



E-Discovery: One Year of the Amended Federal Rules of Civil Procedure

As originally appeared in
New York University Law Review, November 2008.

EMILY BURNS

Cooley Godward Kronish LLP

MICHELLE GREER GALLOWAY

Cooley Godward Kronish LLP

JEFFREY GROSS

Vandenberg & Felio LLP

Cooley
GODWARD KRONISH LLP

E-DISCOVERY: ONE YEAR OF THE AMENDED FEDERAL RULES OF CIVIL PROCEDURE

EMILY BURNS, MICHELLE GREER GALLOWAY,
AND JEFFREY GROSS*

Amendments to the Federal Rules of Civil Procedure (“FRCP”) regarding electronically stored information (“ESI”) took effect on December 1, 2006.¹ Long before those amendments went into effect, however, courts began addressing complex problems regarding the production of ESI.² Indeed, the digital age dawned decades ago but has grown exponentially in recent years. According to a report by technology research firm International Data Corporation

* Emily Burns is a litigation associate with the firm of Cooley Godward Kronish LLP, serves as a guest lecturer at Santa Clara University School of Law in Pretrial Procedures, and is on the adjunct faculty of UC Hastings. She is also active in the training program for the firm’s first year attorneys, Cooley College. Michelle Greer Galloway is Of Counsel at Cooley Godward Kronish, and a lecturer at Stanford Law School and Santa Clara University School of Law, teaching courses in pretrial litigation and in patent litigation, and has lectured and published concerning electronic discovery issues. Jeffrey Gross is Of Counsel at Vandenberg & Feliu and has lectured and published concerning electronic discovery issues.

1. *See* Letter from Chief Justice John Roberts to Rep. J. Dennis Hastert, Speaker of the House (Apr. 12, 2006), <http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf> (transmitting the amendments to the Federal Rules of Civil Procedures that had been adopted by the Supreme Court of the United States pursuant to Section 2072 of Title 28, United States Code).

2. *See, e.g.*, Phoenix Four, Inc. v. Strategic Res. Corp., No. 05 Civ. 4837(HB), 2006 WL 1409413, at *5–7 (S.D.N.Y. May 23, 2006) (awarding monetary sanctions where late production was gross negligence); Hynix Semiconductor Inc. v. Rambus, Inc., No. C-00-20905 RMW, 2006 WL 565893, at *24 (N.D. Cal. Jan. 5, 2006) (holding that adoption of document retention policy was “permissible business decision”); *In re* Universal Serv. Fund Tel. Billing Practices Litig., 232 F.R.D. 669, 674 (D. Kan. 2005) (requiring emails within a strand to be listed separately on privilege log); Hopson v. Mayor of Baltimore, 232 F.R.D. 228 (D. Md. 2005) (addressing challenges and burden of privilege review); Zubulake v. UBS Warburg L.L.C. (*Zubulake V*), 229 F.R.D. 422, 433–34 (S.D.N.Y. 2004) (outlining counsel’s role in preserving and producing electronic discovery); Zubulake v. UBS Warburg L.L.C. (*Zubulake III*), 216 F.R.D. 280, 284 (S.D.N.Y. 2003) (applying seven-factor test to shift twenty-five percent of cost of restoration of backup tapes to plaintiff); Zubulake v. UBS Warburg L.L.C. (*Zubulake I*), 217 F.R.D. 309, 309, 322 (S.D.N.Y. 2003) (ordering production of deleted emails from backup tapes and setting forth seven-factor test for cost shifting); Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 101 (2d Cir. 2002) (holding that courts have discretion in imposing sanctions for discovery abuse).

(“IDC”), the world generated 161 exabytes—each equal to one billion gigabytes—in 2006.³ By 2007, IDC described the “digital universe” as “2.25x10²¹ bits (281 exabytes or 281 billion gigabytes).”⁴ This dwarfs the five exabytes of data that were created in 2002 according to the widely quoted estimate from the University of California, Berkeley.⁵ As described in the Berkeley study, five exabytes is “equivalent in size to the information contained in 37,000 new libraries the size of the Library of Congress book collections.”⁶ Businesses struggle with this explosion of data every day in terms of regulatory compliance, privacy, and retrieval of data necessary to keep enterprises going. For companies involved in litigation, the increase in available ESI also means that a staggering volume of potentially discoverable information may exist.

Two simultaneous developments occurred in the early 2000s to address the discovery of ESI in litigation. First, the American Bar Association (“ABA”)⁷ and the Sedona Conference⁸ began work on developing guidelines for attorneys regarding the production of

3. Brian Bergstein, *So Much Data, Relatively Little Space*, FOXNEWS.COM, Mar. 5, 2007, http://www.foxnews.com/printer_friendly_wires/2007Mar05/0,4675,InformationExplosion,00.html.

4. INT’L DATA CORP., *THE DIVERSE AND EXPLODING DIGITAL UNIVERSE: AN UPDATED FORECAST OF WORLDWIDE INFORMATION GROWTH THROUGH 2011* (2008), <http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>.

5. PETER LYMAN & HAL R. VARIAN, *HOW MUCH INFORMATION* (2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf.

6. *Id.*

7. CIVIL DISCOVERY STANDARDS (2004), *available at* <http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf>.

8. The Sedona Conference creates Working Groups of jurists, lawyers, experts and academics to discuss “forward-looking principles, best practices and guidelines in specific areas of the law that may have a dearth of guidance or are otherwise at a ‘tipping point.’” The Sedona Conference Mission, http://www.thesedonaconference.org/content/tsc_mission/show_page_html (last visited May 18, 2008). For example, the Sedona Principles provide fourteen “best practices recommendations and principles” in these areas of ESI. *See* THE SEDONA CONFERENCE, *THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS AND PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION* (Jonathan M. Redgrave et al. eds., 2d ed. 2007), http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf. In contrast, the amendments to the Federal Rules of Civil Procedure do not address ESI in pre-litigation contexts, nor do they specifically address the common law duty to preserve. *See* Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules*, 12 RICH. J.L. & TECH. 13, ¶¶ 11–12 (2006), *available at* <http://law.richmond.edu/jolt/v12i4/article13.pdf>. For a discussion of the relationship between the Sedona Principles and the 2006 Federal Rules of Civil Procedure amendments, *see* THE SEDONA CONFERENCE, *supra*, at 5–6.

ESI. At the same time, the Advisory Committee on Civil Rules of the Judicial Conference of the United States began to consider amendment of the FRCP to address ESI.⁹

Then, in 2006, amendments to the FRCP changed the Rules in six key areas: (1) ESI became a separate category of discovery materials; (2) the FRCP mandated early attention to e-discovery issues;¹⁰ (3) new rules created a separate procedure for ESI that was “not reasonably accessible”;¹¹ (4) new rules were adopted to allow parties to assert privileges after production;¹² (5) Rules 33, 34 and 45 were revised to apply to ESI, including the form of production;¹³ and (6) Rule 37 set forth a “safe harbor” for ESI lost as a result of the “routine, good-faith operation of an electronic information system.”¹⁴

In the first year under the revised Rules, courts issued numerous opinions about ESI, most of which focused on the final four areas set forth above. In other words, many court decisions focused on the burdens of producing ESI in the context of discovery.¹⁵

The amended Rules were not the only means by which practices changed to embrace electronic discovery. Numerous state ethics committees have addressed ethical issues concerning electronic data, such as how attorneys handle and produce metadata¹⁶ and how to treat underlying information embedded within a document.¹⁷ Furthermore, the Sedona Conference currently publishes

9. By 2005, the Judicial Conference Rules Committee had published draft amendments for comment, held hearings, and approved and transmitted the amendments to the United States Supreme Court. *See* Federal Judiciary Rulemaking, Proposed Amendments for Comment, <http://www.uscourts.gov/rules/proposed0205.html> (last visited June 18, 2008).

10. FED. R. CIV. P. 16(b)(3)(B)(iii), 26(f)(3)(C), Form 35.

11. *Id.* 26(b)(2)(B).

12. *Id.* 26(b)(5)(B).

13. *Id.* 33(d) (dealing with interrogatories); *Id.* 34 (dealing with requests for production of documents and things); *Id.* 45 (dealing with subpoenas to non-parties).

14. *Id.* 37(e).

15. *See supra* note 2.

16. Metadata was defined by an ABA special publication on e-discovery as “information about a particular data set or document that describes how, when, and by whom it was collected, created, accessed, modified, and how it is formatted. . . . Metadata is generally not reproduced in full form when a document is printed.” Jamie B. Schwartz, *Glossary of e-Discovery Terms*, in *E-DISCOVERY: A SPECIAL PUBLICATION OF THE SECTION OF LITIGATION* 46, 47 (Steven A. Weiss & David Coale eds., 2007), *available at* http://www.abanet.org/litigation/sponsors/docs/0307_schwartz.pdf.

17. *See, e.g.*, ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 06-442 (2006) (noting that Model Rule 4.4(b) requires a lawyer who receives informa-

“best practices” guides with respect to various aspects of electronic discovery and evidence.¹⁸ The Judicial Conference, too, proposed amendments to Federal Rule of Evidence 502 to address the challenges created by the high cost of reviewing large ESI productions for privilege, and the question of whether broad subject matter is

tion he knows or should know was sent inadvertently to “promptly notify the sender,” and encourages attorneys to remove metadata before sending documents electronically); Ala. State Bar Office of the Gen. Counsel Formal Op. 2007-02 (2007), *available at* <http://www.alabar.org/ogc/fopDisplay.cfm?oneId=412> (finding an “ethical obligation to refrain from mining an electronic document” for metadata); State Bar of Ariz. Comm. on the Rules of Prof’l Conduct, Formal Op. 07-03 (2007), *available at* <http://www.myazbar.org/Ethics/opinionview.cfm?id=695> (stating that sending attorney must take reasonable precautions to prevent inadvertent disclosure of confidential information; receiving attorney has a “corresponding duty not to ‘mine’ the document for metadata that may be embedded therein or otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel” absent specific enumerated circumstances); Ethics Comm. of the Colo. Bar Ass’n, Formal Op. 119 (2008), *available at* <http://www.cobar.org/index.cfm/ID/386/subID/23789/CEETH> (stating that sending lawyers have a duty “to use reasonable care to guard against the disclosure of metadata containing Confidential Information” and that receiving lawyers “generally may search for and review metadata” unless receiving lawyers “know[] or reasonably should know that the metadata contain or constitute Confidential Information,” in which event they must notify sending lawyers); D.C. Bar Legal Ethics Comm., Op. 341 (2007), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm (prohibiting lawyer from reviewing adversary’s metadata if lawyer has “actual knowledge” that the metadata was sent inadvertently); Fla. Bar Ethics Dept., Op. 06-02 (2006), *available at* <http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument> (requiring lawyer sending ESI to protect confidentiality and lawyer receiving ESI to not mine metadata, but silent as to metadata in ESI produced in discovery); Md. State Bar Ass’n Comm. on Ethics, Op. 2007-09 (2006) (“[T]here is no ethical violation if the recipient attorney . . . reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata.”); N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 749 (2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6533 (prohibiting lawyer from searching adversary’s ESI for metadata); Penn. Bar Ass’n Comm. on Legal Ethics and Prof’l Responsibility, Formal Op. 2007-500 (“[T]he final determination of how to address the inadvertent disclosure of metadata should be left to the individual attorney and his or her analysis of the applicable facts.”).

18. *See, e.g.,* THE SEDONA CONFERENCE, THE SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS (pub. cmt. ver. 2007), http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf; The Sedona Conference, *The Sedona Conference Commentary on Email Management*, 8 SEDONA CONF. J. 239 (2007); The Sedona Conference, *The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery* (2007).

waived when privileged information is disclosed.¹⁹ Similarly, courts are addressing issues regarding the authentication and admissibility of electronic information.²⁰

This Article looks at the law that developed in the first year of the new amendments. In Part I below, we discuss one of the fundamental changes to Rule 26(b)(2), that a party ultimately may not have to produce certain data if it is “not reasonably accessible.” In Part II, we analyze the cases that have struggled with how parties are to review the volumes of business data for privileged information to avoid inadvertent production and/or waiver of privileged information. Part III explores the need for both requesting and responding parties to be explicit regarding the form of production and whether metadata must be produced. It also explores issues concerning metadata in a litigant’s production documents and ethical issues concerning “mining” of metadata by attorneys. Part IV rounds out the analysis of the new amendments by analyzing the “safe harbor” provision of Rule 37 and the ability of parties to argue that they lost information in “good faith.”

In Part V, we turn to the developing area of the evidentiary challenges of ESI, including authentication and admissibility. Finally, we note some of the areas with emerging ESI issues that require litigants and the courts to extrapolate from the new amendments. The explosion of ESI will continue to challenge courts and litigants to find procedures and new ways of seeking and providing discovery in order to find valuable evidence among the chaff (or bytes).

I.

WHAT INFORMATION IS “NOT REASONABLY ACCESSIBLE?”

Perhaps the most significant change regarding ESI was the adoption of a two-tiered approach to discovery. Prior to the amendments, FRCP 34 required a party to produce documents in the party’s “possession, custody, or control,” but the Rule did not explicitly address if it mattered whether information was easy or difficult to find, review and produce.²¹ Although the Rule 34 standard remains in effect, Rule 26(b)(2)(B), as amended, establishes a sec-

19. *See* S. 2450, 110th Cong. (as submitted to Senate, Dec. 11, 2007). The Senate approved S. 2450 without amendment on February 27, 2008. *See* GovTrack.us, S. 2450: A Bill to Amend the Federal Rules of Evidence to Address the Waiver of the Attorney-client Privilege and the Work Product Doctrine, <http://www.govtrack.us/congress/bill.xpd?bill=s110-2450> (last visited June 21, 2008).

20. *See infra* Part V.

21. FED. R. CIV. P. 34(a).

ond tier for discovery of ESI.²² Under the new Rule 26(b)(2)(B), a party responding to a discovery request need not produce ESI from sources that are “not reasonably accessible because of undue burden or cost.”²³ Ultimately, the responding party bears the burden of proving that the data in question is inaccessible.²⁴ However, a court may order the production of inaccessible data if the requesting party demonstrates good cause.²⁵

Notably, the advisory committee’s notes for Rule 26(b)(2)(B) do not provide guidance regarding how courts should determine whether data is “not reasonably accessible.” Instead, the notes state only that “[i]t is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information.”²⁶ This leaves district courts with substantial discretion in interpreting amended Rule 26(b)(2)(B) to define what ESI is “not reasonably accessible.”

Court opinions on the definition of “not reasonably accessible” appear to split into two camps. One group of cases focuses on the technological aspects that make certain ESI not easily searchable, while the other group focuses strictly on the monetary cost of collecting, storing, and reproducing ESI, regardless of whether the data can be searched or made searchable in an inexpensive manner. These two lines of cases are discussed below.

Courts that focus on the technological issues rely heavily on the *Zubulake* series of cases. In *Zubulake I*, Judge Scheindlin of the District Court for the Southern District of New York categorized

22. *Id.* 26(b)(2)(B).

23. *Id.* According to the advisory committee’s notes to Rule 26, the responding party must identify the sources containing potentially responsive information that it is not searching or producing. *Id.* 26 advisory committee’s notes.

24. *Id.* 26(b)(2)(B). See also *Peskoff v. Faber*, 240 F.R.D. 26, 31 (D.D.C. 2007) (“[I]t cannot be argued that a party should ever be relieved of its obligation to produce accessible data merely because it may take time and effort to find what is necessary.”).

25. The factors that the court is to consider in determining whether there is good cause to produce inaccessible data are found in Rule 26(b)(2)(C):

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

FED. R. CIV. P. 26(b)(2)(C).

26. *Id.* 26 advisory committee’s notes.

media on a spectrum which reflected varying degrees of their accessibility.²⁷ She described five types of data: (1) active, online data; (2) near-line data; (3) offline storage/archives; (4) backup tapes; and (5) erased, fragmented or damaged data.²⁸ Judge Scheindlin noted that “backup tapes” and “erased, fragmented or damaged data” are generally considered inaccessible because they are not easily searchable in their current forms and must be restored or otherwise manipulated before they can be used.²⁹

Many recent cases have adopted this taxonomy in whole or in part. For example, citing *Zubulake I*, the court in *Quinby v. WestLB AG* held that backup tapes were inaccessible, noting that “[d]ata stored on backup tapes becomes usable when fragmented data contained on the tapes is unfragmented and erased data is reconstructed.”³⁰ Likewise, the court in *Best Buy Stores, L.P. v. Developers Diversified Realty Corp.* rejected the defendant’s argument that the plaintiff should be required to produce the contents of a database that had been prepared for unrelated litigation.³¹ The plaintiff did not contest that the data was relevant, but stated that the data on the database had been “downgraded” such that it was not easily searchable and, therefore, was not “reasonably accessible.”³² The court agreed with the plaintiff, focusing on the fact that the data, in its current form, was not easily searchable.³³ Similarly, in *W.E. Aubuchon Co. v. BeneFirst L.L.C.*, the court found that medical claim information that had been scanned to disks was not easily searchable and would require extensive cross-referencing to locate particular claims accurately.³⁴ Finding the ESI not reasonably accessible, the court likened the disks to backup tapes because both types of ESI required significant conversion or manipulation before they could be searched.³⁵

Thus, *Quinby*, *Best Buy* and *W.E. Aubuchon* all reflect the continued acceptance of Judge Scheindlin’s analysis in *Zubulake I*. These

27. *Zubulake v. UBS Warburg (Zubulake I)*, 217 F.R.D. 309, 318–19 (S.D.N.Y. 2003).

28. *Id.*

29. *Id.* at 319–20.

30. 245 F.R.D. 94, 99 (S.D.N.Y. 2006) (citing *Zubulake I*, 217 F.R.D. at 319–20); see also *In re Veeco Instruments, Inc. Sec. Litig.*, No. 05 MD 1695(CM)(GAY), 2007 WL 983987, at *2 (S.D.N.Y. April 2, 2007) (determining, without analysis, that backup tapes were inaccessible).

31. 247 F.R.D. 567, 570–71 (D. Minn. 2007).

32. *Id.* at 570.

33. *Id.* at 571.

34. 245 F.R.D. 38, 42–43 (D. Mass. 2007).

35. *Id.*

courts focused mainly on whether the ESI at issue was easily searchable. In these decisions, data was held to be “not reasonably accessible” when it could not be searched without conversion or manipulation.

In another line of cases, however, courts have based accessibility rulings on the explicit language of Rule 26(b)(2)(B), which states that ESI can be considered “not reasonably accessible” as a result of undue burden or cost. These courts have interpreted the burdens or costs involved in storing, collecting, and producing available ESI to mean monetary costs, regardless of whether the ESI requested was easily searchable. For example, in *Ameriwood Industries, Inc. v. Liberman*, the district court determined that the sheer number of emails and electronic documents that were potentially responsive to plaintiff’s broad discovery request (over 55,000) rendered the information sought “not reasonably accessible” due to the costs associated with reviewing it.³⁶ Notably, the court’s analysis did not address whether the ESI required any further manipulation before production.

This focus on monetary costs was also dispositive in *PSEG Power New York, Inc. v. Alberici Constructors, Inc.*³⁷ In *PSEG*, a technical problem with the plaintiff’s production resulted in the separation of emails and their attachments.³⁸ When the defendant moved to compel another copy of the 3,000 emails with their attachments, the plaintiff argued that the information was not reasonably accessible due to the high cost of reproduction.³⁹ Here, there was no question that the ESI existed in an easily searchable format because the plaintiff still had the emails in their native form.⁴⁰ However, the court held that because the reproduction would be expensive, the information was not reasonably accessible.⁴¹

The cost of producing data also influenced the court’s reasoning in *Columbia Pictures Industries v. Bunnell*.⁴² In *Columbia*, the district court again concentrated on the monetary cost of collecting, storing, and producing the ESI at issue. The plaintiff filed a motion to compel production of data stored in the random access memory

36. No. 4:06CV524-DJS, 2007 WL 496716, at *2 (E.D. Mo. Feb. 13, 2007).

37. No. 1:05-CV-657 (DNH/RFT), 2007 WL 2687670, at *10 (N.D.N.Y. Sept. 7, 2007).

38. *Id.* at *2.

39. *Id.* at *10.

40. *Id.*

41. *Id.*

42. No. CV 06-1093FMCJCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007).

(“RAM”) in defendants’ computers.⁴³ This data identified Internet Protocol (“IP”) addresses that had accessed copyrighted content.⁴⁴ While the defendants would not have needed to convert this data before producing it, they argued that the data was not reasonably accessible because of the high cost of collecting, storing, and producing it.⁴⁵ The court ultimately ordered production of the RAM data, stating that the monetary cost of collecting, storing, and producing a mere 400 megabytes a day did not impose an undue burden on the defendants.⁴⁶

Thus, in contrast to the opinions in *Quinby*, *Best Buy*, and *W.E. Aubuchon*, the courts in *Ameriwood*, *PSEG*, and *Columbia* eschew the technological taxonomy of the *Zubulake* opinions, and focus rather on the literal monetary costs involved to determine whether ESI is “not reasonably accessible.” As a result of this split of authority, it is difficult to predict how future courts will determine whether data is accessible under the new Rule 26(b)(2)(B).

II.

WHAT IS “INADVERTENT PRODUCTION” OF PRIVILEGED INFORMATION UNDER THE NEW RULES?

Not only can it be unduly burdensome to locate, review and produce some forms of ESI, but it can also be expensive to review gigabytes or terabytes of information for privilege.⁴⁷ In considering the 2006 amendments, the advisory committee noted:

The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discovery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the diffi-

43. *Id.* at *1.

44. *Id.*

45. *Id.* at *7.

46. *Id.* at *8.

47. *See, e.g.,* Hopson v. Mayor of Baltimore, 232 F.R.D. 228, 232 (D. Md. 2005) (“This case vividly illustrates one of the most challenging aspects of discovery of electronically stored information—how properly to conduct Rule 34 discovery within a reasonable pretrial schedule, while concomitantly insuring that requesting parties receive appropriate discovery, and that producing parties are not subjected to production timetables that create unreasonable burden, expense, and risk of waiver of attorney-client privilege and work product protection.”).

culty in ensuring that all information to be produced has in fact been reviewed.⁴⁸

To address this challenge, Rules 26(b)(5) and 45(d)(2)(B) allow parties that have inadvertently produced privileged information to ask that the document be returned, sequestered, or destroyed pending resolution of the privilege claim. Rule 26(b)(5) states:

(B) *Information Produced.* If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.⁴⁹

Such a provision, often found in protective orders, is referred to as a “claw-back” provision. In other words, a litigant who mistakenly produces a privileged document may claw back the document from production without a finding that privilege has been waived.

However, Rule 26(b)(5) is a rule of procedure that does not alter the substantive law pertaining to waiver of privilege.⁵⁰ Thus, the mere presence of a claw-back provision in a protective order may not resolve the privilege issue. As noted by the advisory committee, the Rule “provide[s] a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery.”⁵¹

The question of whether a privilege asserted after information has been produced is waived by the production is not addressed by the FRCP. Rather, this issue has been addressed in common law cases regarding inadvertent production and in the proposed amendments to Federal Rule of Evidence 502, discussed below.

48. FED. R. CIV P. 26 advisory committee’s notes.

49. *Id.* 26(b)(5); *see also id.* 45(d)(2) (stating the same rule for information produced in response to a subpoena).

50. *Id.* 26 advisory committee’s notes.

51. *Id.*

The courts have considered whether the inadvertent production of an otherwise privileged document waives privilege.⁵² Some courts have adopted a strict standard and have refused to uphold the privilege, finding that production defeats the confidentiality essential to a claim of privilege.⁵³ Other courts have taken a balancing approach, considering factors including the reasonableness of precautions taken by the producing party, the number of inadvertent disclosures, the extent of the disclosure, the time elapsed before the producing party attempted to remedy the disclosures, and the interests of justice.⁵⁴

Several cases have addressed the reasonableness of precautions taken to avoid inadvertent production of privileged documents in the context of ESI. In general, these cases have held that a party must review documents before producing them. For example, in *Ciba-Geigy Corp. v. Sandoz*, the party produced a privileged memorandum from a database that it believed contained only non-privileged documents.⁵⁵ Although there was a claw-back provision in place, the court held that the producing party waived the privilege because on two occasions, counsel failed to conduct a privilege review prior to producing the documents at issue.⁵⁶ More recent cases have reached similar results.⁵⁷ For example, courts have held that a party did not implement “reasonable precautions” when it produced images of documents that were unreadable in the review.⁵⁸ Similarly, courts have found that a party had waived its right to privilege when counsel “merged” otherwise segregated privileged and non-privileged documents.⁵⁹ Recently, a court found that a party waived privilege associated with over 165 documents pro-

52. *See, e.g., Hopson*, 232 F.R.D. at 235–36 (surveying different courts’ methods of handling inadvertent production).

53. *See, e.g., In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989).

54. *See, e.g., Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985).

55. *Ciba-Geigy Corp. v. Sandoz Ltd.*, 916 F. Supp. 404, 407 (D.N.J. 1995).

56. *Id.* at 412.

57. *See Gail v. New England Gas Co.*, 243 F.R.D. 28, 37 (D.R.I. 2007); *Gragg v. Int’l Mgmt. Group*, No. 5:03-CV-0904 (NPM/DEP), 2007 WL 1074894, at *6–7 (N.D.N.Y. Apr. 5, 2007).

58. *See Amersham Biosciences v. PerkinElmer, Inc.*, No. 03-4901 (JLL), 2007 WL 329290, at *7 (D.N.J. Jan. 31, 2007) (finding no abuse of discretion in Magistrate’s ruling that “turning over unintelligible or unreadable documents to an adversary evidences a lack of reasonable precaution” but remanding as to other inadvertent production issues).

59. *See Marrero Hernandez v. Esso Standard Oil Co.*, No. 03-1485 (JAG/GAG), 2006 WL 1967364, at *1, 5 (D.P.R. July 11, 2006).

duced after a keyword search was unsuccessfully used to identify privileged information.⁶⁰

In an effort to unify these approaches, a proposed amendment to Federal Rule of Evidence 502 was submitted to Congress.⁶¹ Under this proposed amendment, there is no waiver of privilege if production was “inadvertent,” reasonable steps were taken to protect privilege, and prompt remedial action was taken.⁶² Until the new amendment becomes law (and even afterwards, given the fact-intensive inquiry into the reasonableness of a party’s efforts to prevent disclosure and the promptness of its corrective action), parties will continue to litigate the question of whether production was inadvertent.⁶³

III. FORM OF PRODUCTION—ASK FOR WHAT YOU WANT

FRCP 26 requires a discovery plan that includes a party’s views on the “form or forms in which” ESI should be produced.⁶⁴ Amended Rules 34(b) and 45(d) provide that the requesting party may specify the form of production for ESI and the responding party may object.⁶⁵ If the requesting party does not specify a de-

60. See *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 262 (D. Md. 2008) (“Use of search and information retrieval methodology, for the purpose of identifying and withholding privileged or work-product protected information from production, requires the utmost care in selecting methodology that is appropriate for the task because the consequence of failing to do so, as in this case, may be the disclosure of privileged/protected information to an adverse party, resulting in a determination by the court that the privilege/protection has been waived.”).

61. See *supra* note 19.

62. Proposed Federal Rule of Evidence 502: “(b) Inadvertent Disclosure.—When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).” S. 2450, 110th Cong. (as submitted to Senate, Dec. 11, 2007).

63. See *Hopson v. Mayor of Baltimore*, 232 F.R.D. 228, 234 (D. Md. 2005).

64. FED R. CIV. P. 26(f)(3).

65. *Id.* 34(b)(1)(C) (“[Requests] may specify the form or forms in which electronically stored information is to be produced.”); *Id.* 34(b)(2)(E)(ii) (“If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms . . .”); *Id.* 45(a)(1)(C) (“A subpoena may specify the form or forms in which electronically stored information is to be produced.”); *Id.* 45(c)(2)(B) (“A person commanded to produce documents . . . may

sired format, ESI may be produced either (1) in the form in which it is “ordinarily maintained” (also referred to as “native”) or (2) in a “reasonably useable” form.⁶⁶ The responding party should state the intended form of production so that the parties may “identify and seek to resolve disputes before the expense and work of the production occurs.”⁶⁷ However, the party need only produce particular ESI in one form.⁶⁸ The producing party’s freedom to choose a format is also constrained by the advisory committee’s admonition that a responding party should not impair the requesting party’s ability to search the data.⁶⁹

A common issue regarding the form of production is whether the producing party shall be required to produce metadata.⁷⁰ Metadata is a term used to describe “data about data” and can range from statistics, such as the number of words in a document, to a history of the document’s creation and use, including changes that were made, by whom, and when.⁷¹ Although the FRCP do not explicitly address metadata, at least one district court has issued local rules providing for a default rule of production of images without metadata.⁷² As set forth below, courts have addressed two

serve on the party or attorney designated in the subpoena a written objection . . . to producing electronically stored information in the form or forms requested.”).

66. *Id.* 34(b)(2)(E)(ii).

67. *Id.* 34 advisory committee’s notes.

68. *Id.*

69. The advisory committee’s notes on the 2006 amendments state that “[a] party that responds to a discovery request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form.” *Id.* The notes further state that “[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.” *Id.*

70. See, e.g., THE SEDONA CONFERENCE, *supra* note 8, at 60; BARBARA J. ROTHSTEIN ET AL., FED. JUDICIAL CTR., *MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 13* (2007), [http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/\\$file/eldscpkt.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf); PAUL W. GRIMM ET AL., *SUGGESTED PROTOCOL FOR DISCOVERY OF ELECTRONICALLY STORED INFORMATION (“ESI”) § 11(B)*, <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf>.

71. For a definition of metadata, see *supra* note 16.

72. See, e.g., N.D. OHIO LOCAL R. app. K § 6 (“Format. If, during the course of the Rule 26(f) conference, the parties cannot agree to the format for document production, electronically stored information shall be produced to the requesting party as image files (e.g., PDF or TIFF). When the image file is produced, the producing party must preserve the integrity of the electronic document’s contents, i.e., the original formatting of the document, its metadata and, where applicable,

primary issues surrounding metadata: first, whether the metadata is relevant to any issue in the case; and second, the potential for waiver of attorney-client or work product privilege when metadata is produced.

The first well-known case discussing metadata is *Williams v. Sprint/United Management Co.*⁷³ This decision involved a discovery dispute over whether Excel spreadsheets had to be produced with metadata, i.e., with embedded formulas.⁷⁴ The district court decided that metadata “should presumptively be treated as part of the ‘document’ and should thus be discoverable” under the emerging electronic discovery standards.⁷⁵ The court then held that the producing party had the initial burden to object to a request for metadata.⁷⁶ In subsequent cases, if document requests did not specifically request metadata, courts have generally not required parties to reproduce documents in native form.⁷⁷ For example, in a proceeding subsequent to *Williams I*, the plaintiff asked the court to order production of some 11,000 emails and attached spreadsheets

its revision history. After initial production in image file format is complete, a party must demonstrate particularized need for production of electronically stored information in their native format.”); *see also* GRIMM ET AL., *supra* note 70, § 11(C) (“Meta-Data, especially substantive Meta-Data, need not be routinely produced, except upon agreement of the requesting and producing litigants, or upon a showing of good cause in a motion . . .”).

73. (*Williams I*) 230 F.R.D. 640 (D. Kan. 2005).

74. *Id.* at 644.

75. *Id.* at 652.

76. *Id.* (“The initial burden with regard to the disclosure of the metadata would therefore be placed on the party to whom the request or order to produce is directed. The burden to object to the disclosure of metadata is appropriately placed on the party ordered to produce its electronic documents as they are ordinarily maintained because that party already has access to the metadata and is in the best position to determine whether producing it is objectionable. Placing the burden on the producing party is further supported by the fact that metadata is an inherent part of an electronic document, and its removal ordinarily requires an affirmative act by the producing party that alters the electronic document.”).

77. *See, e.g.*, *Autotech Techs. Ltd. P’ship v. Automationdirect.com*, 248 F.R.D. 556, 559 (N.D. Ill. 2008) (“It seems a little late to ask for metadata after documents responsive to a request have been produced in both paper and electronic format. Ordinarily, courts will not compel the production of metadata when a party did not make that a part of its request.”); *D’Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.D.C. 2008) (denying motion to compel production of specific document in original format with metadata where plaintiff’s request did not specify production of metadata); *ICE Corp. v. Hamilton Sundstrand Corp.*, No. 05-4135-JAR, 2007 WL 4239453, at *5–6 (D. Kan. Nov. 30, 2007) (denying motion to compel production with metadata where plaintiff never specified form of production in original requests).

in native format.⁷⁸ Because the defendant had produced the emails in hard copy without objection and had established the burden of reproducing the emails in native format, the court denied the plaintiff’s request.⁷⁹ Similarly, in *Kentucky Speedway, L.L.C. v. NASCAR, Inc.*, the district court denied a motion to compel metadata for documents previously produced in hard copy when the request came months after the initial production took place.⁸⁰ Recently, a court declined to order documents produced in native format to be reproduced as static images.⁸¹

In addition to disagreements about the production of metadata, the reported cases reflect numerous disagreements about the form of production. Frequently, courts have disagreed about the sufficiency of the production of static image files, most commonly using the Tagged Image File Format (commonly known as “TIFF” images) or Adobe’s Portable Document Format (“PDF”).⁸² As noted above, some local rules create a presumption favoring TIFF or PDF images for production instead of production in native form.⁸³ Courts, too, have sometimes favored TIFF or PDF productions because these formats are more secure and less likely to be manipulated.⁸⁴ However, other courts have found production of PDF or TIFF images insufficient to meet the obligations of Rule 34.⁸⁵ Moreover, the reported cases reflect fact-specific issues con-

78. *See Williams v. Sprint/United Mgmt. Co. (Williams II)*, No. 03-2200-JWL-DJW, 2006 WL 3691604, at *1 (D. Kan. Dec. 12, 2006).

79. *Id.* at *6–8.

80. No. 05-138-WOB, 2006 WL 5097354, at *8 (E.D. Ky. Dec. 18, 2006). *See also Michigan First Credit Union v. Cumis Ins. Soc’y, Inc.*, No. 05-74423, 2007 WL 4098213, at *3 (E.D. Mich. Nov. 16, 2007) (imposing no sanctions for failure to produce records in native format or with intact metadata where the party objected to production of metadata); *Schmidt v. Levi Strauss & Co.*, No. C04-01026 RMW (HRL), 2007 WL 2688467, at *1–2 (N.D. Cal. Sept. 10, 2007) (denying motion to compel where electronic versions of documents sought six months after discovery cutoff).

81. *See Perfect Barrier L.L.C. v. Woodsmart Solutions Inc.*, No. 3:07-CV-103 JVB, 2008 WL 2230192, at *3 (N.D. Ind. May 27, 2008).

82. *See ROTHSTEIN ET AL.*, *supra* note 70, at 13.

83. *See supra* note 72.

84. *See, e.g., In re Priceline.com Inc. Sec. Litig.*, 233 F.R.D. 88, 91 (D. Conn. 2005) (“TIFF or PDF format is the most secure format . . . [therefore] no inadvertent alterations are made, or more likely, no accusations of alteration can be made.”). The *Priceline* court specifically noted that the parties could seek exceptions to the directive if production in native format were necessary to view or understand a document. *Id.*

85. *See In re Payment Card Interchange Fee & Merchant Disc.*, No. MD 05-1720(JG)(JO), 2007 WL 121426 (E.D.N.Y. Jan. 12, 2007) (refusing to order reproduction in native format but denying protective order as to future production);

cerning whether the form of production of unique data was “reasonably usable.”⁸⁶ The case law is split on whether metadata is relevant.⁸⁷

The cases discussed above focus on the production of documents by a litigant in response to a Rule 34 request for production. However, numerous ethics committees have focused on the more general question of metadata mining. In other words, when adversaries exchange data electronically, may a party “mine the metadata” and seek privileged information, whether attorney-client communications or attorney work product, that may have been embedded in the document? While the ABA has concluded that there is no ethical prohibition on attorneys’ attempting to find and/or use the metadata in documents exchanged outside the Rule 34 context,⁸⁸ state bar ethics committees have reached a variety of conclusions regarding so-called “metadata mining.”⁸⁹ Thus, while amended Rules 34(b) and 45(d) require parties to address issues

Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2006 WL 665005, at *2 (N.D. Ill. Mar. 8, 2006) (finding that conversion to TIFF “altered the format and characteristics of the electronic media . . . essentially creating new documents”).

86. See, e.g., PSEG Power New York, Inc. v. Alberici Constructors, Inc., No. 1:05-CV-657 (DNH/RFT), 2007 WL 2687670, at *8 (N.D.N.Y. Sept. 7, 2007) (ordering emails reproduced where vendor separated emails and attachments); DE Techs. v. Dell, Inc., No. 7:04CV00628, 2007 WL 128966, at *1 (W.D. Va. Jan. 12, 2007) (overturning magistrate’s sanction order where defendant produced 543,000 documents in electronic, searchable form, but not with “live electronic directory” to which employees had access).

87. For example, in *Kentucky Speedway, L.L.C. v. NASCAR, Inc.*, No. 05-138-WOB, 2006 WL 5097354 (E.D. Ky. Dec. 18, 2006), the court denied a motion to compel metadata for documents previously produced in hard copy when the request came months after initial production. The court noted that “[i]n most cases and for most documents, metadata does not provide relevant information.” *Id.* at *8. Similarly, in *Wyeth v. Impax Labs., Inc.*, No. 06-222-JJF, 2006 WL 3091331, at *2 (D. Del. Oct. 26, 2006), the court found that “[m]ost metadata is of limited evidentiary value, and reviewing it can waste litigation resources.” *But see* Ryan v. Gifford, No. 2213-CC, 2007 WL 4259557, at *1 (Del. Ch. Nov. 30, 2007) (finding that metadata may be “especially relevant” in an options backdating case where the integrity of the dates of documents was at issue and the company’s special committee had reviewed documents in native form).

88. In 2006, the American Bar Association issued Formal Opinion 06-442, which concluded that “[t]he Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party.” ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 06-442 (2006).

89. See *supra* note 17.

concerning the form of production in advance, there are many unresolved legal issues concerning the exchange of electronic data.

IV.

NO “SAFE HARBOR” FOR PARTIES PRODUCING ESI

Another unresolved legal issue is the extent to which litigants may rely on new provisions in the FRCP to shield themselves from liability for destruction of evidence. FRCP 37(e) provides that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”⁹⁰ This new addition to the FRCP was described as a “safe harbor” and was hailed by some commentators as an opportunity to help companies escape sanction when their systems automatically caused the destruction of ESI even though they were under a duty to preserve data.⁹¹

Other e-discovery commentators argued that the advisory committee’s notes, which require that a party have acted in good faith, significantly undercut the appearance of protection reflected in the text of Rule 37(e).⁹² Some have argued that the connection of the “good faith” standard to the producing party’s duty to preserve has rendered the Rule ineffective.⁹³ In other words, if the party cannot avail itself of the safe harbor because it had a duty to preserve data in the first instance, then Rule 37 does little to change the state of the pre-existing common law.⁹⁴ The language of the advisory com-

90. FED. R. CIV. P. 37(e). This section of the Federal Rules, formerly FED. R. CIV. P. 37(f), was converted to FED. R. CIV. P. 37(e) with the renumbering of certain Federal Rules of Civil Procedure, effective 12/1/2007. This restyling of the Federal Rules was not intended to make any substantive changes to the rules. See *id.* 37 advisory committee’s notes.

91. See Thomas Y. Allman, *Defining Culpability: The Search for a Limited Safe Harbor in Electronic Discovery*, 2006 FED. CTS. L. REV. 7, at 1 (2006), available at <http://www.fclr.org/docs/2006fedctsrev7.pdf> (“Rule 37[(e)] will provide relief from rule-based sanctions for routine losses due to operations of information systems when a party has exercised ‘good faith’ in planning for and executing preservation obligations. There will be cases where losses to e-discovery from the operation of information systems are not sanctionable even though the preservation obligations have been triggered.”).

92. Michael R. Nelson & Mark H. Rosenberg, *A Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery*, 12 RICH. J.L. & TECH. 14, ¶ 48 (2006), available at <http://law.richmond.edu/jolt/v12i4/article14.pdf>.

93. *Id.* ¶ 50.

94. *Id.* ¶ 49. The 2006 amendments to the Federal Rules of Civil Procedure did not alter the duty to preserve, which arises under the common law. Even before the amendments, the courts were addressing issues of preservation in the

mittee's notes, reproduced below in relevant part, justifies this concern:

Rule 37[e] applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37[e] means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically discovered information.

Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.⁹⁵

Recent decisions have justified this skeptical view of the safe harbor provided by Rule 37(e). Indeed, the courts that have assessed the producing party's good faith in the operation of routine

context of ESI. In any event, the duty to preserve requires "more than a mere possibility of litigation." See *Cache La Poudre Feeds, L.L.C. v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 623 (D. Colo. 2007) (citing *Hynix Semiconductor Inc. v. Rambus, Inc.*, No. C-00-20905 RMW, 2006 WL 565893, at *21 (N.D. Cal. Jan. 5, 2006)) (stating that a letter that alluded to possible "exposure" without threatening litigation and "hinted at the possibility of a non-litigious resolution" did not trigger duty to preserve); *In re Kmart Corp.*, 371 B.R. 823, 836, 844 (Bankr. N.D. Ill. 2007) (finding that an email to one Kmart employee about the certainty of legal action was insufficient to trigger a duty of preservation, but filing of an administrative claim containing sufficient information to put Kmart on notice *did* trigger duty).

95. FED. R. CIV. P. 37(e) advisory committee's notes.

systems have focused on whether the producing party had an obligation to preserve the destroyed information in the first instance. For example, in *Columbia Pictures Industries v. Bunnell*, the plaintiffs sought data stored in the defendants' RAM that identified the IP addresses that had accessed copyrighted content (the Server Log Data).⁹⁶ The defendants had not retained this data, which was only available on their website server for six hours after the information was generated.⁹⁷ The plaintiffs argued that the defendants had been, and continued to be, obligated to preserve the Server Log Data.⁹⁸ The district court ordered the defendants to preserve such data in the future but suggested that there was no pre-existing duty to preserve it.⁹⁹ The court based this holding on the lack of prior precedent regarding the preservation of RAM data and the plaintiffs' failure to specifically request its preservation.¹⁰⁰ Consequently, the court did not issue sanctions because it found that "defendants' failure to retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required."¹⁰¹ In so holding, even though the court spoke in terms of "good faith" (a phrase borrowed from Rule 37(e)), it ultimately declined to award sanctions because no obligation to preserve the data had attached.¹⁰²

In contrast, another recent decision, *In re Krause*, illustrates how courts have refused to apply the safe harbor provision if a party violated its duty to preserve evidence.¹⁰³ Here, the debtor reinstalled a program called GhostSurf on his desktop just days after he was ordered to produce electronic records, and on his laptop the day before turning it over to the Trustee.¹⁰⁴ The GhostSurf program contained a command to remove, or "wipe," all deleted files, precluding restoration of the files or data.¹⁰⁵ The debtor previously had the GhostSurf program running on both computers, during the period after which the duty to preserve attached.¹⁰⁶ The district

96. No. CV 06-1093FMCJCX, 2007 WL 2080419, at *2-3 (C.D. Cal. May 29, 2007).

97. *Id.* at *3.

98. *Id.* at *7.

99. *Id.* at *14.

100. *Id.*

101. *Id.*

102. *Id.*

103. *United States v. Krause (In re Krause)*, 367 B.R. 740 (Bankr. D. Kan. 2007).

104. *Id.* at 748.

105. *Id.* at 750.

106. *Id.* at 749.

court disregarded the debtor's argument that he could claim the safe harbor of Rule 37(e) because allowing the GhostSurf program to destroy data after the duty to preserve had attached and reinstalling the software mere days before turning over the computers were not actions done in good faith.¹⁰⁷ The court also questioned whether running the GhostSurf program was a routine operation and stated that "[j]ust as a litigant may have an obligation to suspend certain features of a 'routine operation,' the Court concludes that a litigant has an obligation to suspend features of a computer's operation that are not routine if those features will result in destroying evidence."¹⁰⁸

Doe v. Norwalk Community College reflects an even more limited view of the protection afforded by Rule 37(e).¹⁰⁹ In that case, the district court explicitly held that a party seeking to invoke the good faith exception in Rule 37(e) must "act affirmatively to prevent [its routine system operations] from destroying or altering information, even if such destruction would occur in the regular course of business."¹¹⁰ The court also noted that Rule 37(e) requires operation of a "routine system," that is, a system which is "generally designed, programmed, and implemented to meet the party's technical and business needs."¹¹¹ The court suggested that the deletion of the defendant's emails was not the result of an established system, but rather of ad hoc decisions by individual custodians.¹¹²

Other courts have taken the producing party's "shield" embodied in Rule 37(e) and turned it into a "sword" to be used by the requesting party to prove spoliation of evidence. At least one well-respected e-discovery jurist has interpreted the advisory committee's notes to Rule 37(e) as actually imposing a separate *affirmative* obligation on parties to disable any routine systems that would eliminate discoverable information after the duty to preserve had attached.¹¹³

107. *Id.* at 768–69.

108. *Id.* at 768.

109. 248 F.R.D. 372 (D. Conn. 2007).

110. *Id.* at 378.

111. *Id.* (quoting FED R. CIV. P. 37 advisory committee's notes).

112. *Id.*

113. See Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007) ("[I]t is clear that [Rule 37(e)] does not exempt a party who fails to stop the operation of a system that is obliterating information that may be discoverable in litigation."); *Peskoff v. Faber*, 244 F.R.D. 54, 60 (D.D.C. 2007) ("The Advisory Committee comments to amended Rule 37[(e)] make it clear that any automatic deletion feature should be turned off . . . once litigation can be reasonably anticipated.").

In sum, *Columbia Pictures*, *Krause* and *Doe* adopt and strengthen the advisory committee's marriage of the "good faith" standard to the duty to preserve. Whereas the advisory committee's notes state that "[g]ood faith in the routine operation of an information system *may* involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information," the trend in the case law appears to hold that litigants *must* disable such features to be able to take advantage of Rule 37(e).¹¹⁴ One district court judge even went so far as to warn litigants that "they should be very cautious in relying upon any 'safe harbor' doctrine as described in new Rule 37[(e)]."¹¹⁵

V. EVIDENTIARY ISSUES FOR ESI

The cost of preserving, reviewing, and producing electronic data is undeniably high. But parties will waste an extraordinary amount of time and money if they cannot admit the data into evidence or use it to support or oppose a motion for summary judgment. Chief Magistrate Judge Grimm in the District of Maryland highlighted this issue in one of the most important e-discovery cases decided in 2007, *Lorraine v. Markel American Insurance Company*.¹¹⁶ In *Lorraine*, the consequences of paying insufficient attention to evidentiary issues were substantial. The lawsuit concerned the proper insurance recovery arising from damages caused to a boat by light-

114. FED R. CIV. P. 37 advisory committee's notes. The only anomaly in this trend appears to be *Escobar v. City of Houston*, No. 04-1945, 2007 WL 2900581 (S.D. Tex. Sept. 29, 2007), the only case found to have permitted the producing party to take advantage of the safe harbor of Rule 37(e). In *Escobar*, the plaintiffs requested that the court assess sanctions against the defendant, the City of Houston, for neglecting to disable an email auto-delete function, which resulted in the destruction of emails sent within the City Police Department during the twenty-four hours following the officer-involved shooting at issue. *Id.* at *17. The court declined to award sanctions, ruling that plaintiffs had not met their burden of showing that the emails were relevant or that they were destroyed in bad faith, and noting that the officers involved were not likely to have used email to communicate about the incident. *Id.* at *18–19. Seemingly as an afterthought, the court also stated that "under Rule 37[(e)] of the Federal Rules of Civil Procedure, if the electronic communications were destroyed in the routine operation of the [Department's] computer system, and if there is no evidence of bad faith in the operation of the system that led to the destruction of the communications, sanctions are not appropriate." *Id.* at *18.

115. *Oklahoma ex rel. Edmondson v. Tyson Foods, Inc.*, No. 05-CV-329-GKF-SAJ, 2007 WL 1498973, at *6 (N.D. Okla. May 17, 2007).

116. 241 F.R.D. 534 (D. Md. 2007).

ning.¹¹⁷ On cross-motions for summary judgment, the parties sought to resolve the narrow issue of whether an arbitrator had the power to reduce insurance recovery from \$36,000 to \$14,000.¹¹⁸ Because the summary judgment motions were based entirely on electronic evidence without an appropriate evidentiary foundation of supporting affidavits and deposition testimony, the Court dismissed both motions, leaving the parties to face the prospects of a trial that might cost nearly as much as the money at stake.¹¹⁹

Thus, *Lorraine* served as a wake-up call. Historically, some courts have admitted electronic evidence upon a minimal showing of reliability and a conclusory showing that the information fell within the business records exception to the hearsay rule.¹²⁰ In essence, these courts have presumed that electronic evidence is reliable absent evidence of tampering or other unusual circumstances.¹²¹ However, other courts have required parties to provide detailed proof that electronic evidence is competent and reliable.¹²² Therefore, well-prepared counsel would be wise to expect a court to apply the most rigorous standards to electronic evidence. While Judge Grimm used *Lorraine* as an opportunity to explore evidentiary issues for ESI in greater detail, the determinative issue was actually the application of traditional rules of authentication, hearsay, and the best evidence rule to ESI.

A. Authentication of Electronic Evidence in General

As interpreted by judges, the Federal Rules of Evidence set a relatively low standard for authenticating evidence.¹²³ Federal Rule of Evidence 901 requires enough evidence “to support a finding

117. *Id.* at 535.

118. *Id.*

119. *Id.* at 537.

120. *See* *Sea-Land Serv., Inc. v. Lozen Int'l, L.L.C.*, 285 F.3d 808, 819 (9th Cir. 2002) (holding that trial court properly admitted electronic bills of lading pursuant to the business records exception to the hearsay rule; it was immaterial that records were maintained electronically and not in paper form); *United States v. Salgado*, 250 F.3d 438, 452–53 (6th Cir. 2001) (admitting computerized telephone billing records even though records custodian was not familiar with the accuracy of the system).

121. *See* *Sea-Land*, 285 F.3d at 819; *Salgado*, 250 F.3d at 452–53.

122. *See, e.g.*, *Am. Express Travel Related Serv. Co. v. Vinhnee (In re Vinhnee)*, 336 B.R. 437, 444–45 (B.A.P. 9th Cir. 2005) (excluding electronic business records and noting that early cases examined the authenticity of ESI with insufficient rigor).

123. *See* *Lorraine*, 241 F.R.D. at 542 (“A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. This is not a particularly high barrier to overcome.” (citation omitted)).

that the matter in question is what its proponent claims.”¹²⁴ In other words, evidence of authentication need not be conclusive; it only need be sufficient to allow a finder of fact to determine that the document is authentic. Electronic evidence is often authenticated by testimony from a witness with first-hand knowledge of its creation or use.¹²⁵ However, Rule 901(b) provides a non-exhaustive list of ways to authenticate evidence, several of which can be used to authenticate electronic evidence.¹²⁶ For example, Rule 901(b)(4) provides that evidence can be authenticated by its “distinctive characteristics,” meaning its “[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.”¹²⁷ Additionally, Rule 901(b)(9) provides that evidence, such as database records, can be authenticated if the proponent “describe[s] a process or system used to produce a result and show[s] that the process or system produces an accurate result.”¹²⁸

Resourceful lawyers can authenticate electronic evidence in other ways. For example, many computer applications assign a unique digital alphanumeric code to each file, commonly known as a hash value.¹²⁹ If files do not already contain hash values, a producing party may assign them before producing the documents. By knowing the hash value assigned to a particular file, a party can find an exact duplicate of the file and authenticate it by its unique digital “fingerprint.”¹³⁰ Alternatively, a proponent of electronic evidence can try to authenticate electronic evidence through its metadata.¹³¹ Certain types of metadata—such as the file name, location, and date of creation or modification—may reflect “distinctive characteristic[s]” of the document and help authenticate it pursuant to Rule 901(b)(4).¹³² Moreover, some electronic evidence can be authenticated without any extrinsic evidence. Rule

124. FED. R. EVID. 901(a).

125. *See, e.g.*, *United States v. Tropeano*, 252 F.3d 653, 661 (2d Cir. 2001) (permitting authentication of audio tapes by testimony of participants in conversation).

126. FED. R. EVID. 901(b).

127. *Id.* 901(b)(4).

128. *Id.* 901(b)(9).

129. Craig Ball, *In Praise of Hash*, LAW TECH. NEWS, Nov. 2006, http://www.lawtechnews.com/r5/showkiosk.asp?listing_id=1272201&category_id=27902. *See also* *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 547 (D. Md. 2007) (suggesting that hash values can be used to identify the final or legally operative version of an electronic file).

130. *See* Ball, *supra* note 129.

131. For a definition of metadata, *see supra* note 16.

132. *Lorraine*, 241 F.R.D. at 547–48.

902(7) provides that evidence is self-authenticating if it contains “[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.”¹³³ Arguably, electronic signatures or a distinctive email address may provide sufficient evidence to authenticate an email.¹³⁴

B. Hearsay

Electronic evidence is also subject to challenge under the hearsay rule. Rule 801 defines hearsay as a “statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.”¹³⁵ For hearsay analysis of electronic evidence, the threshold issue is whether the evidence reflects a “statement.”¹³⁶ A “statement” refers to certain acts by a “declarant,” who must be a human being, not a computer.¹³⁷ Some computer-generated information, such as the date and time stamp on an email, should not be considered a “statement” by a “declarant.”¹³⁸ In general, most computer-generated records arguably do not constitute hearsay. Thus, the hearsay rule—which is designed to ensure that the finder of fact hears evidence from witnesses who are under oath and subject to cross-examination—does not apply to many types of electronic evidence.

The hearsay rule also does not apply if the proponent does not introduce the document for the truth of the matter asserted.¹³⁹ Therefore, if electronic evidence has evidentiary value for other purposes, such as to show the relationship between individuals or a party’s state of mind or motive, it is not hearsay.¹⁴⁰ Given the informality of emails, instant messages (IMs), and text messages, elec-

133. FED. R. EVID. 902(7).

134. See *Superhighway Consulting, Inc. v. Techwave, Inc.*, No. 98 CV 5502, 1999 WL 1044870, at *2 (N.D. Ill. Nov. 16, 1999); 5 JACK B. WEINSTEIN & MARGARET A. BERGER, *WEINSTEIN’S FEDERAL EVIDENCE* § 900.07[3][c][i] (Joseph M. McLaughlin, ed., 2d ed. 1997) (claiming that corporate identification on email may be sufficient to self-authenticate email).

135. FED. R. EVID. 801.

136. *Id.* 801(a) (“A ‘statement’ is (1) an oral or written assertion or (2) non-verbal conduct of a person, if it is intended by the person as an assertion.”).

137. *Id.* 801(b) (“A ‘declarant’ is a person who makes a statement.”).

138. See, e.g., *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 564–65 (D. Md. 2007) (citing cases in which electronic evidence was not considered a “statement”).

139. 2 GEORGE E. DIX ET AL., *McCORMICK ON EVIDENCE* § 249 (Kenneth S. Brown ed., 6th ed. 2006).

140. *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000) (finding that emails showing parties’ relationship and custom of communicating by email were not hearsay); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d

tronic evidence often expresses people’s emotions and reactions, and parties may seek to admit them regardless of whether they are true.

Even if electronic evidence contains hearsay, various hearsay exceptions may apply. The most commonly litigated exception is the business records rule.¹⁴¹ Generally, electronic evidence can qualify as a business record if the proponent can show that (1) it was entered at or near the time of the events it records; (2) by a person with personal knowledge of the event or a business duty to transmit the information; (3) prepared in the ordinary course of business; and (4) it was the business’s regular practice to make the electronic record.¹⁴²

To admit emails as business records, the proponent must show that it was the company’s regular practice to keep and retain this information via email.¹⁴³ Because emails often contain a combination of idle chatter, party admissions, and hearsay, parties must be precise about which parts of emails constitute business records. Indeed, some courts have been reluctant to admit emails that appear to be merely self-serving records.¹⁴⁴ Furthermore, hearsay issues can be particularly difficult in email chains. Some courts have required that every email in an email chain must independently meet the requirements of Rule 803(b)(6).¹⁴⁵ In any event, if the business records rule does not apply to emails and IMs, parties can try to admit them under the present sense impression or excited utterance exceptions.¹⁴⁶ However, to satisfy these exceptions to the hearsay rules, such messages must have been written immediately

1146, 1155 (C.D. Cal. 2002) (holding that printouts from website introduced to show instances of copyright infringement were not hearsay).

141. FED. R. EVID. 803(6).

142. *Id.*

143. See *United States v. Ferber*, 966 F. Supp. 90, 98 (D. Mass. 1997).

144. *Gamber-Johnson, L.L.C. v. Trans Data Net Corp.*, No. 01-0543-FT, 2001 WL 869352, at *1 (Wis. Ct. App. 2001) (unpublished table decision) (excluding email that contained self-serving statement of company’s position).

145. *Rambus Inc. v. Infineon Tech. AG*, 348 F. Supp. 2d 698, 706 (E.D. Va. 2004) (noting that “each participant in the chain which created the record—from the initial observer-reporter to the final entrant—must generally be acting in the course of the regularly conduct[ed] business” (quoting 5 WEINSTEIN & BERGER, *supra* note 134, § 803.08[2])).

146. See *Ferber*, 966 F. Supp. at 99 (finding that an email qualified as a present sense expression under Rule 803(1), but did not qualify as an excited utterance under Rule 803(2)).

after witnessing an event or while under the stress caused by a startling event.¹⁴⁷

C. Best Evidence

Subject to certain exceptions, the best evidence rule requires that a party introduce an original writing or recording to prove its contents.¹⁴⁸ However, an important exception precludes the application of this rule to most electronic evidence. Rule 1001(3) provides that if “data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original.’”¹⁴⁹ Because of this exception, few, if any, reported decisions have discussed serious challenges to electronic records under the best evidence rule. This exception is based on practical considerations—it would not be realistic to expect parties to introduce servers or hard drives into evidence if the data could not be used or understood by jurors without viewing a printout or a screen.

The Federal Rules of Evidence also contain other provisions that may exclude electronic evidence from the ambit of the best evidence rule. For example, Rule 1004 provides, in part, that an original record is not required if the original was lost or destroyed (unless it was destroyed in bad faith by the proponent) or if the original cannot be obtained by judicial process.¹⁵⁰ This exception may apply to electronic evidence if the original computer records may not be readily available, which is often the case for IMs and other ephemeral electronic data.¹⁵¹

147. To admit evidence under the present sense impression exception (1) the declarant must have personally perceived the event described; (2) the declaration must be an explanation or description of the event rather than a narration; and (3) the declaration and the event described must be contemporaneous. 5 WEINSTEIN & BERGER, *supra* note 134, § 803.03; 2 GEORGE E. DIX ET AL., MCCORMICK ON EVIDENCE § 271 (Kenneth S. Brown ed., 6th ed. 2006). Similarly, to admit evidence as an excited utterance, the proponent must demonstrate (1) a startling occasion; (2) a statement relating to the circumstances of the startling occasion; (3) a declarant who appears to have had opportunity to observe personally the events; and (4) a statement made before there has been time to reflect and fabricate. See 6 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 1750 (James H. Chadbourne rev., 1976).

148. FED. R. EVID. 1002.

149. *Id.* 1001(3).

150. *Id.* 1004(1).

151. *Bidbay.com, Inc. v. Spry*, No. B160126, 2003 WL 723297, at *7 (Cal. Ct. App. Mar. 4, 2003) (suggesting that chat room messages would qualify as exceptions to best evidence rule).

VI. CONCLUSION

The technological explosion that has caused the creation of exabytes of data each year creates numerous challenges for litigants and the courts. The 2006 amendments to the FRCP reflect one attempt to address just *some* of those challenges in the limited context of federal civil cases. However, technological and legal challenges for litigants and the courts continue to become both more complicated and more significant to the discovery process.

Litigants will continue to face challenges simply from the amount of new data being created. One significant challenge that parties and the courts continue to address is the common law duty to preserve, including the question of when the duty arises and the scope of the duty.¹⁵² Implementing a program to identify and preserve data once the duty to preserve arises is referred to as a “legal hold.”¹⁵³ The Sedona Conference issued a Commentary on Legal Holds to provide some guidance in this area,¹⁵⁴ but there continues to be considerable uncertainty regarding when the duty to preserve is triggered and the appropriate scope of the duty to preserve.

The amended Rules are limited in application to federal civil cases. Even among federal district courts¹⁵⁵ and among state

152. See, e.g., *In re Intel Corp. Microprocessor Antitrust Litig.*, Civ. No. 05-441-JJF, Civ. No. 05-485-JJF, MDL No. 05-1717-JJF, 2008 WL 2310288 (D. Del. June 4, 2008) (adopting Special Master’s Report and Recommendation granting motion to compel Intel to produce notes of counsel’s notes of designated employee interviews concerning preservation compliance); Report and Proposed Remediation Plan of Intel Corp. and Intel Kabushiki Kaisha to Special Master Pursuant to March 16, 2007 Order re Intel’s Evidence Preservation Issues, *Intel*, 2008 WL 2310288 (Civ. No. 05-441-JJF, Civ. No. 05-485-JJF, MDL No. 05-1717-JJF); *In re Flash Memory Antitrust Litig.*, No. C-07-00086-SBA, 2008 WL 1831668, at *1 (N.D. Cal. Apr. 22, 2008) (“All parties and their counsel are reminded of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data, and tangible things in the possession, custody and control of the parties to this action, and any employees, agents, contractors, carriers, bailees, or other non-parties who possess materials reasonably anticipated to be subject to discovery in this action. . . . Until the parties reach an agreements [sic] on a preservation plan or the Court orders otherwise, each party shall take reasonable steps to preserve all documents, data, and tangible things containing information potentially relevant to the subject mater [sic] of this litigation. In addition, counsel shall exercise all reasonable efforts to identify and notify parties and non-parties of their duties, including employees of corporate or institutional parties, to the extent required by the Federal Rules of Civil Procedure.”).

153. See THE SEDONA CONFERENCE, *supra* note 18, at 1.

154. See *id.*

155. At least thirty-eight district courts have issued local rules or guidelines regarding ESI. See Electronic Discovery Law, Updated List: Local Rules, Forms and

courts,¹⁵⁶ however, ESI is treated in varying ways. Fortunately, the Sedona Conference, although not legally binding, has been cited by federal and state courts analyzing ESI discovery issues¹⁵⁷ and may continue to provide a framework as litigants and courts continue to confront challenges where no rules have been enacted. For example, ESI may be relevant in criminal cases, but there are no rules providing guidance on document production in such instances.¹⁵⁸

Moreover, the global nature of data is also a challenge. Parties may need to produce data that currently is found in other countries, where that data is subject to different rules regarding privilege and privacy. With the growth of outsourced operations and worldwide computer facilities, litigants in an increasing number of cases will have to face these access and privacy constraints. The global nature of electronic data will make it more difficult to determine which vendors, consultants, or affiliated entities are under a party's "control" and therefore the subject of discovery under Rule 26.¹⁵⁹

Litigants also will face technical challenges in searching and/or reviewing the increasing amount of ESI. The amendments to the FRCP do not directly address the challenges of keyword searching,¹⁶⁰ multilingual ESI sets,¹⁶¹ and ephemeral data sources.¹⁶² The

Guidelines of United States District Courts Addressing E-Discovery Issues, <http://www.ediscoverylaw.com/2008/02/articles/resources/updated-list-local-rules-forms-and-guidelines-of-united-states-district-courts-addressing-ediscovery-issues/print.html> (last visited June 21, 2008).

156. At least fifteen states have issued rules regarding ESI. See Electronic Discovery Law, Current Listing of States That Have Enacted E-Discovery Rules, *available at* <http://www.ediscoverylaw.com/2008/01/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules/print.html> (last visited June 21, 2008).

157. A search on Westlaw databases conducted March 17, 2008 found 20 such cases.

158. See *United States v. O'Keefe*, 537 F. Supp. 2d 14, 19 (D.D.C. 2008) (noting that "it is far better to use these [Federal Rules of Civil Procedure] than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems" and granting motion to compel).

159. See, e.g., Erica M. Davila, *International E-Discovery: Navigating the Maze*, 8 U. PITT. J. TECH. L. & POL'Y 5 (2008), <http://tlp.law.pitt.edu/ARTICLES/e-discovery.pdf>; Stephanie J. Fogel & Lauren E. Bishow, *Multinationals Take a Global View of EDD*, LEGAL INTELLIGENCER (Penn.), Sept. 26, 2007, *available at* <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1190745422237>; Jerry F. Barbanel & Daryk Rowland, *Navigating the Complexities of U.S.-E.U. Data Protection and Electronic Discovery Issues*, METRO. CORP. COUNS., Dec. 2007, at 23.

160. Jeffrey Gross, *Comparing the Utility of Keyword and Concept Searches*, 7 Digital Discovery & e-Evidence (BNA) 188 (Sept. 1, 2007), http://ddee.bna.com/subscribers/All.Issues/ps2k_ddee-not_20071201.pdf.

161. See, e.g., Ari Kaplan, *A Primer on Foreign Language E-Discovery*, LEGAL TECH., May 23, 2008, *available at* <http://www.law.com/jsp/legaltechnology/PubArticleFriendlyLT.jsp?id=1202421621436>.

increased volume of electronic discovery will put further economic pressure on the cost of conducting privilege reviews.

Finally, some of the 2007 cases reflect the challenges faced by clients, outside counsel, and vendors working on ESI productions, and it is likely that those challenges will continue.¹⁶³ As the complexity and volume of electronic data and the technology needed to capture, process, review, and produce the data become more complex, more individuals, including clients, information systems departments, in-house counsel, outside counsel, vendors and forensic experts, may be needed in any given case. Coordination of ESI teams will become an important factor in many cases.

These challenges will continue to be addressed by individual magistrates and judges in the context of cases or in a court's standing orders. Some jurisdictions may attempt to address them through local rules. Various organizations, such as the ABA, the Sedona Conference, and state ethics committees, may continue to offer guidance on best practices. Nonetheless, litigants will continue to confront huge volumes of data and uncertainty regarding how individual courts, administrative tribunals, and arbitrators will apply guidance from the amended FRCP or any of the other sources discussed herein.

Although there are many uncertainties, companies can take steps to address the huge volumes of data that may one day be sought as relevant for purposes of discovery. Companies can proactively and prospectively assess their information policies in view of the FRCP to understand their data, how it is generated, used, stored, and retrieved. Once a company is involved in litigation, it should begin to work immediately and closely with litigation counsel to prepare for the conference required pursuant to FRCP 16, and to create a discovery plan that addresses the scope and form of ESI production. The amended Rules require these issues to be ad-

162. *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJX, 2007 WL 2080419 (C.D. Cal. May 29, 2007) (random access memory); see also Jerry F. Barbanel and Bruce W. Pixley, *Looking Beyond E-mail: Alternate Forms of Communication and Their Impact on Electronic Discovery*, METRO. CORP. COUNS., Nov. 2007, at 44.

163. See, e.g., *PSEG Power New York, Inc. v. Alberici Constructors, Inc.*, No. 1:05-CV-657 (DNH/RFT), 2007 WL 2687670, at *11 (N.D.N.Y. Sept. 7, 2007) (ordering reproduction of ESI at party's expense where vendor separated attachments from emails); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, No. 502003CA0050-45XXOCAI, 2005 WL 679071 (Fla. Cir. Ct. March 1, 2005); Susan Beck, *Morgan Stanley's Recipe for Disaster*, AM. LAW., Apr. 2006, at 88; Ben Hallman, *Software Glitch May Have Erased E-Mail Text in Enron Suits*, AM. LAW., Aug. 10, 2006; Anthony Lin, *Sullivan & Cromwell, E-Discovery Vendor Settle Lawsuits*, N.Y. L.J., Jan. 18, 2008; Scott Nagel, Letter to the Editor, AM. LAW., Aug. 11, 2006.

dressed at the conference.¹⁶⁴ Indeed, early attention to such issues is one of the effective ways to reach agreements to limit production (for example, excluding production from backup tapes), to use keyword searching, or to produce in imaged, static formats.

Based on the dizzying array of recent developments in the areas of electronic discovery, Judge Teece, writing the decision in the *PSEG Power* case, summarized the challenges that are ahead: “With the rapid and sweeping advent of electronic discovery, the litigation landscape has been radically altered in terms of scope, mechanism, cost, and perplexity.”¹⁶⁵ Litigation has been proceeding under the amended Rules for over a year now. But they are only the beginning, and the amendments reflect what may be later viewed as one of the first steps taken by the legal world to adapt to the electronic age.

164. FED. R. CIV. P. 26(f).

165. *PSEG*, 2007 WL 2687670, at *1.