6-1-2005

III. Scope of Electronic Discovery and Methods of Production

Ophir D. Finkelthal

III. SCOPE OF ELECTRONIC DISCOVERY AND METHODS OF PRODUCTION*

A. Introduction

With approximately 90% of documents now originating in electronic form,[1] "electronic discovery has moved from an unusual activity encountered in large cases to a frequently-seen activity . . . ."[2] Thus, understanding the challenges and defining the scope of electronic discovery and production has become ever more critical for attorneys and courts.

For instance, attorneys and their clients need to grapple with practical issues related to the volume, format, and platforms of electronic documents. "The sheer volume of [electronic] data, when compared with conventional paper documentation, can be staggering. . . . A CD-ROM, with 650 megabytes, can hold up to 325,000 typewritten pages. . . . [C]orporate computer networks create backup data measured in terabytes . . . [. E]ach terabyte represents the equivalent of 500 billion typewritten pages of plain text."[3] The

---

* Ophir D. Finkelthal: J.D. Candidate, May 2006, Loyola Law School; B.A., Yale College. I thank the editors and staff of the *Loyola of Los Angeles Law Review* for their invaluable assistance with and support of this project. Special thanks go to Chief Developments Editor Heather R. Barber for her insight and encouragement. I also thank my mother for her love and support, and I dedicate this chapter to the memory of my father, Irmin Finkelthal.

1. *In re* Bristol-Myers Squibb Sec. Litig., 205 F.R.D 437, 440 n.2 (D.N.J. 2002) ("According to a University of California study, 93% of all information generated during 1999 was generated in digital form, on computers." (quoting Kenneth J. Withers, Electronic Discovery: The Challenges and Opportunities of Electronic Evidence, Address at the National Workshop for Magistrate Judges, San Diego, Cal. (July, 24 2001))).

2. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE UNITED STATES, REPORT OF THE CIVIL RULES ADVISORY COMMITTEE 2 (2004) [hereinafter REPORT OF THE CIVIL RULES ADVISORY COMMITTEE], http://www.uscourts.gov/rules/comment2005/CVAug04.pdf.

3. *Id.* at 3 (quoting MANUAL FOR COMPLEX LITIGATION § 11.446 (4th ed. 2004)).

breadth of formats of discoverable electronic documents has been described as including:

> [V]oice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information.[4]

Platforms that might be searched for volumes of these types of electronic data include databases, servers, networks, existing and legacy computer software and hardware systems, archives, backup and disaster recovery systems, storage media such as tapes and discs, laptops, personal computers, internet data, personal digital assistants, mobile phones, pagers and other handheld wireless devices, and voice messaging and other audio systems.[5] Further, production may be requested in paper, original electronic format, or both and may need to be delivered in a searchable format and/or accompanied by "the software necessary to retrieve, read or interpret electronic information."[6]

This part addresses the challenges posed by electronic discovery and production[7] and highlights how it differs from traditional

---

4. Super Film of Am., Inc. v. UCB Films, Inc., 219 F.R.D. 649, 657 (D. Kan. 2004) (quoting Kleiner v. Burns, 48 Fed. R. Serv. 3d (West) 644, 649 (D. Kan. 2000); *see also* AM. BAR ASS'N, REPORT 103B, AMENDMENTS TO CIVIL DISCOVERY STANDARDS 3, 8 (2004) [hereinafter AMENDMENTS TO ABA CIVIL DISCOVERY STANDARDS] (identifying potentially discoverable electronic information formats as e-mail, word processing documents, spreadsheets, presentation documents, graphics, animations, images, audio and/or visual recordings and voicemail), http://www.abanet.org/litigation/documents/hod/ABA%20Final%20Revised%202004%20Amendments%20Civil%20Discovery%20Standards.doc; *supra* Part II.

5. AMENDMENTS TO ABA CIVIL DISCOVERY STANDARDS, *supra* note 4, at 3–4.

6. *Id.* at 4–5.

7. *See* Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1160 (W.D. Tenn. 2003);

> Producing electronic data requires, at minimum, several steps: (1) designing and applying a search program to identify potentially relevant electronic files; (2) reviewing the resulting files for relevance; (3) reviewing the resulting files for privilege; (4) deciding whether the files should be produced in electronic or printed form; and (5) actual

discovery. It notes that the underlying principles of Federal Rule of Civil Procedure (FRCP) 26 still apply to serve as a guide to practitioners grappling with the scope of discovery issues and attendant matters.[8] While the prevailing sentiment is that "[e]lectronic discovery injects difficult, expensive and contentious issues into many otherwise routine disputes,"[9] in the seminal case of *Hickman v. Taylor*[10] Justice Murphy admonished that discovery is a method "to narrow and clarify the basic issues between the parties, and [serve] as a device for ascertaining facts, or information as to the existence or whereabouts of facts, relative to those issues."[11] That discovery is to be construed liberally, yet within "ultimate and necessary boundaries"[12] based on necessity or justification,[13] remains apt nearly 60 years later in the context of electronic discovery.[14] Thus, this part will describe how courts prefer opposing parties to themselves agree upon the scope of electronic discovery and the method of production. It will also describe how the courts have attempted to solve difficult matters of electronic discovery when they have been required to intervene.

Also included is an overview of how courts have ruled on requests for expedited discovery and preservation orders, defined the scope of electronic discovery within each of the two tiers of

---

production.

8. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1007614, at *6 (S.D.N.Y. May 16, 2002) (noting that careful application of the principles behind the existing rules on a case-by-case basis make the rules flexible enough to deal with the special problems created by requests for discovery of electronic data).

9. AM. BAR ASS'N, REPORT 103B, EXECUTIVE SUMMARY TO AMENDMENTS TO CIVIL DISCOVERY STANDARDS (2004), http://www.abanet.org/litigation/documents/hod/4%20Executive%20Summary%202004%20Electronic%20Discovery%20Standards.DOC.

10. Hickman v. Taylor, 329 U.S. 495, 501 (1947).

11. *Id.*

12. *Id.* at 507.

13. *See id.* at 509–10.

14. *See* Bishop v. Hoffmann-LaRoche, Inc., No. 8:02-CV-1533-T-30-TBM, 2003 WL 23728321 (M.D. Fla. Dec. 19, 2003) ("[T]here can be little dispute that electronic information contained in computers used by Charles Bishop prior to his suicide . . . satisfies the broad relevance test of Rule 26(b)(1). Such information is reasonably calculated to lead to the discovery of admissible evidence about . . . the fundamental issue of why [he] crashed [the] plane . . . .").

discovery created by the amendments to FRCP 26 in 2000, defined the method of production of electronic documents, applied the availability of electronic documents to interrogatories, and ruled on requests for sanctions related to failure to produce electronic documents.

B. Preparing for the FRCP 26(f) Conference

With limited exceptions, no discovery can occur before the FRCP 26(f) conference between the parties, except by order of the court.[15] Both plaintiff and defense counsel ought to adopt a pragmatic approach to preparation for the discovery conference and to potential requests for or objections to electronic discovery.[16] Given the technical complexities, there is an interrelationship between how well attorneys have understood their clients' or adversaries' computer systems and requests for electronic discovery throughout the life of a case.[17] In other words, it is advisable for requesting counsel to understand early what efforts the opposing side will need to undertake to produce electronic documents and to decide in what form it would like to receive such documents.[18] Similarly,

---

15. FED. R. CIV. P. 26(d) ("[Timing and Sequence of Discovery.] Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E), or when authorized under these rules or by order or agreement of the parties, a party may not seek discovery from any source before the parties have conferred as required by Rule 26(f).").

16. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1,007,614, at *6 (S.D.N.Y. May 16, 2002) ("As electronic mechanisms for storing and retrieving data have become more common, it has increasingly behooved courts and counsel to become familiar with such methods, and to develop expertise and procedures for incorporating 'electronic discovery' into the familiar rituals of litigation.").

17. *See id.* at *1, *10–*11, *16 (holding that the burden of discovery of information from prison database systems about disease and violence due to double-celling inmates outweighed the benefit where the defendant prison provided a detailed description of the construction and operation of its information systems as well as the disruption and security risks such discovery would create while the plaintiff prisoners claimed such discovery would be simple and cheap without any technical substantiation or grasp of the defendant's database systems).

18. *Cf.* DIST. N.J. R. 26.1(d)(2):

> Duty to Notify. A party seeking discovery of computer-based or other digital information shall notify the opposing party as soon as possible, but no [later] than the Fed. R. Civ. P. 26(f) conference, and identify as clearly as possible the categories of information which may be sought.

attorneys should assess what electronic data their client have, how they were created and saved, and how difficult they will be to produce in anticipation of discovery requests.[19]

Courts prefer that the parties take a pragmatic rather than a combative approach to defining discovery early in the process, as courts prefer not to have to intervene.[20] Further, the duty to preserve potentially discoverable electronic documents may attach as early as when a party could anticipate litigation.[21] The duty to preserve

---

A party may supplement its request for computer-based and other digital information as soon as possible upon receipt of new information relating to digital evidence.

19. *See id.* R. 26.1(d)(1):

Duty to Investigate and Disclose. 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.

20. *See Goord*, 2002 WL 1007614, at *15 ("Parties should be encouraged to work out differences amicably; . . . the spirit of cooperation and informality . . . alone make[] effective discovery and settlement possible in overburdened courts."); *see also* DIST. WYO. R. 26.1(d):

(3) Prior to a Fed. R. Civ. P. 26(f) conference, counsel should carefully investigate their client's information management system so that they are knowledgeable as to its operation, including how information is stored and how it can be retrieved. Likewise, counsel shall reasonably review the client's computer files to ascertain the contents thereof, including archival and legacy data (outdated formats or media), and disclose in initial discovery (self-executing routine discovery) the computer based evidence which may be used to support claims or defenses.

(A) Duty to Notify. A party seeking discovery of computer-based information shall notify the opposing party immediately, but no later than the Fed. R. Civ. P. 26(f) conference of that fact and identify as clearly as possible the categories of information which may be sought.

21. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("The duty to preserve attached at the time that litigation was reasonably

"covers the discoverable information that a party knows or reasonably should know may be relevant to the pending or impending litigation."[22] Thus the duty to preserve does not require a court order.[23] Nonetheless, as electronic documents are more vulnerable to early destruction,[24] courts are plied with requests for orders to compel early discovery and requests for preservation or restraining orders to "freeze" a company's computer system with some frequency, even prior to the Rule 26(f) conference.

1. Requests for Early Discovery

Parties to litigation have greater reason to be concerned about the destruction of documents in the electronic environment.[25] In

---

anticipated. . . . [A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary."); *accord* Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 175 (S.D.N.Y. 2004) (quoting Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001)); Wiginton v. CB Richard Ellis, Inc., No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003); Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 99 (D. Md. 2003) (quoting Silvestri v. Gen. Motors Corp., 271 F.3d 583 (4th Cir. 2001)); Renda Marine, Inc. v. United States, 58 Fed. Cl. 57, 61 (2003). *But see* Danis v. USN Communications, Inc., 53 Fed. R. Serv. 3d (West) 828, 834 (N.D. Ill. 2000) (describing the duty to preserve as beginning on the day litigation commenced).

22. *Danis*, 53 Fed. R. Serv. 3d (West) at 875.

23. *See id.* at 843 (describing the inherent duty to preserve as a common law duty); Arista Records, Inc. v. Sakfield Holding Co., 314 F. Supp. 2d 27, 33 (D.D.C. 2004) ("Defendant's argument that it destroyed crucial evidence [prior to a court order, but after notification that a copyright infringement claim had been made against it,] to prevent further transfer of music files is without doubt one of the most ludicrous arguments ever visited upon this Court in written form."); *Thompson*, 219 F.R.D. at 100 ("While a litigant certainly may . . . seek a court order directing that [an adversary preserve electronic records during the pendency of a case], it is not required, and a failure to do so does not vitiate the independent obligation of an adverse party to preserve such information." (footnote omitted)).

24. *Cf. Convolve*, 223 F.R.D. at 176 ("Since computer systems generally have automatic deletion features that periodically purge electronic documents such as e-mail, it is necessary for a party facing litigation to take active steps to halt that process.")

25. *See* Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 650–51 (D. Minn. 2002) (noting that the plaintiff requested expedited discovery and an order to compel early discovery of electronic documents prior to a Rule 26(f) conference in addition to the court's order admonishing the defendant to preserve paper and electronic documents because "data from a computer which

some instances, the parties "stipulate [to a] protective order prohibiting the destruction of discoverable [electronic] evidence by either party" thus adding a layer of court protection to an agreement negotiated between themselves.[26] In other instances, the discovering party asks the court for expedited discovery prior to the Rule 26(f) conference.[27]

One court granted such expedited discovery "to ensure that computer records [were] preserved."[28] It also assured the producing party that while "discovery [would] commence earlier than would usually be the case,"[29] it would have the usual amount of time under the Federal Rules to respond to discovery.[30] To ensure the effectiveness of expedited discovery, a court may couple other orders with an order for expedited discovery. For instance, a computer forensics expert could be employed to create a mirror image of the producing party's computer systems.[31] The producing party would then receive a copy of its data to sift through in response to discovery requests in the usual manner, while the requesting party would be assured that the data was protected from destruction as of a certain date.[32] The court might further protect the producing party by instructing the computer forensics expert to "use its best efforts to avoid unnecessarily disrupting the normal activities or business operations of the [producing party] while inspecting, copying, and

---

has been deleted remains on the hard drive, but is constantly being overwritten, irretrievably, by the Defendant's continued use of that equipment").

26. Kleiner v. Burns, 48 Fed. R. Serv. 3d (West) 644, 648 n.4 (D. Kan. 2000).

27. *See Antioch*, 210 F.R.D. at 650–51.

28. *Id.* at 651; *accord* Physicians Interactive v. Lathian Sys., Inc., CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *29–*30 (E.D. Va. Dec. 5, 2003) ("[T]his case presents the Court with unusual circumstances or conditions that would likely prejudice the party if they were required to wait the normal time to initiate discovery. In this case, electronic evidence is at issue. Electronic evidence can easily be erased and manipulated.").

29. *Antioch*, 210 F.R.D. at 651.

30. *Id.*

31. *Id.* at 653–54; *see also Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *30 (granting the plaintiff "limited expedited discovery to enter the sites where the computers used in the alleged [hacking] attacks are located and to obtain a 'mirror image' of the computer equipment containing electronic data relating to Defendants' alleged attacks on [plaintiff]'s file server . . . with the assistance of a computer forensic expert").

32. *See Antioch*, 210 F.R.D. at 653–54.

imaging,"[33] and by allowing the expert and the producing party to access only copies of the entire set of preserved data.[34]

2. Requests for Preservation Order

As with requests for expedited discovery, in the electronic environment requests for preservation orders are rooted in a fear of document destruction.[35] The discovering party may believe that expedited discovery, which does not preclude the producing party from continuing to operate its information systems, does not adequately protect its interests. Thus, the requesting party may ask the court to issue a preservation order that compels the opposing party to halt the use of its computer systems until discovery has been conducted.

a. Reasonableness of request for preservation order

Freezing a company's computer systems can bring its operations to a virtual halt.[36] Thus, courts may choose to issue a preservation order that does not have a tangible component, but rather "reemphasize[s] that documents should not be destroyed and create[s] incentives to ensure that happens."[37] For instance, the court may remind the producing party of "the looming specter of sanctions—which the case law suggests may be severe, to and including the entry of a default judgment."[38]

---

33. *Id.* at 653.

34. *Id.*

35. Dodge, Warren & Peters Ins. Servs. v. Riley, 130 Cal. Rptr. 2d 385, 388 (Ct. App. 2003) ("[Plaintiff] sought to 'freeze' Defendants' electronically stored data so that it would be available for future discovery, if appropriate, and claimed that even Defendants' innocent use of the media could result in the destruction of potential evidence.").

36. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 7–8 ("[T]he volume and dynamic nature of electronically stored information may complicate preservation obligations. . . . Suspension of all or a significant part of that activity could paralyze a party's operations. An overbroad approach to preservation may be . . . unduly burdensome for parties dependent on computer systems for their operations.").

37. Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 140 (2004); *accord* Walker v. Cash Flow Consultants, Inc., 200 F.R.D. 613, 617 (N.D. Ill. 2001).

38. *Pueblo of Laguna*, 60 Fed. Cl. at 141. The court in this case provided an exhaustive definition of types of data that various government agencies must take internal steps to preserve to comply with the preservation order or face sanctions:

Courts have addressed the reasonableness of requests for intrusive preservation in several ways. One test "requires that one seeking a preservation order demonstrate that it is necessary and not unduly burdensome."[39] To prove need, "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."[40] To prove that a request for a preservation order is not overly burdensome, "the proponent must show that the particular steps to be adopted will be effective, but not overbroad—the court will neither lightly exercise its inherent power to protect evidence nor indulge in an exercise in futility."[41]

Other courts view a "motion to preserve evidence [a]s an injunctive remedy and [believe they] should issue [such an order] only upon an adequate showing that equitable relief is warranted."[42] Under this approach, each federal circuit's standard for injunctive relief would govern the review of requests for preservation orders.[43]

> "Documents, data, and tangible things" is to be interpreted broadly to include writings; records; files; correspondence; reports; memoranda; calendars; diaries; minutes; electronic messages; voicemail; E-mail; telephone message records or logs; computer and network activity logs; hard drives; backup data; removable computer storage media such as tapes, disks, and cards; printouts; document image files; Web pages; databases; spreadsheets; software; books; ledgers; journals; orders; invoices; bills; vouchers; checks; statements; worksheets; summaries; compilations; computations; charts; diagrams; graphic presentations; drawings; films; charts; digital or chemical process photographs; video; phonographic tape; or digital recordings or transcripts thereof; drafts; jottings; and notes. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata, is also included in this definition.

Id. at 143.

39. *Id.* at 138.

40. *Id.*

41. *Id.*

42. Madden v. Wyeth, No. 3-03-CV-0167-R., 2003 WL 21443404, at *1 (N.D. Tex. Apr. 16, 2003) (citing Pepsi-Cola Bottling Co. of Olean v. Cargill, Inc., No. 3-95-784, 1995 WL 783610, at *3 (D. Minn. Oct. 20, 1995) (citing Humble Oil and Ref. Co. v. Harang, 262 F. Supp. 39, 42 (E.D. La. 1966))).

43. *Cf. Madden*, 2003 WL 21443404, at *1 ("In the Fifth Circuit, a party must establish a substantial threat of irreparable harm in order to obtain an injunction. Plaintiffs have made no such showing [in their motion to preserve

In other instances, the plaintiff's request for intrusive court action may take the form of an ex parte request for a temporary restraining order.[44] "Restraining order applications sought *ex parte* require the court to serve as the absent party's advocate, triggering intense judicial scrutiny of a plaintiff's claims, the relief it seeks, and most importantly, its proffered justification for proceeding *ex parte*."[45] There are generally two situations in which a court may issue a temporary restraining order.[46] "First, a plaintiff may obtain *ex parte* relief by showing that it is impossible to give notice to the adverse party because the plaintiff does not know the party's identity or location."[47] It is not likely that a plaintiff will be able to assert this rationale for a restraining order where the request relates to freezing or seizing the defendant's computer systems, because the plaintiff probably needs to explain the threat to electronic documents that would justify such an extreme order with some specificity that can only come through knowledge of the defendant.[48] "The second and remaining way a plaintiff may obtain an *ex parte* restraining order is by showing that proceeding *ex parte* is the 'sole method of preserving a state of affairs in which the court can provide effective

---

evidence]." (citations omitted)).

44. FED. R. CIV. P. 65(b):

> A temporary restraining order may be granted without written or oral notice to the adverse party or that party's attorney only if (1) it clearly appears from specific facts shown by affidavit or by the verified complaint that immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or that party's attorney can be heard in opposition, and (2) the applicant's attorney certifies to the court in writing the efforts, if any, which have been made to give the notice and the reasons supporting the claim that notice should not be required.

45. Adobe Sys., Inc. v. S. Sun Prods., Inc., 187 F.R.D. 636, 639 (S.D. Cal. 1999).

46. *Id.*

47. *Id.*

48. *Cf. id.* at 637–39 (finding that the plaintiff software companies' *ex parte* application for a temporary restraining order, where the software companies contended that their claim of copyright infringement by the jeweler could only be proved by impounding the jeweler's computers without warning as otherwise the jeweler could easily delete unlicensed copies of software, did not and could not use lack of knowledge of identity or locale of the defendant jeweler as a basis for obtaining the restraining order because the application did necessarily identify the address and described the personnel and operations of the jeweler).

final relief,'"[49] which may be proved by the related showing that notice to the defendant "would 'render fruitless further prosecution of the action.'"[50] The plaintiff's burden under this criterion is to do more than merely allege that electronic evidence is easy to destroy.[51] To meet its burden, the plaintiff should "present specific facts showing that the defendant it seeks to enjoin will likely conceal, destroy, or alter evidence if it receives notice of the action. A plaintiff may satisfy this burden by identifying specific instances where the defendant has destroyed evidence or willfully violated court orders in the past."[52] The plaintiff may also carry its burden by linking "the defendant with other persons, engaged in similar unlawful activities, who have destroyed evidence or violated court orders in the past."[53]

Overall, it appears that lawyers should have some understanding of the opposing party's business operations and/or information systems in order to fashion a request for an intrusive order with specificity, and a defined rationale that the court can understand and find credible.[54] It is also suggested that the parties ought to confer

---

49. *Id.* at 639.

50. *Id.* at 643.

51. *See id.* at 641:

> Once notified, a defendant can erase its computer disks, burn, shred, or hide incriminating documents, and intimidate or coach potential witnesses. This opportunity presents itself to defendants in all civil cases, from high stakes technology disputes to routine personal injury and small claims actions. The extraordinary remedy of *ex parte* injunctive relief cannot be justified by merely pointing to the obvious opportunity every defendant possesses to engage in such unlawful deceptive conduct.

52. *Id.*

53. *Id.*

54. *See* Madden v. Wyeth, No. 3-03-CV-0167-R., 2003 WL 21443404, at *1 (N.D. Tex. Apr. 16, 2003) (denying the plaintiff's motion to preserve evidence, specifically the requests that the defendant "preserve all documents and information, whether in paper or electronic format . . . and [] suspend all routine destruction of documents, including but not limited to recycling back-up tapes, automated deletion of e-mail, and reformatting computer hard drives" because the plaintiffs offered no proof that the defendants would spoliate beyond a general assertion that the "defendants and their agents may intentionally or unintentionally destroy relevant documents"); *Adobe Sys.*, 187 F.R.D. at 642–43 (rejecting an unsupported assertion by the plaintiff software companies that the defendant jeweler could destroy electronic evidence of unlicensed software use with a few keystrokes and clicks of a mouse because

amongst themselves before involving the court. Just as with paper discovery, FRCP 26 is meant to assist the parties in accomplishing discovery and production without resort to intrusive orders by the court.[55]

b. Knowledge of a client's computer systems

The earlier a lawyer understands the client's computer environment, the more likely a court will be to find that the party met its inherent duty to preserve and decline a request for a preservation order from the other party. Adequate measures for preservation of electronic documents include a clear policy regarding critical electronic documents, backup sources of documents, proof that key personnel are aware of and are implementing such policies and that otherwise critical potentially discoverable documents are not subject to spoliation by a computer simply being booted up or accessed.[56] Knowledge of how information systems operate and implementation of solid internal document retention policies also play a role in the court's view on spoliation[57] and sanctions.[58]

---

the court's research found that it is generally difficult to completely erase electronic evidence).

55. *See* Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 140, 142 (2004) (instructing the litigants, where the court had entered a preservation order that only reminded the parties of the inherent duty to preserve discoverable documents, to meet, confer and submit a mutually agreeable plan for a proposed court order on discovery matters to include "whether indexation will require suspending or modifying any routine processes or procedures, with special attention to document-management programs and the recycling of computer data storage media"). *See also infra* Part III.C.

56. *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218–19 (S.D.N.Y. 2003) (footnotes omitted):

> By its attorney's directive in August 2002, UBS endeavored to preserve all backup tapes that existed in August 2001 (when Zubulake filed her EEOC charge) that captured data for employees identified by Zubulake in her document request, and all such monthly backup tapes generated thereafter. These backup tapes existed in August 2002, because of UBS's document retention policy, which required retention for three years. In August 2001, UBS employees were instructed to maintain *active* electronic documents pertaining to Zubulake in separate files. Had these directives been followed, UBS would have met its preservation obligations by preserving one copy of all relevant documents that existed at, or were created after, the time when the duty to preserve attached.

57. *See infra* Part VII.

C. The FRCP 26(f) Conference, Mandatory Disclosure and Court Orders Regarding Electronic Discovery

"[C]ounsel should take advantage of the required Rule 26(f) meeting to discuss issues associated with electronic discovery."[59] The discovery rules mandate a conference between the parties to prompt the settlement of discovery matters amongst themselves, provide the standard relevant to a claim or defense as the baseline for determining the scope of discovery, and require the parties' submission of a discovery plan prior to the court issuing a scheduling order.[60] As reflected in the proposed amendments to FRCP 26(f) and

---

58. *See* Danis v. USN Communications, Inc., 53 Fed. R. Serv. 3d (West) 828 (N.D. Ill. 2000) (granting the part of the plaintiff's motions for sanctions that requested a jury instruction indicating that gaps in production of documents are attributable to the defendant telecommunications company, and fining the company's CEO where the defendants did not adequately discharge the duty that arose on the date litigation commenced to preserve discoverable, primarily electronic, documents due to a lack of decisive steps to adequately implement the defendant company's internal document retention policy and the defendants' lack of understanding of the uses, significance or method of generation of its own documents, but denying the sanction of default judgment); *see also* Metro. Opera Ass'n v. Local 100, Hotel Employees & Rest. Employees Int'l Union, 212 F.R.D. 178, 190, 220–231 (S.D.N.Y. 2003) (granting plaintiff's motion for liability against defendant among other sanctions due to defendant's discovery abuses that included lack of electronic document retention policy and a lack of understanding of automatic e-mail deletion among other failures), *adhered to by* 00 Civ. 3613 (LAP), 2004 U.S. Dist. LEXIS 17093 (Aug. 27, 2004); *infra* Part VII; *infra* Part III.G.

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

60. FED. R. CIV. P. 26(f):

> [Conference of Parties; Planning for Discovery.] Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:
>
> (1) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;
>
> (2) the subjects on which discovery may be needed, when

the ABA discovery standards, the ideal contemporary discovery conference includes a broad discussion of electronic discovery issues, including preservation, strategies for determining the scope of discovery, an attempt to make the scope of discovery determination, and the form production will take.[61] One court summarized the

---

> discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;
>
> (3) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and
>
> (4) any other orders that should be entered by the court under Rule 26(c) or under Rule 16(b) and (c).
>
> The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. A court may order that the parties or attorneys attend the conference in person. If necessary to comply with its expedited schedule for Rule 16(b) conferences, a court may by local rule (i) require that the conference between the parties occur fewer than 21 days before the scheduling conference is held or a scheduling order is due under Rule 16(b), and (ii) require that the written report outlining the discovery plan be filed fewer than 14 days after the conference between the parties, or excuse the parties from submitting a written report and permit them to report orally on their discovery plan at the Rule 16(b) conference.

61. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 6:

> Under the proposed amendments to Rule 26(f), the parties are to address during their conference any issues relating to the disclosure or discovery of electronically stored information, including the form of production, and also to discuss issues relating to the preservation of electronically stored information . . . . The results of these discussions are to be included, as appropriate, in the discovery plan presented to the court.

AMENDMENTS TO ABA CIVIL DISCOVERY STANDARDS, *supra* note 4, at 12–13, provides a more thorough best practices description of the matters counsel ought to address in an electronic world:

> [Standard] 31. Discovery Conferences.
>
> a. At the initial discovery conference, the parties should confer about any electronic discovery that they anticipate requesting from one another, including:
>
> i. The subject matter of such discovery.
>
> ii. The time period with respect to which such discovery may be sought.

iii. Identification or description of the party-affiliated persons, entities or groups from whom such discovery may be sought.

iv. Identification or description of those persons currently or formerly affiliated with the prospective responding party who are knowledgeable of the information systems, technology and software necessary to access potentially responsive data.

v. The potentially responsive data that exist, including the platforms on which, and places where, such data may be found as set forth in Standard 29 (a).

vi. The accessibility of the potentially responsive data, including discussion of software, hardware or other specialized equipment that may be necessary to obtain access.

vii. Whether potentially responsive data exist in searchable form.

viii. Whether potentially responsive electronic data will be requested and produced:

A. In electronic form or in hard copy, and

B. If in electronic form, the format in which the data exist or will be produced

ix. Data retention policies applicable to potentially responsive data.

x. Preservation of potentially responsive data, specifically addressing (A) preservation of data generated subsequent to the filing of the claim, (B) data otherwise customarily subject to destruction in ordinary course, and (C) metadata reflecting the creation, editing, transmittal, receipt or opening of responsive data.

xi. The use of key terms or other selection criteria to search potentially responsive data for discoverable information.

xii. The identity of unaffiliated information technology consultants whom the litigants agree are capable of independently extracting, searching or otherwise exploiting potentially responsive data.

xiii. Stipulating to the entry of a court order providing that production to other parties, or review by a mutually-agreed independent information technology consultant, of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection.

xiv. The appropriateness of an inspection of computer systems, software, or data to facilitate or focus the discovery of electronic data.

xv. The allocation of costs.

b. At any discovery conference that concerns particular requests for electronic discovery, in addition to conferring about the topics set forth in subsection (a), the parties should consider, where appropriate, stipulating to the entry of a court order providing for:

i. The initial production of tranches or subsets of potentially responsive data to allow the parties to evaluate the likely benefit

judiciary's preference to issue a discovery order that closely mirrors an agreement worked out by the parties and that addresses electronic discovery:

> [Fed. R. Civ. P.] 26(f) provides that before a Rule 16 Conference, the parties "confer . . . to develop a proposed discovery plan . . . ." In the electronic age, this *meet and confer* should include a discussion on whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing . . . . Moreover, the standard initial scheduling order in this District contains instructions on topics to be discussed in the preparation of a Joint Discovery Plan which include "(3) a description of all discovery problems encountered to date, the efforts undertaken by the parties to remedy these problems, and the parties' suggested resolution of problems; (4) a description of the parties' further discovery needs."[62]

Indeed, the local rules of several districts direct the parties to consider electronic discovery,[63] as do the Proposed Amendments to

---

> of production of additional data, without prejudice to the requesting party's right to insist later on more complete production.
>
> ii. The use of specified key terms or other selection criteria to search some or all of the potentially responsive data for discoverable information, in lieu of production.
>
> iii. The appointment of a mutually-agreed, independent information technology consultant pursuant to Standard 32(a) to:
>
> A. Extract defined categories of potentially responsive data from specified sources, or
>
> B. Search or otherwise exploit potentially responsive data in accordance with specific, mutually-agreed parameters.

62. *Bristol-Myers Squibb*, 205 F.R.D at 443–44.

63. DIST. N.J.R. 26.1.

> (b)(2) The parties shall submit their Fed. R. Civ. P. 26(f) discovery plan containing the parties' views and proposals regarding the following:
>
> . . . .
>
> [(b)(2)](d) Whether any party will likely request or produce computer-based or other digital information, and if so, the parties' discussions of the issues listed under the Duty to Meet and Confer in L. Civ. R.

the Rules of Civil Procedure.[64] When the parties fail to reach an agreement and submit a discovery plan with competing proposals for electronic discovery, however, the court is left to resolve those discovery problems and determine the practical scope of discovery.[65]

1. Emergency Requests for Electronic Material

Sometimes a party will make an emergency request, after discovery has begun, for a preservation order[66] or motion to

---

26.1(d)(3) below;

. . . .

[(b)(2)](g) Any orders, such as data preservation orders, protective orders, etc., which should be entered;

. . . .

(d) Discovery of Digital Information Including Computer-Based Information;

. . . .

[(d)](3) Duty to Meet and Confer. During the Fed. R. Civ. P. 26(f) conference, the parties shall confer and attempt to agree on computer-based and other digital discovery matters, including the following:

[(3)](a) Preservation and production of digital information; procedures to deal with inadvertent production of privilged information; whether restoration of deleted digital information may be necessary; whether back up or historic legacy data is within the scope of discovery; and the media, format, and procedures for producing digital information;

[(3)](b) Who will bear the costs of preservation, production, and restoration (if necessary) of any digital discovery.

See also E. DIST. & W. DIST. ARK. R. 26.1(4); DIST. WYO. LOCAL CIV. R. 26.1(d)(3)(B).

64. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE *supra* note 2, app. 8–9 (proposed amendment to Rule 26(f)):

> the parties must . . . confer . . . *to discuss any issues relating to preserving discoverable information*, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:
>
> . . . .
>
> *(3) any issues relating to disclosure or discovery of electronically stored information, including the form in which it should be produced*

(proposed amendments italicized).

65. *See id.* at 1–2 (FED. R. CIV. P. 16(b) "[Scheduling and Planning]. . . . The [court-entered] scheduling order may also include (4) modifications of the times for disclosures under Rules 26(a) and 26(e)(1) and of the extent of discovery to be permitted; *(5) provisions for disclosure or discovery of electronically stored information.*" (proposed amendment italicized)).

66. In *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 430–31 (W.D. Pa. 2004), both the defendant and the plaintiff filed

compel.[67] For instance, a plaintiff may be "dissatisfied with the results of the discovery process and suspect[] that [the] defendants possess more information than they have produced."[68] As with such motions prior to the discovery conference, the requesting party must have some specific rationale to warrant the intrusion[69] and demonstrate some level of sophistication in regards to information systems.[70]

---

motions for the preservation of "Documents, Software and Things" after a mistrial. The court devised its own test to determine whether a preservation order was warranted:

> An evaluation of a motion for a preservation order therefore demands application of a separate and distinct test, which can be formulated by molding the factors used in granting injunctive relief with the considerations, policies and goals applicable to discovery. . . . [T]his Court believes that a balancing test which considers the following three factors should be used when deciding a motion to preserve documents, things and land: 1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; 2) any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and 3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.

Id. at 433–34 (footnote omitted).

67. Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 644, 645, 651 (S.D. Ind. 2000).

68. Bethea v. Comcast, 218 F.R.D. 328, 329 (D.D.C. 2003).

69. *See Simon Prop. Group*, 194 F.R.D. at 651:

> In separate rulings on plaintiff's initial motion to compel, the court has established an inspection process for the hard drives and other memories of computers used by mySimon and its senior leaders. That process will culminate in defendant supplementing its document production. The court expects that process to address sufficiently the issues raised [in this emergency motion to compel] with respect to electronic mail discovery. To the extent plaintiff seeks additional relief on this topic, that request is denied.

70. *See Bethea*, 218 F.R.D. at 330:

> [P]laintiff seeks to enter defendants' premises and inspect their computer systems merely because they are "believed to contain appropriate discovery information." . . . [P]laintiff is speculating, and such conjecture does not warrant the compelled inspection of a computer system that contains voluminous information relating to many topics other than plaintiff's employment discrimination claim.

2. Scope of Tier One Discoverable Electronic Documents

"Electronic documents are no less subject to disclosure than paper records."[71] Though broad, the traditional mandatory disclosure requirement of tier one discovery does not mean that any paper document ever written by a party must be disclosed.[72] Thus, electronic discovery within tier one cannot be boundless either.[73] The courts are attempting to define what the scope of tier one electronic discovery should be, sometimes dealing with misconceptions about the ease of searching a party's entire information systems network and the nature of discovering material in legacy systems.[74] Here, too, requests for discovery should be made with some specificity that indicates an understanding of computer systems.[75] Similarly, the responding party's understanding

---

> In addition, plaintiff has made no showing that the documents she seeks actually exist or that the defendants have unlawfully failed to produce them. Indeed, plaintiff has not alleged that the defendants failed to make a search of adequate scope or duration.

(footnote omitted) (citation omitted).

71. Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

72. *Cf.* 6 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE § 26.41 (3d ed. 2004) (noting that the amendments to FRCP 26(b) in 2000 created a two-tiered system of discovery, where the "relevant to the claim or defense" standard for determining the scope of the first tier of discovery is narrower than the "subject matter involved in the action" standard that was used to determine the sole scope of discovery prior to the amendments).

73. *See* Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 97 (D. Md. 2003):

> [G]iven the minimal threshold requirements of Rule 26(b)(1) for the discoverability of information (a requesting party is entitled to seek discovery of non-privileged information "relevant" to the claims and defenses raised in the pleadings), and the potentially enormous task of searching for all relevant and unprivileged electronic records, courts have attempted to fashion reasonable limits that will serve the legitimate needs of the requesting party for information, without unfair burden or expense to the producing party.

74. *Cf.* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 10–11 ("[T]he proposed amendment [to Rule 26(b)(2)] is required because of the staggering volume of electronically stored information and because of the variety of ways in which such information is maintained.").

75. *Cf.* DIST. WYO. R. 26.1(d)(3)(A) ("Duty to Notify. A party seeking discovery of computer-based information shall notify the opposing party immediately, but no later than the Fed. R. Civ. P. 26(f) conference of that fact and identify as clearly as possible the categories of information which may be

of its information systems, document retention policy and the specificity of its objection to discovery of electronic documents can impact the court's ruling.[76]

a. Defining the boundaries of users from whom discovery may be had

Just as a party cannot discover the materials contained in every paper filing cabinet in its adversary's far flung network of offices, the scope of discovery of electronic documents must be limited to those generated by people relevant to the requesting party's claim or defense in a tier one analysis.[77] One court applied

---

sought.").

76. *See Rowe Entm't*, 205 F.R.D. at 428:

> [T]he defendants' claims that the e-mail is unlikely to yield relevant information [is un]persuasive. General representations by WMA and Monterey that their employees do little business by e-mail are undocumented and are contradicted by data proffered by these same defendants. Monterey, for example, estimates that its eight computers contain 198,000 e-mail messages .... It is probable that some significant portion of this traffic related to the conduct of business. Furthermore, the supposition that important e-mails have been printed in hard copy form is likewise unsupported. In general, nearly one-third of all electronically stored data is never printed out.... Here, the defendants have not alleged that they had any corporate policy defining which e-mail messages should be reduced to hard copy because they are "important."

77. *See* Tulip Computers Int'l v. Dell Computer Corp., 52 Fed. R. Serv. 3d (West) 1420, 1429 & n.2 (D. Del. 2002) (finding that the plaintiff's attempts to link Michael Dell to involvement in alleged patent infringement was too tenuous to allow broad discovery of Michael Dell's e-mail, while granting access to search other Dell executives' e-mails for responsive documents); *cf.* Jones v. Goord, No. 95 CIV.8026(GEL), 2002 WL 1007614, at *7 (S.D.N.Y. May 16, 2002).

> The [defendant] State, indeed, does not directly challenge the claim that the [electronic] material sought is relevant [to the plaintiff's claim], within the meaning of Rule 26(b)(1). At the same time, it is far from clear from the evidence presented that all of the information in the databases sought goes to these issues. Plaintiffs have not established that the databases are limited to class [action] members, or that they are or could be (without enormous effort and expense) redacted to relate only to maximum-security inmates. So far as the record before the Court indicates, in fact, the opposite is true. That is, the databases appear to be general DOCS managerial tools, covering all inmates in the State correctional system. Nothing in the record suggests that the databases are easily broken down in such a way that

> [T]he common sense principle that people generate data referring to an event, whether e-mail or word processing documents, contemporaneous with that event.... Conversely, it is unlikely that people, working in an office, generate data about an event that is not contemporaneous unless they have been charged with the responsibility to investigate that event or to create some form of history about it.[78]

Careful use of this temporal-individual principle of relevancy can establish a spectrum of users "more likely than not" to have generated electronic documents relevant to a claim or defense within a discrete period of time.[79] Another court, speaking in the context of the duty to preserve electronic records during a litigation hold, used the colloquial term "key players" to define the basic scope of the defendant's employees whose electronic documents would likely be discoverable.[80]

The informal nature of certain electronic documents, such as e-mail, can also lead to special privacy concerns.[81] That is, while an employee might not include personal information in a more formal paper document on a relevant matter, the character of e-mail is such that an employee may mix personal and business matters in electronic messages.[82] One court had little sympathy for such

---

> only the portion relating to the institutions involved in this lawsuit can be separately reproduced or disclosed.

Id In *Kormendi v. Computer Associates International* the court suggests that the plaintiff may propose discovery from employees of the defendant who might have saved e-mails relevant to the plaintiff's termination in addition to those employees the defendant has identified as involved in the termination, but that the plaintiff "has little incentive to demand expensive searches, since plaintiff must pay the cost of the e-mail search." No. 02Civ.2996(LAK)(DFE), 2002 WL 31385832, at *3 (S.D.N.Y. Oct. 21, 2002).

78. McPeek v. Ashcroft, 212 F.R.D. 33, 35 (D.D.C. 2003).

79. *Id.* at 35–37.

80. Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 100 (D. Md. 2003).

81. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at app. 20 ("The volume of [electronic] data, and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming.").

82. *Cf.* Byers v. Ill. State Police, 53 Fed. R. Serv. 3d (West) 740, 754 (N.D. Ill. 2002).

personal privacy concerns: "To the degree the defendants seek to assert the privacy concerns of their employees, those interests are severely limited . . . . [A]n employee who uses his or her employer's computer for personal communications assumes some risk that they will be accessed by the employer or by others."[83] Thus, while some courts may consider personal privacy concerns, the normal privilege and privacy concerns of discovery are paramount in the electronic discovery arena.[84]

b. Determining what documents may be discovered as relevant to a claim or defense

"American lawyers engaged in discovery have never been accused of asking for too little . . . . [L]ike the Rolling Stones, they hope that if they ask for what they want, they will get what they need. They hardly need . . . encouragement to demand as much as they can from their opponent."[85] Where the parties cannot agree at the 26(f) conference whether and where discoverable documents exist or objections are lodged during discovery, the court may attempt to rule on a discovery request under tier one's relevance to a claim or defense scope standard.[86] "Using traditional search methods to locate paper records in a digital world presents unique problems"[87] that courts must address.

> [T]he Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of e-mail files. . . . E-mails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via e-mail. . . . All of these e-mails must be scanned for both relevance and privilege.

Id. (citation omitted).

83. Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

84. *See infra* Part V. for more on privilege and privacy.

85. McPeek v. Ashcroft, 202 F.R.D. 31, 33–34 (D.D.C. 2001).

86. *See id.* (analyzing the plaintiff's motion to compel discovery of electronic documents from backup systems under the relevant to a claim or defense standard).

87. *Id.* at 32.

i. Determining whether documents subject to mandatory disclosure exist

Where the parties cannot come to an agreement on the scope of discovery at the 26(f) conference or where discovery within tier one does not proceed smoothly, courts determine the appropriate scope of mandatory disclosure consistent with their power to compel discovery.[88] There is some onus on the party requesting production not to make an overbroad request from the start.[89] Also, in the extremely large universe of electronic documents, the party asked to make the disclosures may not have a strong enough grasp on its information system(s) to be able to pinpoint the location of discoverable documents, or even to know for certain if discoverable documents exist.[90]

Matters of privilege and confidentiality are also implicated where the court orders untargeted or sample access to electronic documents in order to determine if discoverable documents exist.[91] Therefore, a court may order the parties to try again to work out the scope of discovery between them.[92]

---

88. *See In re* Ford Motor Co., 345 F.3d 1315, 1316–17 (11th Cir. 2003) (stating that a district court has the power to make the producing party comply with mandatory disclosure under the tier one, relevant to a claim or defense standard, as long as it gives some explanation for its ruling).

89. *Cf. id.* at 1317 (granting defendant car manufacturer's petition for writ of mandamus by finding that the plaintiff was not entitled to a broad order from the district court granting direct access to Ford's customer, dealer and employee contacts databases absent "a factual finding of some non-compliance with discovery rules by Ford").

90. *See McPeek*, 202 F.R.D. at 31.

91. *See Ford Motor*, 345 F.3d at 1317:

> [T]he district court granted [the plaintiff] unlimited, direct access to [the defendant]'s databases. The district court established no protocols for the search. The court did not even designate search terms to restrict the search. Without constraints, the order grants [the plaintiff] access to information that would not—and should not—otherwise be discoverable without [the defendant] first having had an opportunity to object.

92. *See In re* Livent, Inc. Noteholders Sec. Litig., 98 Civ. 7161 (VM)(DFE), 2002 U.S. Dist. LEXIS 26446, at *9–*10 (S.D.N.Y. Jan. 2, 2003) (ordering, in response to the plaintiffs' request for additional electronic discovery, the defendant to explain to the plaintiff "all the steps it has taken to find responsive e-mails. As to any further steps . . . [the defendant] and plaintiffs should confer . . . . If they are unable to reach a resolution, they should send me a single joint letter . . . ."). In *Gambale v. Deutsche Bank Ag*,

Finally, a court may employ a variety of strategies to help it reach an informed decision on the scope of discovery:

> 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 and the quality and quantity of the factual information provided by the parties to be used by the court in evaluating the Rule 26(b)(2) factors. The court can, for example, shift the cost, in whole or part, of burdensome and expensive Rule 34 discovery to the requesting party; it can limit the number of hours required by the producing party to search for electronic records; or it can restrict the sources that must be checked. It can delay production of electronic records in response to a Rule 34 request until after the deposition of information and technology personnel of the producing party, who can testify in detail as to the systems in place, as well as to the storage and retention of electronic records, enabling more focused and less costly discovery. A court also can require the parties to identify experts to assist in structuring a search for existing and deleted electronic data and retain such an expert on behalf of the court. But it can do none of these things in a factual vacuum, and ipse dixit assertions by counsel that requested discovery of electronic records is overbroad, burdensome or prohibitively expensive provide no help at all to the court.[93]

---

the court ordered the defendant to submit an affidavit detailing the steps already taken to search electronic files in response to certain discovery requests and explain the "feasibility and cost of retrieving [responsive] e-mails." No. 02 Civ.4791 HB DFE, 2002 WL 31655326, at *1 (S.D.N.Y. Nov. 21, 2002). The plaintiff would then have to either submit to a cost-shifting analysis and protocol to obtain discovery or "argue for a different protocol by conferring with [the defendant] and sending [the judge] a single joint letter outlining the parties' positions on this issue." *Id.*

93. Thompson v. U.S. Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 98–99 (D. Md. 2003). For more on cost shifting see *infra* Parts III.D.2 & IV. For more on application of the FRCP 26(b)(2) factors to determine the scope of discovery, see *infra* Part III.D.1.

(a) Overbroad requests

A common objection raised by the responding party to electronic discovery requests is that the request is too broad.[94] Just as a litigant would not ask the opposition to search its trash bins for all garbage thrown out over the past ten years in the course of traditional discovery, a party that moves for electronic discovery must put some thought into the breadth of the electronic production it has requested.[95] Electronic discovery requests based on speculation are likely to be denied.[96] Similarly, vague assertions by the

---

94. *See In re* Amsted Indus., Inc. "ERISA" Litig., No. 01 C 2963 2002 WL 31844956, at *1–*2 (N.D. Ill. Dec. 18, 2002).

> The parties dispute whether plaintiffs' requests for documents conform to the parameters of Federal Rule of Civil Procedure 26, which provides that a party may request production of any non-privileged documents regarding any matter that is relevant to the claim or defense of any party. . . .
>
> Defendants assert that producing the requested documents, without limitations, will lead to the production of irrelevant material that had no bearing on the decisions [to take certain actions that the plaintiff asserts breached the defendant's fiduciary duties]. . . .
>
> To the extent that defendants' e-mail investigation was limited by their relevancy objections, they should now [conduct a broader search for discovery of electronic data].

Id.(footnotes omitted) (citations omitted).

95. *See* Wright v. AmSouth Bancorporation, 320 F.3d 1198, 1205 (11th Cir. 2003).

> [The plaintiff] sought discovery of a "computer diskette or tape copy of all word processing files created, modified and/or accessed by, or on behalf" of five [of the defendant's] employees over a two and one-half year period. [The plaintiff] made no attempt to narrow his request to something more meaningful and relevant during the discovery period despite an appropriate objection from [the defendant]. The district court denied [the plaintiff]'s motion to compel these items as being overly broad and unduly burdensome. The court also found that [the plaintiff] failed to make a "reasonable showing of relevance" for these items. . . .
>
> This Court has written that discovery in Title VII cases is "not without limits. The information sought must be relevant and not overly burdensome to the responding party." On appeal, [the plaintiff] has not tried to identify particular items within the expansive request nor has he provided a theory of relevance that might narrow the scope of his request. The district court abused no discretion in its ruling on the discovery issue.

Id. (citation omitted).

96. *See* Stallings-Daniel v. N. Trust Co., 52 Fed. R. Serv. 3d (West) 1406,

responding party that electronic discovery requests should be denied as overbroad are not likely to be successful.[97]

The court may also take into account whether all parties to the litigation tried to come to a reasonable agreement as to the scope of electronic discovery between themselves.[98]

(b) Sampling

The court may order that some small percentage of documents from the producing party's information system(s) be produced.[99]

1407–08 (N.D. Ill. 2002).

> Plaintiff wishes to have us review the discovery history of a settled case that was before a different judge and hold that because defendant may have committed some sort of discovery abuse there, it must also be guilty of similar conduct here, justifying electronic discovery for documents she is not sure even exist. . . .
>
> . . . .
>
> Nothing in the documents produced justifies an intrusive and wholly speculative electronic investigation into defendant's e-mail files.

Id. (footnote omitted).

97. *Thompson*, 219 F.R.D. at 98:

> [T]he most important ingredient for the analytical process to produce a fair result is a particularization of the facts to support any challenge to discovery of electronic records. Conclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail.

98. *Cf.* Super Film of Am., Inc. v. UCB Films, Inc. 219 F.R.D. 649, 656–57 (D. Kan. 2004) (rejecting the responding party's contention that a discovery request was overly burdensome where the requesting party "ha[d] attempted to reach a stipulation regarding the scope of the parties' obligations to produce electronic discovery").

99. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. May 13, 2003) ("Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases."); McPeek v. Ashcroft, 202 F.R.D. 31, 34–35 (D.D.C. 2001).

> I have decided to take small steps and perform, as it were, a test run. Accordingly, I will order DOJ to perform a backup restoration of the e-mails attributable to Diegelman's computer during the period of July 1, 1998 to July 1, 1999. I have chosen this period because a letter from plaintiff's counsel to DOJ, complaining of retaliation and threatening to file an administrative claim, is dated July 2, 1998, and it seems to me a convenient and rational starting point to search for evidence of retaliation. I have chosen e-mail because of its universal use and because I am hoping that the restoration will yield both the e-mails Diegelman sent and those he received.

These documents are analyzed to determine if they contain discoverable material.[100] The court can then make its final order based on the results of this analysis, taking into account the effort and expense involved in the search in relation to the discoverable documents, if any, uncovered.[101]

(c) Specialized searching

Where technically feasible, courts may only require the responding party to search its information systems for discoverable material by key term or other such controlled method.[102]

Id.

100. *McPeek*, 202 F.R.D. at 35 (ordering the defendant "to search in the [sample of] restored e-mails for any document responsive to any of plaintiff's requests for production of documents"); *see also Zubulake*, 217 F.R.D. at 324 (ordering the defendant to "prepare an affidavit detailing the results of its search [once completed], as well as the time and money spent").

101. *See Zubulake*, 217 F.R.D. at 324 ("When based on an actual sample, the marginal utility test will not be an exercise in speculation—there will be tangible evidence of what the backup tapes may have to offer. There will also be tangible evidence of the time and cost required to restore the backup tapes," all of which will inform the court's application of the marginal utility test to determine whether to grant plaintiff's request for discovery of electronic documents); *see also McPeek*, 202 F.R.D. at 35 (requiring the defendant, once it has finished searching the sample for responsive documents, to "file a comprehensive, sworn certification of the time and money spent and the results of the search. Once it does, [the magistrate judge] will permit the parties an opportunity to argue why the results and the expense do or do not justify any further search.").

102. *See* McPeek v. Ashcroft, 212 F.R.D. 33, 36 (D.D.C. 2001) ("The backup tape . . . is close enough in time to warrant a search of it with the understanding that the defendant need only search it for references to plaintiff's intention to file suit or to any aspect of Diegelman's activities in reference to JPR in the month of January, 2000."); Tulip Computers Int'l v. Dell Computers Corp., 52 Fed. R. Serv. 3d (West) 1420, 1429 (D. Del. 2002) (ordering search of Dell executives' e-mails "based on an agreed upon list of search terms"). In *Zakre v. Norddeutsche Landesbank Girozentrale*, the court did not require the producing party to conduct key word searches, holding that the producing party met its burden of production by providing the requesting party with CD-ROMS containing potentially responsive e-mails of which the requesting party could conduct text searches. No. 03 Civ. 0257(RWS), 2004 WL 764895, at *1 (S.D.N.Y. Apr. 9, 2004). In *Medtronic Sofamor Danek, Inc. v. Michelson*, the special master was ordered to conduct keyword searches based on a list submitted by the requesting party. 56 Fed. R. Serv. 3d (West) 1159, 1171 (W.D. Tenn. 2003). *But see In re* Amsted Indus., Inc. "ERISA" Litig., No. 01 C 2963, 2002 WL 31844956, at *2 (N.D. Ill. Dec. 18, 2002) (ordering the defendant, which had conducted word searches of backup tapes

(d) Use of a special master

The Federal Rules of Civil Procedure allow judges to appoint special masters to perform certain duties by consent of the parties or under exceptional circumstances where cases present complicated issues that warrant such an appointment.[103] Thus, courts have appointed a disinterested third party to conduct forensic inspections to determine whether potentially discoverable documents exist in the responding party's information systems, which helps address the responding party's concerns about privilege, privacy, and waiver of privilege.[104] See *infra* Part V for more on privilege and privacy.

(e) Sneak peak/clawback

The Court may allow the requesting party to have a "sneak peak" at some of the types of documents it has requested to determine if discoverable material is available.[105] In such cases, the

---

to find documents relevant to the claims in the case, to research tapes and e-mail folders of relevant parties more thoroughly).

103. FED. R. CIV. P. 53(a).

104. *Medtronic*, 56 Fed. R. Serv. 3d (West) at 1171.

> Given the amount of electronic data at issue, the court finds that the appointment of a special master to oversee discovery is warranted and that the special master should be a technology or computer expert. The special master's duties will include making decisions with regard to search terms; overseeing the design of searches and the scheduling of searches and production; coordinating deliveries between the parties and their vendors; and advising both parties, at either's request, on cost estimates and technical issues. The special master shall be subject to all confidentiality requirements and protective orders set forth in this and in other orders in this cause [sic].

Id.; *see also Tulip Computers*, 52 Fed. R. Serv. 3d (West) at 1424–25 (ordering the defendant to produce e-mails a consultant deemed discoverable "subject to [the plaintiff's] review for privilege and confidentiality designations provided under the protective order"); *cf.* First USA Bank v. PayPal, Inc., 76 Fed. Appx. 935, 936 (Fed. Cir. 2003) (rejecting appeal of former CEO of defendant from magistrate judge's order "allow[ing] electronic discovery consultants to create a forensic copy of the [former CEO's] computer's hard drive and identify any potentially relevant documents and, if such documents were found and identified, . . . allow[ing the former CEO] to create a privilege log"); McCurdy Group v. Am. Biomed. Group, 9 Fed. Appx. 822, 831 (10th Cir. 2001) ("[The defendant] has not explained why inspection of the [plaintiff's] zip drive and/or inspection of the hard drive by [a third party] would not have been sufficient to satisfy its concerns [about the plaintiff's full compliance with discovery].").

105. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2,

court usually makes special provisions for privilege claims, return of privileged documents, and non-waiver of privilege.[106]

ii. Producing documents that are not reasonably accessible

"[T]he obligations of a responding party to provide discovery of electronically stored information that is not reasonably accessible [is] an increasingly disputed aspect of such discovery."[107] Reasonably accessible electronic information is "information that the party itself routinely accesses or uses or that is easily located and retrieved."[108] Advances in information technology, as well as business reasons for storing copies of data electronically for recovery in case of system failure has led to categories of electronic data that are considered not reasonably accessible, but that do exist and are sought.[109]

A discussion of how some courts analyze requests for electronic documents that are difficult to retrieve under tier one of discovery follows below. It is first noted, however, that a proposed amendment to FRCP 26(b)(2) acknowledges the difficulties inherent in producing documents that are not reasonably accessible by removing discovery of such electronic material from tier one altogether into tier two of discovery, which would give litigants and courts greater guidance in how to approach discovery of such information.[110]

---

at 8–9 ("Parties frequently attempt to minimize the cost and delay of an exhaustive privilege review by agreeing to protocols that minimize the risk of waiver. Such protocols may include so-called quick peek or claw back arrangements, which allow production without a complete prior privilege review . . . .").

106. *Cf.* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 3–4 (The parties may agree to, and the court may enter a case-management order where, "requested materials [are provided] without waiver of privilege to enable the party seeking production to designate the materials desired for actual production, with the privilege review of only those materials to follow."); see *infra* Part V. for more on privilege and privacy.

107. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 10.

108. *Id.* at 11.

109. *Id.* at 10–11.

110. The REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 6, adds the following language to the end of FRCP 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

(a) Legacy data

"Legacy data is stored information that is no longer used and only maintained on an obsolete system, making it expensive and burdensome to restore and provide."[111] While it is reasonable to produce documents that are routinely accessed from current systems, data in legacy systems, including backup tapes, may not be reasonably accessible.[112] A cautious approach to ordering restoration of legacy data is indicated.[113]

(b) Information on backup systems

Most businesses (and even individuals) back up their information for disaster recovery in case of catastrophic failure.[114] "Backup tapes are by their nature indiscriminate. They capture all information at a given time and from a given server but do not catalogue it by subject matter. Unlike a labeled file cabinet or paper files organized under an index, the collection of data . . . [can be] random."[115] There appears to be "no controlling authority for the proposition that restoring all backup tapes is necessary in every case.

---

may specify terms and conditions for such discovery.

111. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 11.

112. *See* Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1160 (W.D. Tenn. 2003) ("[D]ata on each backup tape must be restored from the backup tape format to a format that a standard computer can read."). In *McPeek v. Ashcroft*, the court appeared to accept the defendant's assertion that

> for the period 1992–1998, the DOJ computer system was known as "Eagle." In 1998, DOJ computers were briefly connected to a system called "JCON1." From 1998 to the present, they have been connected to "JCON2." . . . [Thus] the backup tapes have to be "restored" or rendered readable by returning the files to a source (i.e., a disk or hard drive) from which they can be read by the application which originally created them.

202 F.R.D. 31, 32 (D.D.C. 2001) (citations omitted).

113. *See McPeek*, 202 F.R.D. at 34 (ordering a sample restoration of e-mails from backup tapes covering a discrete time period).

114. *See, e.g.*, *id.* at 33 ("[T]he [backup] system was designed to prevent disaster, i.e., the destruction of all the data being produced on a given day if the network system crashed. Once the day ended and the system had not crashed, the system administrator could breathe a sigh of relief.").

115. *Id.*; *see also* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 11 ("[I]nformation stored only for disaster recovery is generally expensive to restore and is disorganized.").

The Federal Rules of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic . . . ."[116] Consequently, some courts find circumstances where it is reasonable—and develop strategies to help make it reasonable—to require a party to produce documents from backup systems despite the uncertainties, difficulties and expense involved.[117] Other courts, however, do not find any circumstances which warrant the search of backup systems.[118]

(c) Deleted data

"'[D]eleting' electronic records does not actually result in their instantaneous erasure, but rather simply designates [a] file as 'not used,' thereby enabling the computer to write over it . . . . [R]equests seeking 'deleted' electronic records are permissible."[119] The simple

116. *McPeek*, 202 F.R.D. at 33.

117. *See id.* at 33–35 (balancing the likelihood of finding information relevant to a claim or defense with the expense involved in deciding whether to compel a search of backup tapes and order a sample restoration of e-mails from backup tapes covering a discrete time period); *see also* Zhou v. Pittsburg State Univ., No. 01-2493-KHV, 2003 WL 1905988, at *2 (D. Kan. Feb. 5, 2003) (reading FRCP 26(b) in conjunction with FRCP 34, the court found that "[s]imply put, the disclosing party must take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data"). In *Medtronic*, the court ordered backup tapes that both parties conceded would contain relevant electronic data to be searched by a special master, but also ordered that the requesting party share in the cost of production. 56 Fed. R. Serv. 3d (West) at 1161, 1170–77.

118. After the restoration of sample backup tapes ordered in 2001 in *McPeek*, 202 F.R.D at 33–35, was completed, the plaintiff returned to court to request that Magistrate Judge Facciola order further searches of the defendant's backup tapes. McPeek v. Ashcroft, 212 F.R.D. 33, 34 (D.D.C. 2003). In the subsequent proceeding, Judge Facciola applied a "more likely than not" to contain relevant information standard to sixteen additional backup tapes the plaintiff wished to have searched. *Id.* at 34–37. Judge Facciola found that fifteen of the sixteen backup tapes were unlikely to yield electronic documents relevant to the plaintiff's lawsuit, and thus did not require the defendant to search those tapes. *Id.*

119. Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 97 (D. Md. 2003) (citations omitted); *see also* Zhou v. Pittsburg State Univ., No. 01-2493-KHV, 2003 WL 1905988, at *2 (D. Kan. Feb. 5, 2003) (reading FRCP 26(b) in conjunction with FRCP 34, the court found that "[s]imply put, the disclosing party must take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data."); Computer Assoc. Int'l v. Quest Software, Inc., 56 Fed. R. Serv. 3d (West) 401, 402 (N.D. Ill. 2003)

act of booting up a computer or saving a new document may, however, lead to the deletion of electronic data, with no intent to spoliate.[120] Thus, a court may order the production of a sample of material from backup tapes so that the relevance of deleted electronic data, if any, can be assessed.[121] The proposed amendments to FRCP 26(b)(2) would not require tier one (mandatory) disclosure of documents that were deleted in the ordinary course of business.[122]

D. Tier Two Discovery: Broadening the Scope of Discoverable Electronic Documents

The revisions to FRCP 26 made in 2000 mandated disclosure of documents that meet the standard of being relevant to the claim or defense, and also provided a second tier of discovery that allows the pre-revision scope of discovery to be reached.[123] In tier two, the requesting party may obtain a court order authorizing the application of a broader standard of discovery to the subject matter involved in the action with a showing of good cause.[124] "The dividing line

---

(requiring the defendant to bear the full cost of production of copies of hard drives created by a third party that "[would] allow plaintiffs to search for and reconstruct files that have been deleted from the [defendant's] computers and would be otherwise undiscoverable" as the files would likely be relevant to the plaintiff's trade secret misappropriation claim).

120. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 7 ("The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information.").

121. *McPeek*, 202 F.R.D. at 33 ("There is a theoretical possibility that there may be something on the tapes that is relevant to a claim or defense, for example, a subsequently deleted e-mail that might be evidence of a retaliatory motive," thus ordering a sample restoration of e-mails from backup tapes).

122. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 11 ("Deleted data may also be considered inaccessible if, despite the possibility of restoration through forensic techniques, significant cost, effort, and burden is required."); *see also infra* Part VII. for more on spoliation.

123. 6 MOORE ET AL., *supra* note 72, § 26.41 (noting that the amendments to FRCP 26(b) in 2000 created a two-tiered system of discovery, where the second tier used the same "subject matter involved in the action" language that was used to determine the standard for the sole scope of discovery prior to the amendments).

124. FED. R. CIV. P. 26(b)(1):

> For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All

between information relevant to the claims and defenses and that relevant only to the subject matter of the action cannot be defined with precision."[125] Generally, the broader standard may be thought of as allowing discovery of relevant information not admissible into evidence, but reasonably calculated to lead to the discovery of admissible evidence.[126] In keeping with the language of Rule 26(b)(1) as revised in 2000, courts should apply the tests in 26(b)(2) to determine whether to allow broader discovery.[127] The proposed amendments to FRCP 26 attempt to clarify the distinction between the two tiers of discovery within the electronic arena as well as to provide procedural guidance to litigants and courts:

> The proposed addition to Rule 26(b)(2) builds on the two-tier structure of scope of discovery defined in Rule 26(b)(1) and applies the structure to the burden of discovery into electronically stored information. A party must provide discovery of relevant reasonably accessible electronically stored information without a court order. A party need not review or provide discovery of electronically stored information that it identifies as not reasonably accessible. If the requesting party moves for discovery of such information—the second tier—the responding party must show that the information sought is not reasonably accessible. If that showing is made, the court may order the party to provide the information, but the order must be

---

discovery is subject to the limitations imposed by Rule 26(b)(2)(i), (ii), and (iii).

125. FED. R. CIV. P. 26(b)(1) advisory committee note, 192 F.R.D. 340, 389 (2000); *see also* Thompson v. United States Dep't of Hous. & Urban Dev., 199 F.R.D. 168, 172 (D. Md. 2001) ("[T]he philosophical exercise of debating the difference between discovery relevant to the 'claims and defenses' as opposed to the 'subject matter' of the pending action [is] the juridical equivalent to debating the number of angels that can dance on the head of a pin . . . .").

126. *See* FED. R. CIV. P. 26(b)(1) advisory committee note, 192 F.R.D. 340, 389–390 (2000) ("The good-cause standard warranting broader discovery is meant to be flexible. . . . [I]nformation must be relevant to be discoverable, even though inadmissible, and . . . discovery of such material is permitted if reasonably calculated to lead to the discovery of admissible evidence.").

127. *See id.* at 390 ("[A] sentence has been added calling attention to the limitations of subdivisions (b)(2)(i), (ii), and (iii). These limitations apply to discovery that is otherwise within the scope of subdivision (b)(1). The Committee has been told repeatedly that courts have not implemented these limitations with the vigor that was contemplated.").

> based on a showing of good cause by the requesting party. The good-cause analysis balances the requesting party's need for the information against the burden on the responding party. Courts addressing such concerns have properly referred to the limitations in Rule 26(b)(2)(i), (ii), and (iii)—whether the burden or expense of the proposed discovery outweighs its likely benefit taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues—in deciding when and whether the effort involved in obtaining such information is warranted. The rule makes it clear that the producing party has the burden of demonstrating that the requested electronically stored information is inaccessible and that the requesting party has the burden of demonstrating good cause for the production of inaccessible information.[128]

1. The Good Cause Analysis

FRCP 26(b)(2) provides courts with a rubric for balancing the needs of the requesting party for additional discovery against the burden to the responding party:[129]

> The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the

---

128. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 11–12. For a discussion about the definition of information that is not reasonably accessible, see *supra* Part III.C.2.b.ii.; *see also* Kleiner v. Burns, 48 Fed. R. Serv. 3d (West) 644, 649 (D. Kan. 2000) (pre-2000 amendment to FRCP 26) ("The disclosing party shall take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data.").

129. In *Thompson v. United States Department of Housing & Urban Development*, the court reviewed its reasons for holding in prior proceedings that requested electronic documents were discoverable (though apparently under a tier one standard). 219 F.R.D. 93, 96–99 (D. Md. 2003). The court opined that it "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." *Id.* at 98. See also the Civil Rules Advisory Committee's discussion of the proposed addition to Rule 26(b)(2) *supra* in the text accompanying note 110.

> discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).[130]

a. Duplicative or obtainable from some other source

Where the requesting party has received much of the information requested in a traditional form, some showing of the likely additional benefit of also receiving the data in electronic form must be made by the requesting party.[131] For instance, in denying a motion to compel discovery of computer-generated documents and

---

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

131. Jones v. Goord, No. 95 CIV.8026(GEL), 2002 WL 1007614, at *13–*14 (S.D.N.Y. May 16, 2002).

> Though plaintiffs do not need to show that obtaining this data will in fact advance their cause, they do have to provide some basis to believe that specific tests can be run that, with a reasonable degree of scientific certainty, can be expected to yield results that would be relevant to the issues before the Court.
>
> . . . .
>
> . . . [M]uch of the actual *data* in the databases (to the extent relevant) has already been provided to plaintiffs in documentary form. Plaintiffs cite no concrete facts available in the database, relevant to the litigation, and unprivileged, that are not available in the 700,000 pages of material already provided to them.

Id. (citations omitted); *see also* Nicholas v. Wyndham Int'l, Inc., 373 F.3d 537, 543 (4th Cir. 2004) (upholding the district court's denial of the defendant's request for discovery of e-mails from a non-party owned by the plaintiffs as duplicative where the "[p]laintiff's had already produced some 400 pages of e-mails (including e-mails from their [non-party] accounts)"). The appeals court also upheld the district court's entry of a FRCP 26(c) protective order that discovery could not be had from the non-party because the defendant's discovery request was also "unduly burdensome, and harassing." *Id.*

e-mail without prejudice, one court showed a "willing[ness] to reconsider the plaintiffs' request if the plaintiffs indicate the specific factual issue or issue for which they in good faith reasonably believe the requested documents are necessary."[132] The court may inquire into whether the request for wider electronic discovery will likely be duplicative as part of the broader burden versus benefit test.[133]

b. Requesting party had ample opportunity to discover

A finding that a request for electronic discovery is belated may relate to the fact that the responding party has already produced documents in paper form, making the electronic document request overly burdensome.[134] Another situation in which a request for

---

132. *In re* Gen. Instrument Corp. Sec. Litig., No. 96 C 1129, 1999 WL 1072507, at *6 (N.D. Ill. Nov. 18, 1999) (pre-2000 amendment to FRCP 26).

133. *Id.*

> Discovery may be limited if the court determines that "the burden or expense of the proposed discovery outweighs its likely benefit." The court finds that the likely benefit of the requested discovery is minimal. . . . First, the defendants have already produced more than 110,000 pages of documents, including thousands of pages of e-mail. Given the large number of documents already produced, the court finds it unlikely that additional documents are necessary. Second, the plaintiffs have not identified any specific factual issue for which additional discovery would help them prove their case.

Id. (citations omitted); *see also* Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 167–169 (S.D.N.Y. 2004) (denying requests for data stored in electronic form that are likely duplicative as overly burdensome but granting those that are likely to provide additional relevant information).

134. *Goord*, 2002 WL 1007614, at *15–*16:

> The parties have spent years, significant sums, and exhaustive efforts on discovering and analyzing a mountain of paper—a project that, plaintiffs now claim at the eleventh hour before expiration of the n-th discovery deadline, was largely useless, or at least superseded, because the production of electronic data instead would have accomplished the same thing and more. . . .
>
> . . . . Nothing in the record suggests that . . . the plaintiffs took any step to seek discovery of any electronic data until after their adversaries had expended exorbitant sums of public money on conventional discovery, and until the ultimate deadline for completing fact discovery, after seven years of litigation, was at last at hand. Accordingly, the Court is constrained to find that the plaintiffs have had, and let pass, ample opportunity to obtain this information earlier in the discovery process, and that that conclusion strongly supports denying plaintiffs' motion. . . .
>
> . . . .

electronic discovery may be deemed belated occurs when the requesting party has previously indicated that discovery was completed.[135] The court may use the inquiry into whether the request for wider electronic discovery is belated as part of the broader burden versus benefit test.[136]

c. Burden versus benefit of additional discovery

The balancing test of 26(b)(2)(iii) is a more global approach used by courts to assess whether good cause exists to expand the scope of discovery, and may incorporate the other two tests.[137] Such a test is by its nature fact specific.[138] In other words, the balancing

---

> . . . [T]he Court finds that discovery should be denied because defendants have made a compelling showing that the burden of the proposed discovery far outweighs its likely benefit for resolving the issues before the Court, particularly in light of the failure of the plaintiffs to seek such discovery despite ample opportunity to do so in a more timely manner, and the vast amount of material, largely duplicating the contents of the databases now sought, which has already been provided by the defendants.

135. *See Gen. Instrument Corp.*, 1999 WL 1072507, at *6.

136. *See id.*

137. *See Goord*, 2002 WL 1007614, at *10:

> All three of the reasons set forth in Rule 26(b)(2) as rationales for limiting disclosure of otherwise-discoverable information may apply in this case and require denying discovery of the databases. The most important reason for this conclusion . . . is that set forth in 26(b)(2)(iii) . . . . [T]his standard largely subsumes the other considerations reflected in Rules 26(b)(2)(i) and (ii).

138. After analyzing the minimal benefit to the requesting party, *see supra* notes 132–133 and accompanying text, the court, in *Gen. Instrument Corp.*, discussed the contextualized burden to the responding party and concluded:

> The court finds that the burden on defendants would be significant. It does appear to the court that the requested documents could be retrieved from the backup tapes without undue expense. Nevertheless, the technical matter of retrieving the documents from the backup tapes would be just the start of the process. Defense counsel would then have to read each e-mail, assess whether the e-mail was responsive, and then determine whether the e-mail contained privileged information. Given that the volume of e-mail at issue here is potentially very large, the court finds that the burden of reviewing the requested documents would be heavy. The court further notes that expert discovery is beginning. Forcing defense counsel to engage in document review would necessarily distract their energies from the other parts of this ongoing litigation. In weighing the burden of the requested discovery against its likely benefit, the court finds that the

test is a flexible standard rather than a per se rule. For instance, the fact that non-duplicative, relevant data is likely to be produced by a search of inaccessible data does not necessarily equate to a showing of good cause.[139]

Other factors considered in the burden versus benefit analysis include the time involved in satisfying a request for production of inaccessible documents as well as whether the request appears focused on the information systems most likely to yield results.[140] "When faced with a request that would impose a significant cost on the responding party, a court should focus on the marginal utility of the proposed search."[141]

> burden outweighs the benefit and that the plaintiffs' motion should therefore be denied. In making this ruling the court places significant weight on its finding that the plaintiffs have not identified any specific factual issue for which they believe the requested documents would be necessary.

1999 WL 1072507, at *6.

139. Cognex Corp. v. Electro Scientific Indus., Inc., No. Civ.A. 01CV10287RCL, 2002 WL 32309413, at *2–*3 (D. Mass. July 2, 2002):

> The fact that [the producing party] has conducted a thorough search of [its] existing files does not, however, suggest that a search of back-up files would only uncover duplicative documents. . . . [I]n light of the sheer volume of data on the back-up tapes, it is virtually inconceivable that they do not contain additional relevant material which would be appropriate for production.
>
> The fact that the back-up tapes are believed to contain relevant documents does not end the inquiry. . . .
>
> . . . .
>
> . . . Given the nature of the search already conducted and the burden of providing what is being sought, the burden and expense of the proposed discovery outweighs its likely benefit.

140. *See* Byers v. Ill. State Police, 53 Fed. R. Serv. 3d (West) 740, 755–57 (N.D. Ill. 2002).

141. *Id.* at 756. Though finding that the burden outweighed the marginal benefit, the court gave the requesting party the option to obtain electronic discovery if it would bear the unusual costs associated with its request for production of e-mails from an eight-year period that would have to be recovered from an obsolete e-mail program. *Id.* at 755–57; *cf.* Fennell v. First Step Designs, Ltd, 83 F.3d 526, 532–534 (1st Cir. 1996) (analyzing the discovery request made under FRCP 56(f) with reference to FRCP 26(b)(2)(ii), and upholding the district court's denial of a request for discovery of the defendant's complete hard drive due to the "substantial risks and costs" involved and because the plaintiff "did not sufficiently 'set forth a plausible basis for believing that specified facts, susceptible of collection within a reasonable time frame, probably exist.'").

2. Cost Shifting

"'Under [the discovery] rules, the presumption is that the responding party must bear the expense of complying with discovery requests[.]' Nevertheless, a court may protect the responding party from 'undue burden or expense' by shifting some or all of the costs of production to the requesting party."[142] Thus, faced with a difficult decision about whether to allow discovery of electronic data of uncertain probative value under either tier one or tier two of discovery and the somewhat nebulous burden versus benefit analysis, some courts order production but shift the cost of discovery to the requesting party.[143]

3. Regulating and Limiting Tier Two Electronic Discovery

As with tier one discovery, the court may regulate tier two discovery to minimize the burden on the producing party as well as to protect the producing party's privilege and privacy.[144] Similarly,

---

142. Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002) (citations omitted).

143. Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 641 (S.D. Ind. 2000) ("[P]laintiff shall select and pay an expert who will inspect the computers in question to create a 'mirror image' or 'snapshot' of the hard drives."), *supplemented by* No. IP 99-1195-C H/G, 2000 U.S. Dist. LEXIS 8953 (S.D. Ind. June 15, 2000); *see also Rowe Entm't*, 205 F.R.D. at 429–33 (enumerating and applying an eight-factor cost-shifting balancing test resulting in a denial of the defendant's motion for a protective order thus allowing discovery of e-mail "to the extent that the plaintiffs shall bear the costs of production . . ."); Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (holding as part of its order to minimize the burden of discovery on the defendant that the "Plaintiff will pay the costs associated with the information recovery"), *aff'd in part, rev'd in part*, 279 F.3d 796 (9th Cir. 2002). *But see Cognex Corp.*, 2002 WL 32309413, at *5 ("There is something inconsistent with our notions of fairness to allow one party to obtain a heightened level of discovery because it is willing to pay for it. . . . [O]ur system of justice will not be enhanced by the courts participating in giving strategic advantage to those with deeper pockets."). For further in-depth analysis of cost-shifting, see *infra* Part IV.

144. *Playboy Enters.*, 60 F. Supp. 2d at 1054:

> Defendant's privacy and attorney-client privilege will be protected pursuant to the protocol outlined below, and Defendant's counsel will have an opportunity to control and review all of the recovered e-mails, and produce to Plaintiff only those documents that are relevant, responsive, and non-privileged. Any outside expert retained to produce the "mirror image" will sign a protective order and will be acting as an Officer of the Court pursuant to this Order. Thus, this

the court may narrow overbroad requests by issuing a discovery order tailored to yield relevant information.[145] It may also use the various methods described earlier[146] to determine if discoverable documents even exist; in other words, it may require the responding party to employ some technological savvy to discover electronic documents.[147]

The Civil Rules Advisory Committee has acknowledged the importance of a flexible, conditional approach to ensure that discovery proceeds in a manner that accommodates the concerns of all parties to the litigation:

> The court may—as with any discovery—impose conditions and terms in ordering discovery of electronically stored information that is not reasonably accessible . . . . [S]uch terms and conditions could include sampling electronically stored information to gauge the likelihood that relevant information will be obtained, the importance of that information, and the burdens and costs of production; limits

---

> Court finds that Defendant's privacy and attorney-client communications will be sufficiently protected. . . . Lastly, if the work, which will take approximately four to eight hours, is coordinated to accommodate Defendant's schedule as much as possible, the Court finds that the "down time" for Defendant's computer will result in minimal business interruption.

145. *See* Alexander v. FBI, 194 F.R.D. 316, 324–340 (D.D.C. 2000) (pre-2000 amendment to FRCP 26) (narrowing the plaintiff's broad request for general production of e-mails from fifty-seven individuals and a general search by thirty-seven search terms to using one of at most twenty of the search terms as key words for searching only thirty-three individuals' e-mails for relevant information).

146. *See supra* Part III.C.2.b.i.b–e.

147. Itzenson v. Hartford Life & Accident Ins. Co., No. CIV.A.99-4475, 2000 WL 1507422, at *1–*2 (E.D. Pa. Oct. 10, 2000) (pre-2000 amendment to FRCP 26):

> It is difficult to believe that in the computer era when insurers compile an array of claims related statistics for internal purposes that defendant i[s] incapable of at least identifying files with claims for death benefits involving the operation of a motor vehicle, if not those in which there was evidence of intoxication. . . .
>
> . . . .
>
> . . . [D]efendant [shall] use every practicable means promptly to identify files over the past five years regarding pertinent claims and produce them to plaintiff. . . .

> on the amount of information to be produced; and provisions regarding the cost of production.[148]

E. The Method of Production of Electronic Documents

"The form of production is more important to the exchange of electronically stored information than of hard-copy materials, although one format . . . [of production c]ould be hard copy."[149] Because there is a range of information potentially contained in certain electronic formats that simply does not exist in traditional hard copy document production, the method of production can have a strong impact on the substance of discovery:

> [P]roduction may be sought of information automatically included in electronic document files but not apparent to the creator of the document or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic document file but not make them apparent to the reader. 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.[150]

Sometimes the receiving party cannot easily access even the core data it seeks in electronic format. For instance, documents may be written in a proprietary language or in a program or version of a program long relegated to the annals of quaint computer software history.[151] Further, "databases by their nature disclose more than the data that is in them."[152] Revealing the structure of a computer program and/or the format of a database may disclose sensitive

---

148. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 12.

149. *Id.* at 30.

150. *Id.* at 20.

151. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1007614, at *7 (S.D.N.Y. May 16, 2002) ("In order to enable any statistical use of the [potentially relevant] data, the [defendant Department of Correctional Services] would have to affirmatively develop and provide to plaintiffs' experts the equivalent of a manual on how the data is encoded and organized.").

152. *Id.*

information that is not directly relevant to the controversy.[153]

Thus, the matter of delivery format where (potential) electronic production is at issue is a multi-faceted one. The knotty issues include: what is an electronic document, what are its essential features, which party gets to choose the form of production, and at what point in the discovery process. One court ruled that when "a party already possesses relevant information in electronic form, it is obligated, by way of mandatory disclosure, to so advise the adversary. Once advised of the existence of electronic data, a party may then make an informed decision as to the manner by which discovery could be produced."[154] However, the producing "party is not required to disclose to an adversary, absent an express request by the party or order of the court, any intention to prepare for trial by scanning [paper] documents into electronic form."[155] Another court ordered production to be made "in the native electronic format (or a mutually agreeable format)."[156]

---

153. *Id.*

> By producing the electronic material in raw form, the [defendant Department of Correctional Services] would disclose not only the underlying data sought by the plaintiffs, but also the organizational framework of the databases, which would effectively disclose a great deal about the way that [its proprietary system] maintains, stores, and classifies information. . . . [T]he plaintiffs' demands of necessity include the production of information that is not strictly speaking relevant to the case.

Id. In *In re Honeywell International, Inc. Securities Litigation*, the court held that any proprietary software the producing party might have to include with its production of electronic documents to make those documents decipherable was adequately protected by a stipulated confidentiality order. No. M8-85 (WHP), 2003 U.S. Dist. LEXIS 20602, at *6 (S.D.N.Y. Nov. 18, 2003).

154. *In re* Bristol-Myers Squibb Sec. Litig., 205 F.R.D 437, 441 (D.N.J. 2002).

155. *Id.*

156. United States v. First Data & Concord EFS, Inc., 287 F. Supp. 2d 69, 71 (D.D.C. 2003). In *Honeywell International*, the court ordered that documents already produced in hard copy form be produced in electronic format because that is

> how the documents are kept in the usual course of business. . . .
>
> . . . .
>
> . . . [The] Court directs [the producing party] to produce electronically its workpapers by either: (1) producing a copy of its workpapers on CD-ROMs that could be viewed using commercially-available software; or (2) producing a copy of its workpapers on CD-ROMs that could be viewed using [the producing party's] proprietary

Courts are also asked to rule on requests for on-site inspection of and direct access to the producing party's computer/information systems.[157]

The proposed amendments to FRCP 34(b) add language that attempts to clarify the procedures relating to form of discovery and the duties of the parties: it would allow the requesting party to "specify the form in which electronically stored information is to be produced."[158] The producing party would, in turn, be allowed to make "an objection to the requested form for producing electronically stored information, stating the reasons for the objection."[159] Finally, a proposed new subsection to the Rule, FRCP 34(b)(ii), would provide that "if a request for electronically stored

---

software, as well as producing the proprietary software to the extent it is necessary to view the workpapers. . . .

. . . .

. . . Finally, this Court declines [the requesting party's] invitation to rule on whether [the producing party] may convert some [of] its workpapers to a PDF file format to protect their integrity.

2003 U.S. Dist. LEXIS 20602, at *5–*7 (citations omitted).

157. *In re* Ford Motor Co., 345 F.3d 1315, 1316–17 (11th Cir. 2003) (basing its conclusion in part on the Advisory Committee's Notes to the 1970 amendments to FRCP 34(a)).

> 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 to copy the product—whether it be a document, disk, or other device—resulting from the respondent's translation of the data into a reasonably usable form.
>
> . . . Rule 34(a) does not give the requesting party the right to conduct the actual search.

Id. In *Playboy Enters., Inc. v. Welles*, the court allowed some degree of intrusion, ruling that the defendant had to provide a third party neutral expert access to its hard drive in order to copy the drive and recover deleted documents. 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999), *aff'd in part, rev'd in part*, 279 F.3d 796 (9th Cir. 2002). The defendant would then "review any recovered documents and produce to [the p]laintiff those communications that are responsive to any earlier requests for documents and are relevant to the subject matter of this litigation." *Id.* at 1055. The court explained that the "[p]laintiff needs to access the hard drive of [the d]efendant's computer only because [the d]efendant's actions in deleting those [discoverable] e-mails made it currently impossible to produce the information as a 'document.'" *Id.* at 1053.

158. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 26.

159. *Id.*

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."[160]

For more on method of production concerns including the definition of a document, form of production and metadata concerns, see supra Part II.

F. Interrogatories

A reasonable search of electronically stored information may need to be conducted in response to interrogatories.[161] The Civil Rules Advisory Committee explained how its proposed amendment to FRCP 33 would clarify the role electronic discovery and production plays in the response to interrogatories regarding business records, and acknowledged the issues that may still arise:

> The proposed amendments to Rule 33 clarify that an answer to an interrogatory involving review of business records should also involve a search of electronically stored information and permit the responding party to answer by providing access to that information. Consistent with the

160. *Id.* at 27. However, the Committee Note discussing the proposed FRCP 34(b)(ii) muddies the waters: "[It] provides that electronically stored information ordinarily need be produced in only one form, but production in an additional form may be ordered for good cause. One such ground might be that the party seeking production cannot use the information in the form in which it was produced." *Id.* at 31. The Committee opines that "[a]dvance communications about the form that will be used for production might avoid that difficulty." *Id.*

161. *See* Hayes v. Compass Group USA, Inc., 202 F.R.D. 363, 366 & n.5 (D. Conn. 2001) (requiring the defendant to electronically search for responsive files regarding age discrimination claims against it from the date of implementation of its computerized case management system in response to the plaintiff's interrogatories, but not requiring the defendant to conduct a manual search to find claims files from prior to that date for which only a general computer file listing the names of all types of litigants and the location of their paper files was available). In *Multitechnology Servs. v. Verizon S.W.*, the court ordered production of relevant, discoverable electronic information not discoverable from other sources in response to interrogatories. No. 4:02-CV-702-Y, 2004 U.S. Dist. LEXIS 12957, at *5 (N.D. Tex. July 12, 2004), *objection overruled by* No. 4:02-CV-702-Y, 2004 U.S. Dist. LEXIS 13622 (N.D. Tex. July 19, 2004). The court also ordered the litigants to split the cost incurred by conducting electronic discovery in response to interrogatories. *Id.* at *5–*6.

> option to produce hard-copy or paper business records in response to interrogatories, Rule 33(d) allows a responding party to substitute access to electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party. Under Rule 33(d), a party electing to respond to an interrogatory by providing electronically stored information must ensure that the interrogating party is able to locate and identify it as readily as the responding party, and the responding party must give the interrogating party a "reasonable opportunity to examine, audit or inspect" the information. [It is] recognize[d] that special difficulties may arise in satisfying these provisions as applied to electronically stored information. Aspects of the form in which the information is maintained or the need for a particular system to make it intelligible may require the responding party to provide some combination of technical support, information on application software, or other assistance. The key question is whether such support enables the interrogating party to use the electronically stored information as readily as the responding party.[162]

G. Sanctions

A wide array of penalties is available to courts to sanction parties for failure to make or cooperate in discovery, including entry of default judgment against the offending party, designating facts requested in discovery as established, or making an award of attorney's fees.[163] Where the decision to sanction a party in the electronic document arena varies significantly from the analysis in traditional paper discovery, is in the more complex assessment of spoliation.[164]

---

162. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 14–15.

163. *See* FED. R. CIV. P. 37.

164. *See* Lexis-Nexis v. Beer, 41 F. Supp. 2d 950, 954–56 (D. Minn. 1999) (the court was unable to determine that relevant electronic data was destroyed where the responding party deleted the original version of a discoverable database, but did produce a copy which it conceded was missing some data that had been overwritten—it claimed inadvertently—when it made the copy; coupled with the responding party's delay in turning over discoverable e-mails

> Most—but not all—courts require a level of fault beyond negligence before imposing a severe sanction—such as dismissing an action—for a party's failure to preserve discoverable material, depending in part on whether the failure has resulted in prejudice. Lesser sanctions—such as awarding the costs of discovery or attorney's fees—have been imposed without requiring such high culpability.[165]

One aspect of electronic information that makes the spoliation determination more difficult is the "unique and necessary feature of computer systems—the automatic recycling, overwriting, and alteration of electronically stored information. There is great uncertainty as to whether and when a party may continue some or all of the routine recycling or overwriting functions of its computer system without risk of sanctions."[166] The difficulty in divining spoliation in the electronic context is illustrated by the gymnastics of the court in "the fifth written opinion in [*Zubulake v. UBS Warburg LLC*] . . . . In order to decide whether sanctions are warranted, the following question must be answered: Did [the responding party] fail to preserve and timely produce relevant information and, if so, did it act negligently, recklessly, or willfully."[167] The court opined that "[o]ne of the primary reasons that electronic data is lost is ineffective communication with information technology personnel."[168] After a detailed description of communicative steps taken and missed to prevent spoliation, the court held that "[t]his case represents a failure of communication, and that failure falls on counsel and client alike."[169] The court then attempted to fashion sanctions that would primarily "restore [the plaintiff] to the position that she would have been in had [the responding party] faithfully discharged its discovery

---

in violation of a court order, the court held that the responding party's "actions—and his delay in revealing them to the opposing party—set off a high-tech wild goose chase that has needlessly multiplied the time and expense of this litigation. Accordingly, the court concludes that monetary sanctions are appropriate."); *see also* discussion *supra* note 56.

165. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 19.

166. *Id.* at 17.

167. Zubulake v. UBS Warburg LLC, No. 02 Civ. 1243(SAS), 2004 WL 1620866, at *1 (S.D.N.Y. July 20, 2004).

168. *Id.* at *10.

169. *Id.* at *10–*12.

obligations."[170] The sanctions ordered included an "adverse inference instruction with respect to [certain deleted] e-mails .... pay[ment by the responding party of] the costs of any depositions or re-depositions required by the late production .... [And] pay[ment of] the costs of this motion."[171] In the same case, the sanction for destruction of a backup tape was merely to pay the cost of producing a different backup tape that complemented an erroneously restored backup tape, to "recreate the lion's share of data [from the destroyed] tape," as well as to pay for re-depositions that might be warranted.[172]

A proposed amendment to FRCP 37 would add a new subsection in an attempt to provide guidance in the analysis of spoliation in the electronic data arena:

> (f) [Electronically Stored Information.] 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 information if:
>
> > (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.[173]

See infra Part VII. for a more wide-ranging, detailed discussion on spoliation, safe harbor and sanctions.

H. Conclusion

Information systems continue to evolve. Lawyers should continue to educate themselves. While the rules of discovery may be modified to reflect technological change, in our common law system

---

170. *Id.* at *12.

171. *Id.* at *13 (footnotes omitted).

172. *Id.* at *14 (footnotes omitted).

173. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *supra* note 2, at 31–32. However, the footnote to this proposed new subsection of FRCP 37 acknowledges that the issue is a knotty one: "Some have voiced concerns that the formulation set out [in the proposed amendment] is inadequate to address the uncertainties created by the dynamic nature of computer systems and the information they generate and store." *Id.* at 32 n.**.

statutes rarely provide all the answers.

The ways in which information can be generated, communicated and stored has expanded. At times, trying to fit a contemporary discovery scenario into the existing rules may seem like trying to squeeze into a favorite pair of pants. While some unease occurs, the basic tenets of discovery should provide lawyers the same basic comfort as that of a well-worn pair of pants that, after all, are only half a size too small. Lawyers should think of educating themselves (and their clients) about new information technologies and approaches to dealing with them in the discovery context, analogous to adjusting the pants; with careful consideration, minor alterations can have major results. A sober appreciation of the longstanding principles governing discovery, filtered through a realistic understanding of information technology and recent case law, makes a determination of the scope of discovery and method of production manageable.