties and, perchance, to find in its own trove some treasure. The court will need to resolve many new discovery issues driven by a kaleidoscope of emerging technologies.

[II.G.3] A few cases[60] and articles[61] are beginning to discuss these issues. Here are some samples of sources of information beginning to appear in litigation:

- Event data recorders in cars, truck, airplanes and other modes of transportation currently record large amounts of information, and will record more soon.[62]

---

[59] *Id.* at 29.

[60] *E.g.*, *Thompson v. United States Dep't of HUD*, 219 F.R.D. 93, 96 (D. Md. 2003) ("[T]he scope of what is included in the phrase 'electronic records' can be enormous, encompassing voice mail, e-mail, deleted e-mail, data files, program files, back-up files, archival tapes, temporary files, system history files, web site information in textual, graphical or audio format, web site files, cache files, 'cookies' and other electronically stored information.").

[61] David K. Isom, *Electronic Discovery Source Checklist for Plaintiffs and Defendants* (Spring 2004), *at* http://www.isomlaw.com/published-works.asp; Kristin M. Nimsger & Alan E. Brill, *Looking Outside the Box* (Oct. 28, 2002), *at* http://www.law.com/jsp/article.jsp?id=1032128827685; Lesley F. Rosenthal, *Electronic Discovery Can Unearth Treasure Trove of Information or Potential Land Mines*, 75 N.Y. ST. B.A.J. 32 (Sept. 2003), http://www.krollontrack.com/Publications/.

[62] Nat'l Highway Traffic Safety Admin., *Event Data Recorder (EDR) Research History, at* http://www-nrd.nhtsa.dot.gov/edr-site/history.html (last visited Oct. 26, 2004). *See also* Auto Alliance, *Today's Automobile: A Computer on Wheels* (Mar. 22, 2004), *at* http://www.autoalliance.org/archives/000131.html ("The computer technology in today's cars, minivans, SUVs and trucks is nearly one thousand times more powerful than that which guided the Apollo moon mission.").

- Emergency communication systems in cars.[63]
- Internet service providers.[64]
- Voice mail.[65]

[II.G.4] The new ABA Civil Discovery Standards[66] list various types and platforms of data to consider. Though the sources and types of data to consider are expanding, here is a slightly overlapping list to stimulate thinking about the emerging multiplicity: animations; anti-theft systems and databases; archives; audio systems; audiotapes and discs; backup data; blogs; cartridges; cell phone memory; chat rooms; computers; credit cards and records; databases; debit cards and records; deleted information; digital cameras and photographs; discs; drives; email; email attachments; event data recorders (in cars, trucks, ships, planes); external hard drives or "thumb" drives; fax machines; global positioning systems data; graphics; handheld wireless devices; hardware; images; instant messages; internet data; internet service providers; intranets; keyloggers; laptops; legacy data; medical devices and records; memory sticks and flash cards; metadata; mobile telephones; networks; paging devices; personal computers; personal digital assistants; presentation data; printers; radio frequency identification tags or chips (RFIDs); removable discs, including floppy discs; retail purchase card databases; security cameras and other security devices; servers (external and internal); software; spreadsheets; spyware databases; surveillance cameras and devices; tapes; text message databases; toll road cards; videotapes and discs; voicemail; word processing documents.

[II.G.5] Given the welter of potentially responsive information, and the multitude of sources that a party may need to consider, courts will face the issue of responsibility for preserving, finding, and producing information of which a party is ignorant. This is discussed in the spoliation section below.

H. Solving Technological Problems with Technology

[II.H.1] Many of the problems that appear to be created by technology can be solved by technology.

[II.H.2] In paper discovery, process and format questions can usually be reduced to three: where to inspect the paper, how to handle duplicates, and how to manage redactions of privileged or

---

[63] *See Company v. United States*, 349 F.3d 1132 (9th Cir. 2003) (discussing capability of such systems to record and transmit data).

[64] *See United States v. Councilman*, 373 F.3d 197 (11th Cir. 2004), *reh'earing granted*, 385 F.3d 7932004 U.S. App. LEXIS 20756 (1st Cir. Oct.ober 5, 2004).

[65] *See Jasmine Networks, Inc. v. Marvell Semiconductor, Inc.*, 12 Cal. Rptr. 3d 123 (Cal. App. 2004), *review granted and briefing deferred by* 94 P.3d 475 (Cal. Jul 21, 2004).

[66] Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29)(a)(i)&(ii), *supra* note 17.

confidential information. The electronic process and format issues are more diverse, more complicated and, well, more fun.

[II.H.3] Electronic discovery technology is developing faster than the law of electronic discovery. Therefore, most electronic discovery issues presented to a court will outpace prior judicial decisions. If the parties supply competent experts, or if the court appoints a knowledgeable neutral expert or special master, innovative and cost-effective solutions may be possible that otherwise might elude the court and the parties.

[II.H.4] Perhaps the most innovative solutions will be achieved by collaboration among the court and the parties. Judges ought to work with the lawyers to persuade the parties to stipulate regarding production format, process, protocol and other technological issues. The next two sections give examples of possible technological solutions to nettling and expensive electronic discovery problems.

I. RECOVERING DATA FROM BACKUP TAPES

[II.I.1] The rap that electronic discovery is expensive comes primarily from the cases reporting huge actual or estimated costs of recovering data from backup tapes and of privilege review. This section discusses backup tapes, and the next discusses privilege review.

[II.I.2] Counting only the cost of restoring backup data (and excluding attorney and paralegal review time, which in most reported cases is pricier than the restoration process itself), these cases report the following actual or estimated restoration costs:

- *Rowe Entertainment, Inc. v. William Morris Agency, Inc.* -- $9.75 million[67]
- *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.* -- $6.2 million[68]
- *Medtronic Sofamor Danek, Inc. v. Michelson* -- "several million" dollars[69]
- *Wiginton v. CB Richard Ellis, Inc.* -- $249,000[70]

---

[67] No. 98 Civ. 8272, 2002 WL 975713, *9 (S.D.N.Y. May 9, 2002).

[68] No. 99-3514, 2002 WL 246439, at *3 (E.D. La. Feb. 19, 2002). 2 Fed. R. Serv. 3d 1159, 2002 WL 246439, *3 (E.D. La. 2002).

[69] No. 01-2373, 2003 WL 21468573, at *7 (W.D. Tenn. May 13, 2003).

[70] 2004 WL 1895122, at *1 (N.D. Ill. Aug. 9, 2004).

- *Zubulake III* -- $166,000[71]

[II.I.3] The reasons for this level of expense are many.

[II.I.4] One is sheer magnitude. Over three billion business emails, for example, are sent each day in the United States, most of which are archived. One large American company now backs up 45 terabytes (a terabyte is equal to approximately a billion pages) of information daily, which may be typical of large companies.[72]

[II.I.5] Another is redundancy. Most of the information archived each day by traditional backup technology is duplicative. If an individual sends an email to two colleagues with copies to two others within the company then a total of five copies of this one message exist. If each of the four recipients forwards the email to five others, there are now 25 versions of the original message. If the company backs up its data each night, 50 copies will exist the next day. Because traditional backup systems record everything in each computer each backup period (sometimes daily), and not just what is new since the last backup, the emails may be re-copied each night. In three years, a single email will have generated 27,274 clones, all of which are likely to be useless except, perhaps, in litigation in which the archiving process itself is at issue.

[II.I.6] Another reason for high costs is torpor. Because magnetic tape storage is designed for disaster recovery – not for ready, text-searchable access – recovering data is time-consuming and labor-intensive (which explains why the court could say in *Medtronic* that "the quote of approximately $4881 per tape for all professional restoration, searching, and de-duplication services appears reasonable."[73] Traditional recovery requires: re-creation of the original hardware and software ("native environment") in use at the time the data was created and stored; labor-intensive manual intervention; and the costs of equipment capable of storing the same amount of data as the data that is being recovered.

[II.I.7] The cases cited above suggest at least two ways to contain costs: (a) sampling a segment of the data to determine whether the search is cost-effective; (b) narrowing the search either by date or physical location, thereby limiting the amount of data at issue.

[II.I.8] One court has suggested that a corporation may have a duty to use "accessible searchable media, or . . . [to pressure] its software contractors to create such media or software."[74] Such technology is now available – technology that can reduce backup tape restoration costs significantly.

---

[71] 216 F.R.D. 280, 283 (S.D.N.Y 2003).

[72] October 23, 2004 conversation between author and electronic discovery vendor.

[73] *Medtronic*, 2003 WL 21468573, at *11.

[74] *Wiginton*, 2004 WL 1895122, at *8.

For example, one company (RenewData) offers a process that converts non-text-searchable data from tapes to text-searchable disc data without recreating native hardware and software. This significantly reduces the need for manual intervention and the overall costs associated with electronic discovery productions.[75]

[II.I.9] The high costs of electronic discovery arise in part because electronic data stored for one purpose is suddenly requested for another purpose, especially if the specific software designed for the business purpose of the producing party is not be capable of performing the winnowing the requesting party requires. But non-specific approaches to storage and retrieval of data are now being developed that may eventually moot this lack of fit between the producing party's system design and the requesting party's needs.

[II.I.10] In the long run, companies can reduce expenses by initiating non-matter specific planning and proactively storing emails and user files to be used for future litigation. This technology will de-duplicate the emails and user files on the fly, make retrieval and search easier, and significantly lower the cost of electronic discovery of stored data.[76]

J. PROTECTING PRIVILEGE

[II.J.1] The nature and volume of electronic discovery make it likely that old attorney-client privilege issues will need to be examined in a new light.

[II.J.2] The first issue is whether privilege is forfeited by the inadvertent production of privileged information? The enormous volume of electronic information requested and produced in some cases increases the risk of inadvertent disclosure production. The proposed rule change on this issue seeks to reduce the risk, and therefore the cost, of inadvertent production of privileged documents by giving the court and the parties wide latitude in producing documents without waiving privilege.

[II.J.3] The proposed new rules would largely resolve, at least as among the parties,[77] the consequences of inadvertent production of privileged information. Proposed Rule 26(b)(5) would provide:

---

[75] RenewData, *Electronic Evidence and Preservation Archiving*, http://www.renewdata.com (last visited Jan. 13, 2005).

[76] RenewData, *Proactive Preservation Management Whitepaper*, http://www.renewdata.com/fclr (last visited Jan. 13, 2005).

[77] There lingers the problem that the production of otherwise privileged documents pursuant to proposed Rule 26(b)(5)(B), though not a forfeiture or waiver of privilege as between the parties, might constitute a waiver or forfeiture of privilege as to third parties.

> (B) Privileged information produced.
>
> When a party produces information without intending to waive a claim of privilege it may, within a reasonable time, notify any party that received the information of its claim of privilege. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies . . . .[78]

[II.J.4] Proposed Rule 26(f)(4) would require the parties to develop a discovery plan that indicates the parties' views and proposals as to "whether on agreement of the parties, the court should enter an order protecting the right to assert privilege after production of privileged information . . . ."[79] Proposed Rule 16(b)(6) would suggest that the scheduling order might include an "adoption of the parties' agreement for protection against waiving privilege . . . ."[80] The Committee Notes for these changes explain that they are intended "to facilitate discovery by minimizing the risk of waiver of privilege."[81] The Committee Note also reflects the intention to facilitate various pragmatic approaches to privilege review.

[II.J.5] One approach, sometimes called the "quick peek" or "claw back" approach, is that a party would produce information without a prior privilege review. This reduces the initial burden of review for the producing party. The seeking party would review the information for responsiveness before the producing party conducts a privilege review. The parties would stipulate, and the court could order, that no privilege would be waived by this initial production.

[II.J.6] Other innovative ways to reduce privilege review costs, such as use of a neutral expert or reviewer, ought to be considered. The new ABA Civil Discovery Standards suggest various ways to make privilege review of electronic information more effective and less expensive.[82]

[II.J.7] Also, the parties and the court might consider other ways to minimize the roles (and costs) of attorneys in the privilege review process. For example, parties might stipulate, or the court might order, that "performing a key word search for a privilege review rather than examining each document"[83] is desirable and sufficient.

---

[78] Proposed Rules, *supra* note 6, at 7.

[79] *Id.* at 9.

[80] *Id.* at 2.

[81] *Id.* at 3.

[82] Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(32), *supra* note 17.

[83] *Wiginton*, 2004 WL 1895122; *Wiginton v. CB Richard Ellis, Inc.*, No. 02-6832, 2004 WL

(continued...)

[II.J.8] The parties might stipulate and the court might order that "concept search" or "fuzzy search" software[84] might supplement attorney review for privilege. Some studies are suggesting that humans, even lawyers, are not as well-suited as computers to making decisions about which documents are privileged among a large group of documents. Several companies are developing data that suggest that concept search-assisted privilege review can be less expensive, and more accurate and effective, than privilege reviews done only by attorneys.[85]

[II.J.9] Another issue that may continue to merit attention is who pays for privilege review? So far, most courts have required the party asserting privilege to pay the privilege review costs.[86]

K. ALLOCATING THE COST OF ELECTRONIC DISCOVERY

[II.K.1] Under the federal discovery rules, "the presumption is that the responding party must bear the expense of complying with discovery requests, but may invoke the district court's discretion under Rule 26(c) to grant orders protecting [it] from 'undue burden or expense' in doing so, including orders conditioning discovery on the requesting party's payment of the costs of discovery."[87] Rule 26(c) provides that, upon a motion by the party or person from whom discovery is sought, "for good cause shown," the court "may make any order which justice requires to protect a party or person from . . . undue burden or expense . . . ."[88]

---

[83] (...continued)
1895122, at *8 (N.D. Ill. Aug. 9, 2004).

[84] "Concept search" and "fuzzy search" are searches that find information by searching "ideas" rather than exact terms. A large number of concept search engines is commercially available. Though the mathematics behind the technology is complex and in general not publicly available, the idea is that such searches can essentially ignore minor misspellings and can assign words different values that depend upon context. The word "diamond," for example, is treated differently in this process if it is near terms like baseball and Red Sox than if it is near words like carat and bride.

[85] *See, e.g.*, Act Litigation Services, http://www.actlit.com (last visited Jan. 13, 2005).

[86] *E.g., Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373, 2003 WL 21468573, at *8 (W.D. Tenn. May 13, 2003); *Rowe Entertainmen't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. at 421, 432-33 (S.D.N.Y. 2002).

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

[88] Though Rule 26(c) identifies more factors than burdensomeness to be weighed in the scale, this article uses the shorthand "unduly burdensome" to summarize all of the Rule 26(c) factors.

[II.K.2] Who pays for electronic discovery has received extraordinary attention[89] during the last few years, primarily because, in absolute dollars, the cost of electronic discovery has been so high in some reported cases. There are three extant judicial approaches to deciding whether the cost of production ought to be shifted to the requesting party.[90]

[II.K.3] The first is direct application of Rule 26(c). Magistrate Judge Paul W. Grimm, after reviewing the other approaches discussed below, held that the language of Rule 26(b)(2) provided a sufficient guide:

> In addition to the tests fashioned by these courts, it also can be argued with some force that the Rule 26(b)(2) balancing factors are all that is needed to allow a court to reach a fair result when considering the scope of discovery of electronic records. Rule 26(b)(2) requires a court, *sua sponte,* or upon receipt of a Rule 26(c) motion, to evaluate

---

[89] Sedona Conference, *The Sedona Guidelines: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* Sedona Conference Working Group Series 2004) (Sept. 2004), *at* http://www.thesedonaconference.org/publications_html; Am. Bar Ass'n, *Amendments to Civil Discovery Standards*, *supra* note 17.

[90] *Hagemeyer North America, Inc. v. Gateway Data Sciences, Corp Inc.*, 2 F.R.D. 594, 601-02 (E.D. Wisc. 2004), and Stephen D. Williger & Robin M. Wilson, *Negotiating the Minefields of Electronic Discovery*, RICH. J.L. & TECH. 52 (2004), identify four approaches. Two of the three approaches that I believe are vital (the seven-factor test of *Zubulake* and the marginal utility test of *McPeek*) are the same as those in *Hagemeyer* and Williger & Wilson.

The differences are that Judge Rudolph T. Randa in *Hagemeyer* and the Williger & Wilson article credit the approach of *Rowe Entm't*, 205 F.R.D. at 429, which I believe has been eclipsed by *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 316 (S.D.N.Y. 2003) ("*Zubulake IV*"), for the reasons discussed by Judge Randa in *Hagemeyer*.

Also, they credit and then reject an approach that I agree should be rejected. That approach, suggested by Marnie H. Pulver, Note, *Electronic Media Discovery: The Economic Benefit of Pay-Per-View*, 21 CARDOZO L. REV. 1379 (2000), would have distinguished electronic discovery from paper discovery and shifted to the seeking party the cost of discovering computer-generated information. I reject this approach for the same reasons that Judge Randa rejected it: "first, it fails to accommodate documents stored on electronic media that are cheaper to produce than paper-based documents and, second, it ignores the presumption that the requesting party pays the costs of production." *Hagemeyer*, 222 F.R.D. at 601.

Finally, I include an approach not included in *Hagemeyer* or Williger & Wilson: the direct application of the language of Rule 26(c), as illustrated by Judge Grimm's opinion in *Thompson v. United States Dep't of Housing & Urban Dev'p*, 219 F.R.D. 93, 98 (D. Md. 2003).

> the costs and benefits associated with a potentially burdensome discovery request. The rule identifies the following factors to be considered: whether the discovery sought is unreasonably cumulative or duplicative; whether the information sought is obtainable from some other more convenient, less burdensome or inexpensive source; whether the party seeking the information already has had adequate opportunity to obtain the information; and whether the burden or expense of the proposed discovery outweighs its likely benefit, taking into consideration the following: the needs of the case, the amount in controversy, the resources of the parties, the importance of the issues at stake in the litigation and of the discovery sought to the resolution of the issues.[91]

[II.K.4] Judge Grimm's approach is likely to endure. As courts confront rapidly changing technology and unforeseen discovery problems, they ought to feel free to apply basic principles to reach innovative solutions.

[II.K.5] The second approach is that of *Zubulake IV*.[92] There, District Judge Shira Scheindlin weighed seven factors[93] in the following order of importance:

> (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.[94]

---

[91] *Thompson*, 219 F.R.D. at 98.

[92] 217 F.R.D. at 316.

[93] Some confusion surrounds the application of this seven-factor test because Judge Scheindlin held that the test only applies to "inaccessible" documents. This raises two questions. First, does this imply that costs should not be shifted if documents are accessible? *Cf. Wiginton*, 2004 WL 1895122, at *3 n.6. Second, what definition of "inaccessible" should govern this distinction, and why? I discuss the issue of inaccessibility below.

[94] *Zubulake IV*, 217 F.R.D. at 322.

[II.K.6] The third is the "marginal utility" approach of Magistrate Judge John M. Facciola in *McPeek v. Ashcroft*.[95] In *McPeek I,* Judge Facciola weighed the likelihood that a request will unearth critical evidence against the cost of the production: "the more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the [responding party] search at its own expense."[96]

[II.K.7] The new ABA Civil Discovery Standards suggest a list of sixteen factors that the court should consider to decide whether to allow requested discovery and to allocate the costs of that discovery.[97] Counsel and judges should imaginatively consider the factors and approaches that make sense in individual cases, because the law in this area develops only as new factual situations and corresponding analyses occur.

L. MAKING PARTIES RESPONSIBLE FOR ELECTRONIC DISCOVERY: SPOLIATION

[II.L.1] Owners and custodians[98] of information have a duty to preserve[99] information for civil litigation, the breach of which is spoliation. Spoliation cases are much more prevalent in electronic discovery than in paper discovery, perhaps because electronic information is more likely to be destroyed[100] inadvertently than paper and because, whether information is destroyed intentionally or

---

[95] 212 F.R.D. 33 (D.D.C. 2003) ("*McPeek II*"); 202 F.R.D. 31, 34 (D.D.C. 2001) ("*McPeek I*").

[96] *McPeek I*, 202 F.R.D. at 34.

[97] Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29)(b)(iii), *supra* note 17.

[98] The new ABA Civil Discovery Standards state that courts, lawyers and parties should consider the preservation of data in the possession of both a party and a "third person under the control of the party (such as an employee or outside vendor under contract)." Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII (29)(a)(ii), *supra* note 17. It is clear that the duty of a party to preserve documents includes documents in the possession of a third party whom the party controls.

[99] I use "preservation" to refer to the duty to maintain information for specific litigation. "Retention" typically refers to the process of keeping (and destroying) information for historic, proprietary and business reasons other than for specific litigation.

[100] Few spoliation cases examine the extent to which "destroyed" or "deleted" documents might be recovered by forensic examination, either because the parties stipulate that the information at issue is gone, or because there is simply no evidence in the record. Most "deleted" documents can be recovered by forensics unless the disc or drive is melted or otherwise physically destroyed. *See, e.g.*, *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 46 n.8 (D. Conn. 2002); Steven C. Bennett & Thomas M. Niccum, *Two Views from the Data Mountain*, *at* http://www.krollontrack.com/publications/ (last visited Oct. 21, 2004); Sharon D. Nelson & John W. Simek, *Finding and Securing Electronic Evidence* (2002), *at* http://www.senseient.com/ (continued...)

accidentally, the destruction of all copies of electronic information is so much more difficult to accomplish and difficult to hide than with paper. For example, there are more reported spoliation cases in the 10 years from 1994 to 2004 than in the 200 years before.[101] The big issues here are: (1) the sources, and therefore the nature, of the duty; (2) when the preservation duty arises; (3) the degree of intention or culpability required for liability; and (4) the remedies for breach of the duty.

1. Sources of Duty

[II.L.2] These are the principal sources of the duty of parties[102] to preserve documents:

(1) Court's inherent power;[103]

(2) Rules of civil procedure;[104]

(3) Statutes and regulations;[105]

---

[100] (...continued)
default.asp?page=publications/article13.htm. "In identifying electronic data that parties may be called upon, in appropriate circumstances, to preserve or produce, counsel, parties and courts should consider . . . [w]hether potentially producible electronic data may include data that have been deleted but can be restored." Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29)(a)(iii), *supra* note 17.

[101] Lexis' "Federal & State, Combined" library contains more spoliation cases (search: "spoliation w/ 10 [document or data or paper or information]") during the 10 years from January 1, 1994 through January 1, 2004 (195) than during the 200 years before January 1994 (155).

[102] Additional duties for lawyers are based in ethical rules and in Rule 11 of the Federal Rules of Civil Procedure.

[103] *E.g.*, *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *103 (N.D. Ill. October. 247, 2003) ("Courts have the inherent power to impose sanctions for abuse of the judicial system, including the failure to preserve or produce documents."); *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001) ("The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation . . . .").

[104] *E.g.*, *Landmark Legal Found. v. Environmental. Prot.ection Agency*, 272 SF. Supp. 2d 70, 74-75 (D.D.C. 2003) (analyzing Rule 65(d) contempt power); *Wiginton*, 2003 WL 22439865, at *3 n.5 (Rule 37 sanctions for destroying evidence contrary to a prior court order).

[105] *E.g.*, 18 U.S.C. § 1512(c) ("Whoever corruptly -- (1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding . . . shall be fined under this title or imprisoned not (continued...)

(4) Tort law.

2. When the Duty Arises

[II.L.3] The duty to preserve can arise before the action begins. The leading view is that the duty arises "when a party reasonably should know that the evidence may be relevant to anticipated litigation."[106]

3. Degree of Culpability

[II.L.4] *Residential Funding Corp. v. DeGeorge Corp.*[107] is the leading case. There, the Second Circuit held that sanctions for failure to produce requested e-mails would be justified by conduct that is intentional or willful, grossly negligent or simply negligent, including "purposeful sluggishness." "District courts should not countenance 'purposeful sluggishness' in discovery on the part of parties or attorneys and should be prepared to impose sanctions when they encounter it."[108] The degree of culpability impacts the extent to which the claimant must prove the relevance of the destroyed data and the gravity of the remedy appropriate for the spoliation.[109]

4. Remedies for Spoliation

[II.L.5] Sanctions for spoliation typically fall into four categories, depending upon the degree of culpability and the extent of the impact of the spoliation upon the opposing party: (1) default judgment against the spoliator; (2) adverse evidentiary inferences against the spoliator; (3) contempt; and (4) monetary fines or sanctions, including forcing the spoliator to pay the damages, including attorney fees, caused by the spoliation.[110]

---

[105] (...continued)
more than 20 years, or both.").

[106] *Silvestri v. General Motors Corp.*, 271 F.3d at 591.

[107] 306 F.3d 99 (2d Cir. 2002).

[108] *Id.* at 113.

[109] *Thompson v. U.S. Dep't of HUD*, 219 F.R.D. 93 (D. Md. 2003); *Zubulake v. USBS Warburg LLC*, No. 02- Civ 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) ("*Zubulake V*").

[110] *See, e.g.*, *Advantacare Health Partners, LP v. Access IV*, C 03-04496, 2004 WL 1837997, at *4, *11-12 (N.D. Cal. Aug.ust 17, 2004); *Metro. Opera Ass'n Inc. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union*, 212 F.R.D. 178, 219 (S.D.N.Y. 2003), *aff'd on motion for reconsideration*, 2004 WL 1943099 (Aug. 27, 2004).

M. DEFINING LAWYERS' RESPONSIBILITIES FOR ELECTRONIC DISCOVERY

[II.M.1] Preserving, gathering and producing responsive electronic data is much trickier and riskier than paper discovery. Because the rules do not clearly allocate between the party and the lawyer the responsibility for assuring complete production of documents, courts must allocate that duty, and sanctions for breaching that duty, between the lawyer and the client.[111] The current rules require that the "party" must serve the response to the Rule 34 request and that the attorney for a represented party shall sign the response. The Advisory Committee Notes to the 1983 Amendments to Rule 26(g) clarify that the current rules do not require either the lawyer or the party to warrant completeness of production: "Rule 26(g) does not require the signing attorney to certify the truthfulness of the client's factual responses to a discovery request. Rather, the [lawyer's] signature [on the Rule 34 response] certifies that the lawyer has made a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand."

---

[111] The power to sanction lawyers who fail their document production duties has been grounded, not in Rule 34, but in three other sources. For example, in sanctioning lawyers for production failures in *Metropolitan Opera*, Judge Loretta Preska adduced three other bases for the duty to produce documents.

First, she found such a duty in the Rule 26(g)(2) mandate that the signature on a Rule 34 response constitutes a certification that the response is "consistent with [the Federal Rules] and warranted by existing law or a good faith argument . . . .; (B) not interposed for any improper purpose . . . ; and (C) not unreasonable or unduly burdensome." *Metro. Opera*, 212 F.R.D. at 218-19.

Next, Judge Preska adduced 28 U.S.C. § 1927, which provides that:

> any attorney or other person admitted to conduct cases in any court of the United States . . . who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct.

Id. at 220.

Finally, Judge Preska relied upon the "inherent" or "implied" power of a court to manage its own affairs. *Id.*

[II.M.2] Given the failure of the federal rules[112] to allocate document production responsibility, courts are forced to develop law allocating this responsibility. The section above on spoliation summarizes the duties of parties in relation to producing documents. This section focuses on the duties of lawyers.

[II.M.3] The principle guiding the allocation of the preservation duty ought to be: in the whole process of producing information, who, as between the lawyer and party, has the ability to assure that proper steps are taken to preserve what ought to be disclosed and produced? If the lawyer, for example, is unimpeachably diligent in advising the client and setting up a procedure to preserve, disclose and produce responsive documents, while the client takes a casual or ineffective approach, failing to protect data sources, failing to search it out, hiding information or denying its existence or availability, the client ought to bear responsibility for spoliation sanctions. Two recent notable cases, however, have placed much of the responsibility upon the lawyers, on the ground that lawyers know better than the client what must be preserved, protected, disclosed and produced and are best situated to assure compliance with those duties:

- *Metro. Opera Ass'n v. Local 100, Hotel Employees and Restaurant Employees Int'l Union*;[113]

---

[112] Some courts have developed local rules that define lawyer duties for managing document production and assuring completeness. The rules of the United States District Court for the District of New Jersey, for example, provide:

> Prior to a Fed. R. Civ. P. 26(f) conference, counsel shall review with the client the client's information management systems including computer-based and other digital systems, in order to understand how information is stored and how it can be retrieved. To determine what must be disclosed pursuant to Fed. R. Civ. P. 26(a) (1), counsel shall further review with the client the client's information files, including currently maintained computer files as well as historical, archival, back-up, and legacy computer files, whether in current or historic media or formats, such as digital evidence which may be used to support claims or defenses. Counsel shall also identify a person or persons with knowledge about the client's information management systems, including computer-based and other digital systems, with the ability to facilitate, through counsel, reasonably anticipated discovery.

Local Civil and Criminal Rules of the United States District Court for the District of New Jersey, Local Civil Rule 26.1(d)(1), *at* http://www.kenwithers.com/rulemaking/index.html (last visited Jan. 13, 2005).

[113] 212 F.R.D. 178 (S.D.N.Y. 2003).

- *Zubulake v. USB Warburg LLC;*[114]

[II.M.4] Taken together, these cases place the following duties upon lawyers once they are retained for a matter:

– To define for the client what information must be preserved[115] and produced. This duty includes sending to the client the document requests, and more: it requires defining what material may be withheld on claims of privilege, and translating into simple, non-legal language precisely what information is now subject to the judicial process. It is not enough, for example, in response to a document request from Metropolitan Opera, simply to instruct the client to produce all "Met-related" documents.

– To create a "litigation hold" that stops the destruction of information that may need to be disclosed or produced. This includes sending a clearly stated email or other written communication to all persons who may have control or custody of requested information, and more: "The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees."[116] "A party's discovery obligations do not end with the implementation of a 'litigation hold' -- to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."[117]

– To assure that responsive data is preserved in all of its formats, including paper and electronic data. This includes not only active files, but backup tapes and other archived data. It also includes the duty to become aware of the vast possible sources where responsive data may be found in a company, such as email, servers, internet service providers, digital printers, voice mail and other sources.

---

[114] *Zubulake V*, 2004 WL 1620866, at *9 (S.D.N.Y. July 20, 2004) ("A lawyer cannot be obliged to monitor her client like a parent watching a child. At some point, the client must bear responsibility for a failure to preserve. At the same time, counsel is more conscious of the contours of the preservation obligation; a party cannot reasonably be trusted to receive the "litigation hold" instruction once and to fully comply with it without the active supervision of counsel.").

[115] The new ABA Discovery Standards concur: "When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences of failing to do so." Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § IV(10), *supra* note 17.

[116] *Zubulake V*, 2004 WL 1620866, at *9.

[117] *Id.* at *7.

– To be familiar with the client's document and data retention policies and practices so that those policies and practices can be interrupted, monitored and controlled.

– To capture responsive data created before the lawsuit started and during the litigation.

– To understand the client's computer systems and "retention architecture." "This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy."[118]

– To communicate – preferably in face-to-face interviews – with key players to find out the idiosyncrasies of how documents and data were actually created, managed, destroyed, and preserved, as opposed to what the company's policies and manuals may have specified.

– To negotiate with opposing counsel to try to clarify, simplify and narrow what information must be retained. These parameters might be defined by source, search terms, date range, key players, type of document or other parameters.

– To educate each lawyer who works on the case, and especially each lawyer specifically responsible for preservation, disclosure and production duties, about the detailed history of the information management effort.

– To follow through with the client to assure that all documents and data that the lawyer requests are in fact preserved, gathered, disclosed, and produced.

– To keep a detailed record of preservation, disclosure, and production efforts to evidence those efforts with admissible facts if challenged.

N. BALANCING SECRECY AND ACCESS TO ELECTRONIC DISCOVERY: THE IMPACT OF ELECTRONIC FILING AND ELECTRONIC ACCESS

[II.N.1] Parties to civil litigation often have important and understandable interests – privacy, trade secrets, confidentiality and privilege – in keeping their dispute secret. Protective orders have almost become routine. These orders often provide that information exchanged will be used only for litigation purposes, protected through the litigation, and destroyed or returned at the end of litigation. Most orders restrict dissemination to attorneys and parties, but some restrict access to outside litigation counsel and approved experts, denying access to parties and in-house counsel. Parties negotiating these orders are focused on their respective interests. Beyond the parties, the public and the press have important – and, in some respects, constitutional – interests in knowing about civil

[118] *Id.* at *8.

litigation. Balancing these interests has created a jurisprudence that allows only one abstraction: protective orders blocking access to court proceedings should not be entered autonomically.[119]

[II.N.5] Under Rule 26(c), a protective order requires "good cause." This means that a court's analysis of whether to enter a protective order sealing or otherwise blocking public access to discovery filed with the court[120] must not stop with the simple fact that the parties have requested or stipulated to such an order.[121] Rather, the court must balance competing interests of secrecy and access.

[II.N.6] The advent of electronic filing and electronic access to court records impacts the secrecy/access balance. As more court records become available electronically, the old "practical obscurity" of paper documents buried in musty archives – where only the parties or, in rare cases, the press, would find them – will disappear.[122] How to balance these competing interests has received increasing attention.[123] With electronic data, both sides of the balance are heavier. Litigants will be even more reluctant to file information that they know may become instantly accessible and distributable throughout the world. The press, the public and information vendors will also find the information more valuable and useful. Courts will be asked to be the arbiters of these intense competing interests.[124] In short, courts must consider numerous competing interests before entering

---

[119] *See generally* Laurie Kratky Dore, *Settlement, Secrecy and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements*, 55 S.C. L. REV. 791 (2004); Laurie Kratky Dore, *Secrecy by Consent: The Use and Limits of Confidentiality in the Pursuit of Settlement*, 74 NOTRE DAME L. REV. 283 (1999).

[120] In general, discovered information is not filed with the court until it is used to support a motion or as evidence at trial. Until discovery is filed, there is normally no public right of access to the information. *E.g.*, *Baxter Int'l v. Abbott Lab.*, 297 F.3d 544, 545 (7th Cir. 2002).

[121] *See, e.g.*, *Chicago Tribune Co. v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304 (11th Cir. 2001); *Citizens First Nat'lional Bank v. Cincinnati Ins.urance Co.*, 178 F.3d 943 (7th Cir. 1999).

[122] *See generally United States Dep't of Justice v. Reporters Comm.ittee for Freedom of the Press*, 489 U.S. 749 (1989).

[123] For example, The Sedona Conference has created a working group (Working Group 2) that is analyzing these issues and plans in 2005 to recommend "principles and best practices addressing protective orders, confidentiality issues, and motions to vacate or modify to permit public access." *See* The Sedona Conference, Working Group Series, http://www.thesedonaconference.org/wgs (last visited Jan. 14, 2005). The author is a member of this working group. The views expressed here are those of the author and not necessarily those of the working group or any of its members.

[124] George F. Carpinello, *Public Access to Court Records in New York: The Experience Under Uniform Rule 216.1 and the Rule's Future in a World of Electronic Filing*, 66 ALB. L. REV. 1089, (continued...)

protective orders sealing or redacting or otherwise preventing access to electronic discovery that has been filed with the court or entered into evidence.

O. UNDERSTANDING METADATA

[II.O.1] Metadata will present many issues to courts that have not yet been decided.

[II.O.2] All electronic files, including websites, email messages, spreadsheets, and word processing documents, contain metadata ("meta" – about or behind or beyond; "data" – things or information). For example, Microsoft Word, Access, Excel and PowerPoint documents contain a variety of information that remains hidden and unknown (or, at least, unseen) to the typical creator or recipient of the document,[125] but the data can be revealed in various ways, including using the "properties" and "track changes" functions or reading the document with commercially available software designed for that purpose.[126]

[II.O.3] Metadata is typically described as "data about the data" or "data beyond the obvious data." That is, metadata refers to the normally hidden data contained within an electronic document or data file. Examples of metadata for a word processor document are the date the file was last modified, or the identification of the printer on which the document was last printed. The legal issues surrounding metadata can only become focused if the boundary between data and metadata is defined.

[II.O.4] The most common boundary is the distinction between that portion of the data that appears on paper when a document is printed ("data") from that which does not ("metadata"). But other definitions are implicit in many discussions of metadata. For example, in some discussions of metadata, the distinction between data and metadata is whether the creator of the document was aware of the data at some point—if not, then the data is deemed metadata. The Committee Note to Proposed Rule 26(f) states: "Information describing the history, tracking, or management of an electronic document (sometimes called 'metadata') is usually not apparent to the reader viewing a hard copy or a screen image."[127] This distinction underlies many of the horror stories of people revealing embarrassing information unwittingly.

---

[124] (...continued)
1123 (2003).

[125] David A. Karp, *Revealing Codes*, PC MAGAZINE (June 8, 2004), *at* http://www.pcmag.com/article2/0,1759,1585411,00.asp.

[126] *See* metadatarisk.org: The Definitive Source for Content Security, *at* http://metadatarisk.org/faq/faq_overview.htm (last visited Jan. 14, 2005).

[127] Proposed Rules, *supra* note 6, at 20.

[II.O.5] The new ABA Civil Discovery Standards contain this description of metadata: "A party requesting information in electronic form should also consider . . . [a]sking for the production of metadata associated with the responsive data — i.e., ancillary electronic information that relates to responsive electronic data, such as information that would indicate whether and when the responsive electronic data was created, edited, sent, received and/or opened."[128]

[II.O.6] Courts will face numerous issues relating to metadata, including the following.

[II.O.7] Ought metadata to be categorically less (or more) discoverable than data? Some have argued that metadata ought to be less readily discoverable than other data,[129] but there appears to be no legal or practical support for this assertion. Others have recognized that the removal of metadata (by producing only paper or converting a native file to a .tiff or .pdf image, for example) might constitute spoliation.[130]

[II.O.8] Proposed Rule 26(f)(3) would require the parties to discuss "the form in which [electronically stored information] should be produced . . . ." Given the complexity and variety of issues surrounding metadata, the court ought to discuss format and metadata issues in the Rule 16 conference.[131] The Committee Note to Rule 26(f) says that "whether [metadata] should be produced may be among the topics discussed in the Rule 26(f) conference."[132]

[II.O.9] In the absence of a stipulation or order, Proposed Rule 34(b) would allow the requesting party to choose the format of production (knowledgeable seekers will know or can find out which format will maximize metadata if the metadata might be useful).[133] The responding party may object

---

[128] Am. Bar Ass'n, *Amendments to Civil Discovery Standards* § VIII(29)(b)(ii)(B), *supra* note 17.

[129] For example, Sedona Principle 12 states: "Unless the producing party knows the particular metadata is material to the resolution of a dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court." Sedona Conference, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (Jan. 2004) 41-43, *at* http://www.thesedonaconference.org/publications_html.

[130] Dennis Kennedy & George Socha, *Muddling Through the Metadata Morass* (May 2004), *at* http://www.discoveryresources.org/04_om_electronic_discoverers_0405.html.

[131] Proposed Rule 16(b)(5), *supra* note 6, at 2, urges the court to enter a scheduling order that specifies "provisions for disclosure or discovery ~~or disclosure~~ of electronically stored information . . . ." Proposed Rule 34(b), *supra* note 6, at 27, then gives the parties options for production format, "unless the court otherwise orders," suggesting again that the court manage these issues.

[132] Proposed Rules, *supra* note 6, at 20.

[133] "The request may specify the form in which electronically stored information is to be produced."
(continued...)

to the requested format.[134] If the seeker does not specify a production format, and there is no agreement or order regarding format, the producing party would have the option under Proposed Rule 34(b) to produce electronic information "in a form in which it is ordinarily maintained, or in an electronically searchable form. The party need only produce such information in one form."[135] This might allow a producing party to convert data to a format that would destroy or eliminate some metadata, but this result may be limited by a good faith requirement.

[II.O.10] Whether information is classified as metadata is typically irrelevant to its discoverability. Traditional discoverability tests, such as relevance to claims and defenses, should govern discoverability of metadata. For example, in a forgery case in which a party claims that the data that a document bears is false, the date on which the document was created might be the most important information to be discovered. Metadata that show a discrepancy between the date typed on the document and the date that the computer shows the document was created might be dispositive.

[II.O.11] A related issue is whether metadata ought to be more or less readily discoverable because the creator of a document was unaware that she was creating metadata or did not intend to create the metadata. In some cases, such information might be probative exactly because it is created unwittingly. For example, metadata "may be more valuable in building or defending a case as it is often not consciously created by a user and is less vulnerable to manipulation after the fact."[136]

P. SELECTING PRODUCTION FORMATS

[II.P.1] The format in which electronic information is produced in the action requires real thought. Format will have a bearing on other issues discussed elsewhere in this article, including whether to seek production of data or inspection of computers, what metadata will be included, and what production protocol is indicated. This section focuses on what the proposed new rules say about production format and then discusses issues that may arise in connection with certain formats.

[II.P.2] The proposed new rules envision a four-step process by which production format may be determined.

[II.P.3] First, the Proposed Rules encourage an agreement of the parties or court order specifying format. Proposed Rule 26(f)(3) would require counsel and the parties early in the action to discuss and develop a discovery plan about "any issues relating to disclosure or discovery of electronically

---

[133] (...continued)
Proposed Rule 34(b), *supra* note 6, at 26.

[134] *Id.*

[135] *Id.* at 27.

[136] Michael R. Arkfeld, ELECTRONIC DISCOVERY AND EVIDENCE 1-5 (2003).

stored information, including the form in which it should be produced."[137] Proposed Rule 16(b)(5) would provide that the scheduling order may include "provisions for disclosure or discovery of electronically stored information."[138]

[II.P.4] Second, the proposed rules invite the requesting party to specify the format of production. "The request may specify the form in which electronically stored information is to be produced."[139]

[II.P.5] Third, the proposed rules create a default for determining format if no format is specified in the document request. Proposed Rule 34(b)(ii) would provide that, in the absence of a format specified in the request, and in the absence of a contrary order or agreement, "if a request for electronically stored information does not specify the form of production, a responding party must produce the information in a form in which it is ordinarily maintained, or in an electronically searchable form. The party need only produce such information in one form."[140]

[II.P.6] Fourth, Proposed Rule 34(b) would authorize the responding party to object "to the requested form for producing electronically stored information, stating ~~in which event~~ the reasons for the objection ~~shall be stated~~."[141]

[II.P.7] Proposed Rule 45 has similar provisions relating to the format in which subpoenaed electronic information is to be produced.

[II.P.8] If the production format requires use of proprietary hardware or software, or passwords or encryption keys, these issues arise.

[II.P.9] Must the producing party provide the hardware, software, passwords or encryption keys needed to access the information? Subject to the considerations discussed in the next paragraph, the answer is clearly yes. Proposed Rule 34(a) (like current Rule 34(a)) would authorize the requesting party to request production and inspection of "any designated electronically stored information … and other data and data compilations in any medium from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form…."

[II.P.10] Even if the necessary software (or hardware) is proprietary, production should normally be required. If the producing party owns the proprietary interest, that interest can typically be

---

[137] Proposed Rules, *supra* note 6, at 9.

[138] *Id.* at 2.

[139] Proposed Rule 34(b), *supra* note 6, at 26.

[140] Proposed Rule 34(b)(ii), *supra* note 6, at 27.

[141] Proposed Rules, *supra* note 6, at 26.

protected by a protective order.[142] If the proprietary interest is owned by a third party, the producing party might assert a contractual restriction against using the proprietary software for litigation. Such a claim is unlikely to stand, either because the contract does not in fact prevent using a limited use for litigation, or because, if it did, the contract would be void as against public policy. In any event, a court order would trump a contract purporting to prevent use of software for litigation.[143]

Q. PRESCRIBING PRODUCTION PROTOCOLS

[II.Q.1] Courts managing electronic discovery will often need to prescribe protocols for the discovery process or to approve parties' stipulated protocols, especially if a party is allowed to inspect another party's computers. In general, proper production and inspection protocols must assure the following:

> That evidence is not destroyed or altered by the discovery process. In *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*,[144] Gates' expert destroyed 7-8% of the data on Bando's computer by copying data onto a hard drive without first creating a mirror image of the data. Though mirroring hard drives was an available, superior technology, it had been used rarely by the late 1990s. Still, the court held that Gates had a duty "to utilize the best technology available" for electronic discovery.
>
> That irrelevant, privileged, confidential and private[145] information is protected.[146]
>
> 1. That the process establishes chain of custody and preserves authenticity.

---

[142] *E.g.*, *In re Honeywell Int'ernational, Inc. Sec.urities Litig.*, No. M8-85, 2003 WL 22722961, at *2 n.1 (S.D.N.Y. Nov. 18, 2003); *In re Livent, Inc. Noteholders Sec. Litig.,* No. 98- Civ 7161, 2003 WL 23254, at *1-2 (S.D.N.Y. Jan. 2, 2003).

[143] The problem might also be solved by the payment by the producing party of a license fee. If so, whether that cost should be shifted to the requesting party could be analyzed under the cost-shifting tests discussed above.

[144] 167 F.R.D. 90, 112-13 (D. Colo. 1996).

[145] Of course, confidential and private information may be discoverable, but may need to be confined to the litigation by a protective order.

[146] *E.g.*, *Playboy Enterprises., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999).

2. That the burden upon the producing party is reasonably minimized.[147]

3. That the process is efficient and cost-effective.

[II.Q.2] Though the details of protocols will need to be tailored for each case, these cited cases provide thoughtful and fact-rich sources of protocols that have gone before.

R. NAVIGATING THE SAFE HARBOR

[II.R.3] The proposed new rules would add as Rule 37(f) the following provision, characterized in the committee notes as a "safe harbor":

> Unless a party violated an order in the action requiring it to preserve electronically stored information, a court may not impose sanctions under these rules on the party for failing to provide such informationif:
>
> (1) the party took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action: and
>
> (2) the failure resulted from loss of the information because of the routine operation of the party's electronic information system.[148]

[II.R.4] This section, if adopted, will pose numerous questions for courts to resolve.

[II.R.5] The main question will be: Is this a big deal or a little deal? Critics worry that it will be a big deal – that it will insulate parties from real responsibility to produce documents critical to civil litigation. On its face, the rule seems to provide some protection for a party who fails to produce relevant, requested information if the party took reasonable steps to preserve the information but lost the information through routine computer operations.

[II.R.6] The gist of the committee notes is that this rule should not be a big deal. The notes emphasize that this rule applies only to electronic information, and only to information lost to "routine operation of the party's electronic information system." The notes also point out that there is no safe

---

[147] *E.g.*, *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 653-54 (D. Minn. 2002); *Simon Prop. Group, L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000).

[148] Proposed Rules, *supra* note 6, at 31-32.

harbor here for a party that fails to take reasonable steps to preserve evidence. Also, no violation of a preservation order is protected.[149]

[II.R.7] Further analysis suggests that the proposed safe harbor might be narrow indeed, depending how the phrase "sanctions under these rules" is interpreted. That is, Proposed Rule 37(f) only protects against "sanctions under these rules," and not sanctions grounded in other sources. This suggests that the safe harbor is not intended to protect parties (or lawyers) from spoliation sanctions grounded in the other three sources of sanctions discussed above – namely, statutes, tort or a court's inherent power.

[II.R.8] The Committee Notes to Proposed Rule 37(f) clarify that the proposed safe harbor does not preclude statute-based or regulation-based penalties for spoliation: "Whether or not Rule 37(f) is satisfied, violation of such a statutory or regulatory requirement for preservation may subject the violator to sanctions in another proceeding--either administrative or judicial--but the court may not impose sanctions in the action if it concludes that the party's steps satisfy Rule 37(f)(1)."[150]

[II.R.9] It also seems clear that tort liability for spoliation is not a sanction "under these rules" excused by this rule: "Rule 37(f) addresses only sanctions under the Civil Rules and applies only to the loss of electronically stored information after commencement of the action in which discovery is sought. It does not define the scope of a duty to preserve and does not address the loss of electronically stored information that may occur before an action is commenced."[151]

[II.R.10] Whether the safe harbor would prevent sanctions arising from a court's inherent power might be knottier. Inherent power, however, normally is defined as power needed for the proper exercise of judicial power where no rule (or statute or other substantive law) otherwise creates the power. A restriction of "sanctions under these rules" should therefore not abridge inherent powers that exist outside of the rules.

[II.R.11] All this taken together would seem to mean that Proposed Rule 37(f) is intended to insulate a party only from sanctions under Rule 37(b)(2). This rule, however, only provides sanctions for the failure "to obey an order to provide or permit discovery . . . ." But here's the rub:

> – There are therefore no rules-based sanctions for failure to produce documents in the absence of a court order;[152] and

---

[149] *Id.* at 33-34.

[150] *Id.* at 35-36.

[151] *Id.* at 34.

[152] Sanctions under Rule 11(c) are limited to situations in which Rule 11(b) has been violated, *i.e.*, (continued...)

– Proposed Rule 37(f) does not harbor a party from sanctions for failure to produce documents that a court has ordered produced.

[II.R.12] That is, if the court has already entered an order preventing destruction of evidence, proposed Rule 37(f), by its own terms, does not apply. If, on the other hand, the court has not already entered a document preservation order, no rules-based sanctions are available to be inoculated against by Rule 37(f).

S. ADDING PROTECTION FOR INACCESSIBLE DOCUMENTS

[II.S.1] The proposed new federal rules would add the following to Rule 26(b)(2):

> A party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible. On motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause and may specify terms and conditions for such discovery.[153]

[II.S.2] If this proposed rule is adopted,[154] courts will have to resolve several thorny issues created by the rule:

---

[152] (...continued)
"a pleading, written motion, or other paper" that did not meet the Rule's standards has been "present[ed] to the court." FED. R. CIV. P. 11(b), 11(c). A simple failure to produce documents or otherwise respond to a discovery request does not come within Rule 11's proscriptions. Moreover, Rule 11(d) specifically exempts "disclosures and discovery requests, responses, objections, and motions that are subject to the provisions of Rules 26 through 37" from Rule 11 coverage. FED. R. CIV. P. 11(d); *Patelco Credit Union v. Sahni*, 262 F.3d 897, 913 n.15 (9th Cir. 2001); *Avent v. Solfaro*, 223 F.R.D. 184, 187-88 (S.D.N.Y. 2004).

Likewise, although Rule 26 is a source for determining the discovery duties of the parties, it cannot properly be considered as a source of the court's authority to impose sanctions. That authority resides in Rule 37. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 49 n.13 (1991) ("The Notes to Rule 26(g) . . . point out that the rule 'makes explicit the authority judges now have to impose appropriate sanctions and requires them to use it. This authority derives from Rule 37, 28 U. S.C. § 1927, and the court's inherent power.'").

[153] Proposed Rule 26(b)(2), *supra* note 6, at 6.

[154] Significant criticism is emerging about this proposal, which may signal that this proposed rule will not be adopted as proposed.

– A cardinal rule of construction is that new language in a rule or statute ought to be interpreted to effect some sort of change. Without this new language, a party requested to produce documents is already protected by current Rule 26(b)(2) from having to produce documents that are unduly burdensome. Does this proposed new language mean, then, that a party need not produce "inaccessible" data even though the production is not unduly burdensome (because if it were unduly burdensome, the rules would already provide protection)?

– What is the definition of "not reasonably accessible"? The Committee Note to this proposed rule suggests that the answer will depend upon a variety of circumstances, such as whether the owner of the information routinely uses or accesses the information, the purpose for which the information has been retained, whether the data are searchable, whether the holder has the hardware and software needed to recover the data, and whether the information has been deleted or has otherwise become expensive or difficult to recover.

T. SUPERVISING SUBPOENAS AND THIRD PARTY ELECTRONIC DISCOVERY

[II.T.1] The proposed rules would apply essentially the same changes to Rule 45 subpoenas for electronic discovery to nonparties as to Rule 34 requests to parties. For example, "electronically stored information" may be subpoenaed for production, inspection, sampling or testing.[155] The subpoena may specify production format,[156] but, if not, the nonparty must produce "the information in a form in which the person ordinarily maintains it, or in an electronically searchable form."[157] Protection of nonparties relating to inaccessible documents[158] and privilege forfeiture for inadvertent production[159] is nearly identical to the protection for parties.

[II.T.2] The proposed new rules on electronic discovery appear not to have changed the procedure and burdens relating to the cost of discovery that exist in current Rule 45. The principal difference between electronic discovery from third parties – as compared to electronic discovery from parties – is that third parties enjoy more protection from burdensome and costly discovery than do parties. For example, though a third party in some instances[160] must pay all[161] or part[162] of the discovery costs,

---

[155] Proposed Rule 45(a)(1)(c), *supra* note 6, at 37.

[156] Proposed Rule 45(a)(1), *supra* note 6, at 38.

[157] Proposed Rule 45(d)(1)(B), *supra* note 6, at 47.

[158] Proposed Rule 45(d)(1)(C), *supra* note 6, at 47-48.

[159] Proposed Rule 45(d)(2)(B), *supra* note 6, at 48-49.

[160] Several cases have adopted a three-part test to decide whether the third party must pay the discovery costs: "whether the nonparty actually has an interest in the outcome of the case, whether
(continued...)

Rule 45 requires that a "party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena."[163] The "expense" for producing documents may include attorney fees for reviewing the subpoenaed documents, including privilege review.[164]

[II.T.3] The law of third-party electronic discovery is beginning to develop.[165]

U. LEARNING MORE: ELECTRONIC DISCOVERY RESOURCES

[II.U.1] Because technology is moving faster than law, legal precedent on electronic discovery lags behind the technology. The whole process of learning about electronic discovery must therefore be different than the ways we used to learn about paper discovery.

[II.U.2] While paper books are still invaluable, book learning must be honed by learning from electronic sources. Here are some of the best books and electronic resources.

III. BOOKS

Michael R. Arkfeld, *Electronic Discovery and Evidence* (2003): strong combination of law and technology by one of the most experienced lawyers in the field.

Adam I. Cohen & David J. Lender, *Electronic Discovery: Law and Practice* (2003): excellent survey of electronic discovery law and practice.

---

[160] (...continued)
the nonparty can more readily bear the costs than the requesting party and whether the litigation is of public importance." *E.g.*, *FTC v. U.S. Grant Res., LLC*, No. 04-596, 2004 WL 1396315, at *4 (E.D. La. June 18, 2004) (quoting *In re Exxon Valdez*, 142 F.R.D. 380, 383 (D.D.C. 1992)).

[161] *E.g.*, *In re Honeywell Int'l, Inc. Sec. Litig.*, No. M8-85, 2003 WL 22722961 (S.D.N.Y. Nov. 18, 2003).

[162] *E.g.*, *Linder v. Adolfo Calero-Portocarrero*, 251 F.3d 178 , 179-80, 182-83 (D.C. Cir. 2001) (discussing district court's requirement that subpoenaed party pay half of the discovery costs).

[163] Fed. R. Civ. P. 45(c)(1).

[164] *E.g.*, *In re Appplication of the Law Firms of McCourts & McGrigor Donald*, No. M19-96, 2000 WL 345233, at *3 (S.D.N.Y. Nov. 19, 2001).

[165] *E.g.*, *In re Honeywell Int'l*, 2003 WL 227229611 (resolving motion to compel subpoenaed electronic documents); *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 20043), *cert. denied*, 125 S. Ct. 48 (2004) (noting that overbroad subpoena for electronic discovery may violate the Stored Communications Act and the Computer Fraud and Abuse Act).

Douglas Downing, *Dictionary of Computer and Internet Terms* (2003): the vocabulary of electronic discovery is developing so quickly that paper dictionaries age quickly, but this is the best glossary of computer and internet terms in print. Many excellent online glossaries can be found by searching the internet for "glossary" or "dictionary" and the term at issue.

Michele C. S. Lange & Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know* (2004): excellent, practical advice from lawyers at one of the major electronic discovery vendors.

IV. LEGAL WEBSITES AND BLOGS

The following websites offer up-to-date developments in electronic discovery law and practice:

Michael Arkfeld: http://arkfeld.blogs.com/ede/: up-to-date and informative blawg (web log about law).

Richard Best: http://californiadiscovery.findlaw.com/index.htm: comprehensive collection of electronic discovery information by a former commissioner of the San Francisco Superior Court.

Department of Justice: http://www.usdoj.gov/: particularly helpful on criminal issues in electronic discovery.

EDDix: http://www.eddixllc.com/blogs/archives/2004/07/the_eddix_50.asp: this connects you to another lode of electronic discovery websites, blogs, blawgs and newsletters.

Sabrina Pacifici: http://www.bespacific.com/: "accurate, focused law and technology news."

Sedona Conference: thesedonaconference.org: resources on electronic discovery, cost shifting, document retention and electronic filing and electronic access to courts.

Sensei Enterprises: http://www.senseient.com/default.asp?page=main.htm: Sharon Nelson is a lawyer whose writing is delicious, and John Simek supplies insightful forensics. Their collaboration adds up to wonderful articles on electronic discovery.

Withers: http://www.kenwithers.com/: Ken Withers is the associate at the research center at the Federal Judicial Center "responsible for developing and conducting policy-oriented research on the discovery of electronic evidence in civil litigation, supporting the Advisory Committee on Civil Rules of the Judicial Conference of the United States." Withers is at the center of the development of electronic discovery in the federal courts, and his website is the clearing house for many electronic discovery developments.

V. VENDOR WEBSITES

These vendor websites have useful collections of cases and legal developments. Most offer free newsletters of legal developments:

ACT Litigation Services: http://www.actlit.com

Applied Discovery: http://www.lexisnexis.com/applieddiscovery/

EED: http://www.eedinc.com/

Encase: http://www.guidancesoftware.com/

Fios, Inc.: http://www.discoveryresources.org/

KrollOntrack: http://www.krollontrack.com/