6-1-2005

II. Defining Document in the Digital Landscape of Electronic Discovery

Shannon M. Curreri

II. DEFINING "DOCUMENT" IN THE DIGITAL LANDSCAPE OF ELECTRONIC DISCOVERY*

A. Introduction

In this era of modern technology, information is increasingly created in, conveyed in, stored in, and exchanged through digital or electronic media.[1] As a result, there has been a drastic growth in the amount of information to review and produce during the discovery phase of civil litigation. In addition to challenges raised by volume,[2] varying levels of sophistication with respect to technological expertise, system configurations, and data management add to the complexity of exchanging information in a coherent and comprehensive manner between adverse parties. Central to addressing the unique obstacles posed by electronic discovery is the need to define what constitutes discoverable electronically stored information. What that definition will encompass and in what form such information will be produced carries significant implications for the scope and cost of discovery, authentication, and overall litigation strategy.

---

* Shannon M. Curreri: J.D. Candidate, May 2006, Loyola Law School, Los Angeles; A.B. Princeton University, June 2000. My gratitude goes to the staff and editors of the *Loyola of Los Angeles Law Review* for their hard work, dedication, and encouragement. Special thanks to Heather Barber for her input and advice throughout this project. The ongoing support of my family and Laurence Treviño is also greatly appreciated.

1. One report estimates that 30% of all corporate records now exist *only* in electronic form. *See* Pike & Fischer, *Digital Discovery & e-Evidence*, *at* http://www.pf.com/law_internet_digitaldisc.asp (last visited Feb. 28, 2005); *see also* Joan E. Feldman, *Lost? No. Found? Yes: Those Computer Tapes and E-mails Are Evidence*, *at* http://www.forensics.com/pdf/Lost_no_Found.pdf (last visited Mar. 5, 2005).

2. To better understand the volume challenges created by electronic versus paper discovery, consider that a standard floppy disk contains enough data to fill 720 pages of text, a CD-ROM fills 325,000 pages of text, and the average laptop computer 20 gigabyte hardrive can store what in print would fill ten million pages of text. MICHAEL R. OVERLY, OVERLY ON ELECTRONIC EVIDENCE IN CALIFORNIA 4 (2004).

In August 2004, the Civil Rules Advisory Committee published proposed amendments to the Federal Rules of Civil Procedure to acknowledge the increasing role of electronic discovery in modern litigation.[3] The Committee's notes and the proposed rules' language warrant consideration for two major reasons. First, they draw attention to the scope of electronic discovery, the different mindset often needed in drafting and responding to electronic discovery requests, and the technological issues presented by the vast digital landscape. Moreover, the changes proposed by the Civil Rules Advisory Committee carry potentially far-reaching implications for the content, scope, and implementation of electronic discovery. While some proposals seek to codify practices already adhered to by many federal courts, others diverge from such efforts, and their impact and possible interpretations merit analysis.

Part A explores the definition of "document" in the context of electronic discovery. Part B covers the courts' treatment of requests for electronically stored information and then proceeds to describe the major types of electronically stored information and their potential utility in civil discovery. Part C deals with the distinctions between traditional documents and electronically stored information. In addition, it critiques the Advisory Committee's proposed approach to managing those differences. Part D focuses on the forms of production in which electronically stored information may exist and the implications of proposed Federal Rule of Civil Procedure (FRCP) 34(b)'s requirements. Finally, Part E briefly discusses electronically stored information in the context of depositions and interrogatories, and Part F examines judicial treatment of electronically stored information under selected rules of evidence and other litigation-relevant rules.

B. The Current Definition of "Document" Under Federal Rule of Civil Procedure 34(a)

Absent an explicit reference to "electronically stored information" in FRCP 34(a), judicial authorities have interpreted "document" requests to encompass varying amounts and types of

3. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE CIVIL RULES ADVISORY COMM. (2004), [hereinafter REPORT OF THE CIVIL RULES ADVISORY COMM.], *available at* http://www.uscourts.gov/rules/comment2005/CVAug04.pdf.

electronic information.[4] In general, electronically stored information encompasses a broad spectrum of information that does not fit within the traditional notion of a document. Thus, a variety of data, including meta data,[5] system data,[6] deleted data,[7] and legacy data,[8]

4. *See, e.g.*, Mosaid Techs., Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 336 (D.N.J. 2004) (holding plaintiff's request for documents, including "'typed . . . matter,' 'other data compilations,' 'letters,' 'correspondence,' 'notes to the files,' 'interoffice communications,' [and] 'statements,'" most certainly included defendant's e-mails); Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 96 (D. Md. 2003) (finding deleted e-mails are discoverable electronic records); Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 312, 317 (S.D.N.Y. 2003) (addressing whether the term document "'includ[es], without limitation, electronic or computerized data compilations'," the court permitted discovery of e-mails stored on backup disks); Metro. Opera Ass'n, Inc. v. Local 100, Hotel Employees Int'l, 212 F.R.D. 178, 209–10 (S.D.N.Y. 2003) (sanctioning defendants in a labor dispute, in part for their counsel's failure to instruct the defendant-client as to what constitutes a document, and proceeding to include e-mails, computer files, and files saved and deleted on a diskette as falling within this definition); Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (holding deleted computer files are discoverable under FED. R. CIV. P. 34(a)); Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428, 433 (S.D.N.Y. 2002) (identifying hard drives containing e-mails and back-up tapes as discoverable electronic information); United States v. Holihan, 236 F. Supp. 2d 255, 261–62 (W.D.N.Y. 2002) (granting defendant's motion to compel the production of documents, including a history of the bank's computer terminal "sign on" and "sign off" times and daily logs of computer entries); McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) (finding that e-mails on back-up tapes from a defined time period were discoverable and ordering their production); Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) (holding computer records that have been deleted are documents); Ranta v. Ranta, FA980195304S, 2004 Conn. Super. LEXIS 462, at *1 (Conn. Super. Ct. Feb. 25, 2004) (unreported) (ordering production of "programs, files and[/]or folders," as well as floppy disks, CDs, zip files, or other similar types of computer storage devices); Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462,015, at *2 n.3 (Mass. Super. Ct. June 16, 1999) (unreported) (permitting the broad definition of "document" to include "'any record . . . of any kind . . . however made, produced, or reproduced, or stored . . . [in] the form of any medium . . . including, without limitation, computer memory, [and] computer disk'" according to the MASS. R. CIV. P. 34, which mimics FRCP 34).

5. Meta data include information contained within an electronic file that hold information about that file, such as date of creation, author, source, history, and how the data was formatted. *See* Webopedia, *at* http://www.webopedia.com/TERM/m/meta_data.html (last modified April 26, 2001). "Meta data is essential for understanding information stored in data warehouses." *Id.*

all appear to meet the definition of electronically stored information and are potentially discovery-relevant. Due to the potentially "enormous" scope of electronic record requests,[9] some courts have limited the type of electronic information which may be sought.

Several observers have suggested using intent as a factor in determining whether electronically stored information is discoverable.[10] Thus, absent specific objections or agreement between parties, only data that a computer user intentionally enters and saves are fair targets of FRCP 34 requests.[11] Such a definition could severely limit the advantages associated with using electronically stored information to build a case, since this

---

6. System data include records regarding the "interdependent items that interact regularly to perform" a computer's tasks, including when user(s) logged on or off, Web sites visited, passwords used, and documents printed/faxed. Webopedia, *at* http://www.webopedia.com/TERM/s/system.html (last modified Feb. 19, 2003).

7. Deleted data include data that a user has "deleted" that are not actually removed from the hard drive until that space is needed to store actively-used data. *See, e.g.*, Webopedia, *Are Deleted Files Completely Erased?*, *at* http://www.webopedia.com/DidYouKnow/Hardware_Software/2002/erasing_Deleted_Files.asp (last visited Jan. 25, 2005); *see also infra* Part II.B.3.

8. Legacy data consist of stored information no longer used and only maintained on an obsolete system, which may cause requests for such data to be expensive and burdensome. *See* Alan Walter, *Modeling Networks—Leveraging Legacy Data*, *at* http://www.spatialinfo.com/pdf/Leveraging%20Legacy%20Data_Whitepaper-AW.pdf (last visited Mar. 5, 2005); *see, e.g.*, Webopedia, *at* http://www.webopedia.com/TERM/l/legacy_application.html (last visited Jan. 29, 2005).

9. *Thompson*, 219 F.R.D. at 96–97 (employing Rule 26(b)(2)'s cost-benefit balancing factors where electronic record requests might encompass "voice mail, e-mail, deleted e-mail, data files, program files, back-up files, archival tapes, temporary files, system history files, web site information in textual, graphical or audio format, web site files, cache files, [and] 'cookies'").

10. NINTH CIR. ADVISORY BD., PROPOSED MODEL LOCAL RULE ON ELECTRONIC DISCOVERY 4 (May 2004) (proposal to the Ninth Circuit and District Courts on the Ninth Circuit, presented to the Ninth Circuit Judicial Council on May 25, 2004, http://www.ce9.uscourts.gov/Web/OCELibra.nsf/0/ca95e32198b6592888256ea0006f1def?OpenDocument) http://www.krollontrack.com/library/9thCirDraft.pdf [hereinafter NINTH CIR. ADVISORY BD.]; *see also* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up To the Task?*, 41 B.C. L. REV. 327, 333 n.24 (2000) (noting that computers store a broad amount of ESI without a user's knowledge).

11. NINTH CIR. ADVISORY BD., *supra* note 10; *see also* Scheindlin & Rabkin, *supra* note 10 at 333 n.24.

characterization would preclude parties from requesting useful information such as meta data. Ultimately, however, "[a] discovery request aimed at the production of records retained in some electronic form is no different, in principle, from a request for documents contained in an office file cabinet"[12]—the end goal is to gather as much information as possible to support or defend the claims at issue.

1. Understanding Meta Data and Related Concerns

Perhaps the most important concept to grasp in understanding meta data is that they do not comprise separate documents; rather, they consist of pieces of information about the document, file, or application in which they are contained.[13] Defined simply, meta data are "data about data."[14] Defined more broadly, meta data "describe[s] how, when, and by whom an electronic document was created, modified, and transmitted."[15] Most types of electronic documents contain meta information, even though a printed document does not usually reveal such information.[16]

The primary benefits derived from using meta data are forensic capability and the ability to lend functionality to large volumes of randomly assorted electronically stored information.[17] The forensic, or investigatory, value of meta data exists because the data provide

12. Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *6 (Mass. Super. Ct. June 16, 1999) (unreported) (noting that "there is nothing about the technological aspects involved which renders documents stored in an electronic media 'undiscoverable.'").

13. *Id.*

14. Interactive Numeric & Spatial Information Data Engine, *What is Metadata*, INSIDE Tutorial, *at* http://www.insideidaho.org/tutorial/metadata/WhatIsMetadata.htm (last visited Feb. 28, 2005).

15. Carrie Davey, *Find It Fast: Leveraging Meta Data*, THE APPLIED DISCOVERY ORANGE PAGES ELECTRONIC DISCOVERY NEWSLETTER 1, 5 (Applied Discovery Aug. 2003), *at* http://www.lexisnexis.com/applieddiscovery/lawlibrary/newsletter/TheOrangePages_Aug03.pdf.

16. *See* OVERLY, *supra* note 2, at 3 (noting that word-processing files, spreadsheets, e-mail, records of instant messaging exchanges, Web pages, online order forms, databases, and digitized pictures, video, and audio files may include meta data).

17. *See* Chris O'Reilly & Jason Derting, *Electronic Disclosure—The Way Ahead*, *at* http://www.pagebid.com/tools/article_oreilly.asp (last visited Jan. 25, 2005) (noting that meta data can be extracted and added to field databases, enabling search capability).

clues not visible on a printed document, such as the author of a file, when the file was last saved or printed, whether someone made any revisions, and the identity of the user who edited the file.[18] In this way, meta data carry evidentiary value by supporting authentication of electronically stored information with details surrounding its creation, the way in which the information has been used, and even a chain of custody in some circumstances.[19] Meta data might also prove to be discovery-relevant in situations where the merits of a claim or defense depend on how and when various authors altered a document, or what information a witness possessed at a given time.[20] The process of using meta data to cull such investigatory information, otherwise known as "mining," tends to be most productive in reviewing e-mails and word processing files, but it can also reveal valuable information about other electronic document formats.[21]

---

18. *See* OVERLY, *supra* note 2, at 24.

19. The role of meta data in authentication can be demonstrated with the following hypothetical (based loosely on the Martha Stewart trial, United States v. Stewart, 323 F. Supp. 2d 606, 612 (S.D.N.Y. 2004)): Assistant Ann drafts a computer message on the afternoon of December 27, 2001. On January 31, 2002, Assistant Ann's boss views the December 27 message, deletes its contents and changes the title. Meta data will later enable one to determine which message was actually drafted on December 27, obtain the information needed to retrieve its contents, and distinguish it from the January message.

20. Scott Nagel, *Embedded Information in Electronic Documents: Why metadata Matters* (July 2004), *at* http://www.abanet.org/lpm/lpt/articles/nosearch/ftr07044_print:.html. The utility of meta data, in combination with system data, has been demonstrated in numerous cases. *See, e.g.*, R.S. Creative, Inc. v. Creative Cotton, Ltd., 89 Cal. Rptr. 2d 353, 356–57 (Ct. App. 1999) (discussing how a computer expert revealed the precise dates on which a computer and laptop had been used and the name of a word processing file deleted in the relevant time frame).

21. Robert Douglas Brownstone, *Collaborative Navigation of the Stormy E-Discovery Seas*, 10 RICH. J.L. & TECH. 53, *2 (2004), http://law.richmond.edu/jolt/v10i5/article53.pdf. Meta data contained in word-processing documents, for example, can reveal the timing and content of prior revisions, recipients of those versions, and the identities of prior recipients who did not receive subsequent versions of the document. *Id.; see also* Nagel, *supra* note 20 (explaining that "track changes" showing modifications by multiple recipients contain meta data, as do CAD drawings that can reveal who created previous versions of an architectural design).

Another highly attractive feature of meta data is that they add functionality to large sets of electronically stored information.[22] A typical paper document production will involve individual review of files for privileged content and extensive categorizing and coding of files to comply with FRCP 34(b). With meta data, technical experts can easily search, filter, and categorize electronically stored information.[23] Once an opponent produces electronically stored information, the requesting party can use meta data to track down words, phrases, data, particular documents, messages, and even fragments that are responsive to the request.

a. Production and form

Meta data typically become a factor in discovery via one of two routes. In some instances, meta data are introduced into the discovery landscape when a responding party opts to produce documents in native electronic format[24] or when a requesting party specifies native file format as the form of production. The requesting party may then access meta data from the electronic documents.[25] The other way in which meta data enter the discovery picture occurs when a document demand specifies that documents be produced in document image format, with accompanying meta data, such that the

22. *See* OVERLY, *supra* note 2, at 5.

23. Computer forensic experts are typically hired to perform the search and often create a functional database that can be easily searched by attorneys. *See id.* Databases enable users to filter out irrelevant material and eliminate the need to manually code information according to type of document (e.g. presentation, correspondence, spreadsheet). An entire industry has sprung up around the provision of electronic discovery services, with involved parties spending over $500 million in 2003. *Conference Report: Judicial Panelists Debate Need for Rules Covering Discovery of Electronic Data*, 72 U.S. LAW WEEK 2519, 2520 (2004).

24. Native format refers to a file in its original format, including the software program used to create the file. *See* Sue Chastain, *Native File Format*, http://graphicssoft.about.com/od/glossary/g/nativeformat-P.htm (last visited Jan. 25, 2005). This is in contrast to a document image, which is essentially a photograph of the document stored in either portable document format ("PDF") or one of several other image formats, such as tagged image file format ("TIFF") or joint photographic experts group ("JPEG"). *See id.*

25. This requires access to the software programs that originally created the files. *See* Michael M. Wechsler & Michele C.S. Lange, *Digging for Data: Today's Discovery Demands Require Proficiency in Searching Electronic Documents*, N.Y. ST. B. J., Mar.–Apr. 2004, at 18, 22.

responding party carries the initial burden of revealing the underlying meta data. Requesting documents in a universal image format accompanied by meta data avoids the need for a requesting party to obtain the software programs needed to read native format files.

"Meta data" is not explicitly mentioned in either the current version of FRCP 34, or in the proposed amended rule.[26] However, the recently published Report of the Civil Rules Advisory Committee (and underlying principles governing the federal discovery rules) supports the notion that production requests seeking files with all associated meta data "should be conditioned upon a showing of need or sharing expenses."[27] This comment raises an interesting issue that hinges on the form in which a party requests electronically stored information. Meta data are only accessible when a party produces electronic files (e.g., word processing documents, spreadsheets, power point presentations, e-mails) in native file format.[28] Thus, if a responding party provides electronic information in native format, there will be no need for a separate request for meta data since such data are accessible from the files themselves.[29] However, in situations where a party produces electronically stored information in either paper or document image format, a separate request for meta data may be made if the authenticity of the documents or files is in question.[30] It is in this latter scenario where parties might need to make a precise showing for why meta data are relevant before a court orders their production. Even in the former scenario of native file production, the question remains: who should bear the cost of hiring experts to "mine" the meta data and lend sophisticated searching capability to the file set?

---

26. FED. R. CIV. P. 34; REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 24–25 (proposed amendment to Rule 34(a)).

27. *Id.* app. at 14 (internal citation omitted). The good cause analysis under FED. R. CIV. P. 26(b)(2)(i–iii) provides at least a framework for parties who disagree over the scope of a production request for meta data. For a more in-depth discussion of how to determine whether the scope of an electronic document production request is reasonable, and related fee-shifting issues, see *infra* Part III.D.1 and Part IV.C.2, respectively.

28. *See* Wechsler & Lange, *supra* note 25, at 22.

29. *See id.*

30. *Cf. infra* note 231 and accompanying text.

At least one federal court, pursuant to FRCP 34, has included meta data, absent such a precise showing of need, when ordering the production of documents.[31] In large part, it appears that judicial activity in this area is in response to the obvious utility of meta data in authenticating a document, or in establishing facts material to a dispute.[32]

Although courts have not expressly declined to order the production of meta data, a court would probably do so if the request for their production placed too high a burden on the responding party, or if the data were highly unlikely to lead to the discovery of admissible evidence. One argument offered for not requiring the production of meta data is that while they are generated and stored as a byproduct of parties' ordinary course of business, meta data "are not routinely retrieved and used for business purposes."[33] Nevertheless, it appears that meta data will only play a more prominent role in electronic discovery as methods for retrieving it become more accessible to litigants. While blanket requests for meta data associated with all requested electronically stored information will be unreasonable in most circumstances, meta data requests will be appropriate where the authorship or timing of a particular document is relevant to a claim or defense.[34]

---

31. *See* Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 143 (2004) (ordering the production of documents, including "[i]nformation that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata").

32. *See id.*; *see also* Tulip Computers Int'l v. Dell Computer Corp., No. CIV.A. 00-981-RRM, 2002 WL 818061 (D. Del. Apr. 30, 2002). The court in *Tulip Computers* recognized the value of enabling the plaintiff to use meta data to search a CD-ROM of e-mails ordered to be produced by defendant. *Id.* at *4, *7. The plaintiff was permitted to search the e-mails (using meta data) for specified key words, including plaintiff's name and code words for the product at issue in the patent infringement suit. *Id.* at *4. Plaintiff, in turn, would request that defendant produce e-mails shown to be responsive to the key word search. *Id.* at *7. In this way, the use of meta data narrowed an otherwise broad request for countless e-mails to a defined set of potentially relevant documents.

33. Ronald J. Hedges, *Discovery of Digital Information* 4 (Sept. 27, 2004) (quoting THE MANUAL FOR COMPLEX LITIGATION §11.446 (Judge Stanley Marcus et al. eds., 4th ed. 2004), *at* http://www.kenwithers.com/articles/hedges092704.pdf).

34. Spoliation of meta data may, in fact, become more of an issue as production in native file format increases. For a thorough discussion on judicial treatment of the spoliation of electronic evidence, see *infra* Part

b. A brief note on native file review and production

Although the production of electronically stored information in native file format may carry significant advantages for both propounding and responding parties,[35] there may be circumstances under which a propounding party would prefer to have information produced in document image format—or even hard copy—depending on cost concerns, the purpose for which the information will be used, and the size of the litigation team.[36] Thus far, judicial acknowledgement of the native file versus document image dilemma has been limited; courts seem to focus on the request at issue and rarely meddle in a requesting party's preference for native files over document images, or vice versa.[37] As technologies continue to develop and make native file review and production more convenient, this form of production may supersede, or at least supplement, the review and production of document images.[38]

VII.A.2.

35. *See* Wechsler & Lange, *supra* note 25, at 22 (describing the advantages of native file production as follows: "Some believe that reviewing native files as a whole is somehow more holistic, or that it offers some 'special' information, or that it is more cost-effective than reviewing documents converted to .tiff or .pdf—perhaps because the files are reviewed exactly as they were created and no data conversion is needed.").

36. *See id.* at 23 ("Others believe that conversion of files to a uniform format is the best choice because it allows the lawyer all of the advantages of high-speed processing technology, and there is no need to have "native" applications on every computer used in the review. . . . In short, many believe that document conversion is the fastest and most inexpensive method for narrowing down thousands and millions of electronic documents for review and ultimately for finding and producing responsive documents.").

37. *But see* United States v. First Data, 287 F. Supp. 2d 69, 71 (D.D.C. 2003) (instructing the parties to "produce documents in either hard copy form, or, in the case of electronic documents, in the native electronic format (or a mutually agreeable format)"). Judicial activity in this area is likely to grow as native file production becomes more appealing.

38. Parties utilizing electronic documents, whether they are standard image format files or native files, may use either litigation databases or online repositories to review information. *Wechsler & Lange*, *supra* note 25, at 23. Litigation databases are localized, whereas online repositories allow attorneys to access the database remotely through a secure connection. *See id.* With online repositories, parties place documents onto a web-based tool that enables both viewing and searching. *Id.* Repositories convert documents to either document images or a file that contains both text and meta data, thus preserving the benefits of the native file. *Id.* In the past, one of the major disadvantages associated with native file review was the inability to redact and

c. Cost concerns related to meta data

For the aforementioned reasons, meta data are often a focal point of discussions focusing on the benefits of electronic discovery. However, the utilization of meta data may be more expensive and resource intensive than traditional indexing and organization of paper documents.[39] Nevertheless, the utility of meta data, with respect to both functionality and investigatory potential, increasingly appears to justify incurring the added expense of hiring experts to mine meta data from an opponent's electronically-produced documents. This is particularly so if the authorship or timing of a file's creation is critical to a party's claim.[40]

2. Embedded Data

Like meta data, embedded data is "information about a document"[41] and consists of substantive information within its host electronic file.[42] Embedded information may consist of embedded comments, a "blind copy" or "bcc" field of an e-mail, or even hidden columns in a spreadsheet.[43] Most word processing and spreadsheet

---

Bates stamp (both are possible with document images). *Id.* at 22. Now, however, some online repositories allow users to view documents both as images and as native files, thereby enabling attorneys to harness not only the organizational benefits of images, but also the searching and investigatory potential of native files. *Id.* at 23.

39. Whether using meta data is more expensive than traditional paper-based discovery depends on the resources available to the litigation team. Some litigants may have access to in-house technical experts who can extract meta data and use that information to search files. Other litigants may require outside hiring of consultants to perform these tasks, which adds to the overall expense of litigation.

40. An actual cost-benefit analysis of the use of meta data during discovery could assist litigants in deciding whether to shoulder, or perhaps share, the burden of hiring consultants to mine meta data from electronic documents. It does not appear that a thorough cost-benefit comparison of paper versus electronic discovery has been undertaken, although one source has quoted the average cost of paper discovery at $2.20–$3.54 per page, and electronic discovery at less than $0.25 per page. *See* Greg McPolin, *E-Discovery: A Common Term That is Little Understood*, N.Y. L.J., Jan. 27, 2003, at T5.

41. OVERLY, *supra* note 2, at 24.

42. *Id.*

43. *See* Mary Kay Brown & Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 30 LITIG. 31, 32 (2003), *available at* http://www.bipc.com/documents/pdf/article_897.pdf. Embedded data can be likened to a Post-It note that one sticks on a paper draft to make comments

programs track the editorial history of their files.[44] Moreover, editorial comments, whether textual or digitally recorded spoken comments, comprise embedded data and can be "fruitful sources of evidence."[45] One of the main distinctions between embedded and meta data is that embedded data are almost always created intentionally, whereas meta data tend to be generated automatically, and most users are unaware of the data's existence beyond what they can find by looking at the "properties" feature of a file.[46]

Because extracting embedded data generally requires technical expertise, these types of discovery requests implicate cost and time concerns. Whether judges will permit unfettered requests for discovery of embedded data remains to be seen, but courts will probably continue to review the reasonableness of such requests according to the guidelines provided by FRCP 26.[47]

3. Deleted Data

Most computer users can relate to the unfortunate experience of accidentally deleting a needed file, or seemingly losing an electronic document when a computer freezes or power is disconnected. Yet, common experience also reveals that much of this "deleted" information is, in actuality, still located on a computer's hard drive and thankfully can be retrieved. In the case of discovery-relevant deleted data, however, a producing party might be disappointed to find that data still exist, particularly if the information is harmful to the party's case.[48]

When a program recovers deleted data from a hard drive, it is typically the result of one of two processes. In one instance, the program in which the user is working automatically creates and

---

or remind an author of changes that need to be made.

44. OVERLY, *supra* note 2, at 24.

45. *Id.*

46. Hon. Shira Ann Scheindlin et al., Panel Discussion, *Rules 33 and 34: Defining E-Documents and the Form of Discovery*, 73 FORDHAM L. REV. 33, 42–43 (2004) (Judicial Conference Advisory Committee on the Federal Rules of Civil Procedure: Conference on Electronic Discovery) (comments of Paul M. Robertson).

47. For an in-depth discussion of form and reasonableness of requests, see *infra* Part III.C.1(b) and D.1.

48. As two lawyers recently noted: "E-limination is difficult." Jerold S. Solovy & Robert L. Byman, *Discovery in the E-Age*, NAT'L L.J., Mar. 15, 2004, at 11.

periodically saves copies of the file in other files known as "replicant data," temporary files, or "file clones."[49] In the other instance, pressing the delete button does not permanently delete the file. Instead, the program removes the file from directory listings and the bits and bytes that comprise the file remain on the hard drive.[50] Once the space occupied by these deleted bits and bytes is needed for new data, the file is overwritten.[51]

Judicial decisions in a number of federal district courts have made it clear that deleted computer files fit under the definition of "documents" in FRCP 34, thus qualifying as discoverable electronically stored information.[52] Likewise, courts have made

---

49. *See* Joan E. Feldman & Rodger I. Kohn, *The Essentials of Computer Discovery*, *in* 2 THIRD ANNUAL INTERNET LAW INSTITUTE 51, 54 (1999).

50. *Id.* at 55.

51. *Id.*; *see also* OVERLY, *supra* note 2, at 43–44 (noting the portions of the deleted file remain on the disk until they are overwritten by new data). Advances in modern computer forensics, such as Magnetic Force Microscopy ("MFM"), have expanded the ability to retrieve deleted data. *Id.* at 43. Overwriting data can be thought of as a process in which layers of data are created. *Id.* Thus, when the area occupied by a deleted file on a hard drive is overwritten to make space for new data, the deleted data remains, but is one layer "deeper" in the hard drive. *See id.* Whereas previously forensics experts believed that overwriting an area nine times made deleted data sufficiently deep or inaccessible, MFM technology makes recovery possible where space has been overwritten in excess of a dozen times. *Id.*

52. *See, e.g.*, Anderson v. Crossroads Capital Partners, No. Civ.01-2000 ADM/SRN, 2004 WL 256,512, at *2 (D. Minn. Feb. 10, 2004) (acknowledging the Magistrate Judge's order that plaintiffs produce "a 'copy of all documents/files relevant to this litigation that exist on Ms. Anderson's personal computer as well as those that have been deleted or otherwise adulterated.'"); Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) ("[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable."); Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428, 431 (S.D.N.Y. 2002) (stating that "[e]lectronic documents are no less subject to disclosure than paper records," and questioning who should bear the cost of such discovery, especially for back-up tapes or deleted e-mails); McPeek v. Ashcroft, 202 F.R.D. 31, 32, 34 (D.D.C. 2001) (declaring that, "[d]uring discovery, the producing party has an obligation to search available electronic systems for information demanded," and ordering a limited back-up restoration of e-mails); Kleiner v. Burns, No. 00-2160-JWL, 2000 WL 1,909,470 at *4 (D. Kan. Dec. 15, 2000) (noting that Rule 26 (a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that "[t]he 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

deleted data the subject of protective orders.[53] Although deleted data are retrievable, they are not nearly as accessible as meta data.[54] Due to the technical expertise required to recover once-deleted files and their inherent inaccessibility, some judicial bodies have proposed that responding parties only be required to preserve, review, or produce deleted (or residual) data or documents upon a showing of special need and relevance.[55]

Courts have varied in their approach to ordering the production of deleted data.[56] In *Playboy Enterprises, Inc. v. Welles*,[57] for example, the court ordered the production of deleted e-mails on the defendant's computer system because "the probability that at least some of the e-mail may be recovered is just as likely, if not more so, than the likelihood that none of the e-mail will be recovered."[58] Moreover, the production order was contingent on the plaintiff's ability to provide an expert report demonstrating the feasibility of the production.[59] The court in *Simon Property Group v. mySimon, Inc.*,[60] however, required the plaintiff's expert to report findings to the court as to the scope and volume of work performed, as well as any "available information showing when any recovered 'deleted' file was deleted"[61] and "available information about the deletion and contents of any deleted file that cannot be recovered."[62] In the

---

any 'deleted' electronic data"); Simon Prop. Group v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("First, computer records, including records that have been 'deleted,' are documents discoverable under FED. R. CIV. P. 34."); Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) ("Plaintiff needs to access the hard drive of Defendant's computer only because Defendant's actions in deleting those e-mails made it currently impossible to produce the information as a 'document.'").

53. *See, e.g.*, Aero Prods. Int'l v. Intex Recreation Corp., No. 02 C 2590, 2004 WL 417,193, at *2 (N.D. Ill. Jan. 30, 2004) (discussing a previously entered protective order requiring the defendant to recover "any and all destructed electronic documents, including e-mail.").

54. *See* NINTH CIR. ADVISORY BD., *supra* note 10, at 3 (noting active data permits efficient searching and retrieval while production of backup tape data is burdensome and costly).

55. *See id.*

56. *See infra* notes 57–63.

57. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

58. *Id.* at 1054.

59. *Id.* at 1054–55.

60. 194 F.R.D. 639 (S.D. Ind. 2000).

61. *Id.* at 641.

62. *Id.*

interest of efficiency, the court also limited recovery to word-processing documents, e-mail, Power Point or "similar presentations," spreadsheets, and other similar files, avoiding the need to recover files comprising operating systems or higher level programs that are probably irrelevant to discovery.[63]

4. Other Sources of Potentially Relevant Electronically Stored Information

Other sources of electronic data exist in the scheme of the digital landscape, including residual (or ambient) data, migrated data, system data, legacy data, backup data, temporary files, mirror disks, instant messages, and internet related data, such as history and cookie files.[64] Each fits within the broad definition of electronically stored information, although the reasonableness of requests for such data will vary depending on the nature of a litigant's claims.[65] In many circumstances, a propounding party will likely need to make a specific justification for requesting these types of data if their potential relevance is not readily apparent.

a. Backup data

Backup tapes, on which backup data are typically stored, "are by their nature indiscriminate,"[66] meaning "they capture all information at a given time from a given server, but do not [sort the information] by subject matter."[67] Federal and some state courts have generally accepted backup data as discoverable, particularly in instances where relevant e-mails are known or highly suspected of being located on backup tapes.[68]

---

63. *Id.*

64. "Cookies" consist of small data files which are installed on a visitor's hard drive upon visiting a Web site. OVERLY, *supra* note 2, at 30–32. When the Web site is revisited, the site reads the cookie file to track areas of interest to the repeat visitor and collects additional marketing information. *Id.* at 31. Most users are able to select a feature on their Web browser to block the acceptance of cookies. *See id.* at 31–32.

65. Arguably, some of these types of information do not fit within the four corners of Federal Rule of Civil Procedure 34. *See* Scheindlin & Rabkin, *supra* note 10, at 350–51.

66. McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001).

67. *Id.*

68. *See, e.g.*, Zubulake v. UBS Warburg, 217 F.R.D. 309, 313–14 (S.D.N.Y. 2003); Rowe Entm't, Inc. v. William Morris Agency, Inc., 205

b. Legacy data, residual data, and system data

Less familiar sources of potentially discoverable electronically stored information include legacy data, residual data, and system data. Legacy data, or "applications", are those "in which a company or organization has already invested considerable time and money."[69] Thus, "[a]n important feature of new software products is the ability to work with a company's legacy applications, or at least be able to *import* data from them."[70] Discovery of legacy data typically becomes an issue when a party maintained or stored information in a proprietary system that is no longer in use, or in a system that has been rendered obsolete by newer, or more sophisticated programs.[71] One could imagine circumstances in which the need for legacy data is pressing enough to warrant its production while the cost of converting the data into an understandable or usable format is a definite concern. Residual data are data that are no longer active on a computer system.[72] Residual data requests often coincide with

---

F.R.D. 421, 428–29 (S.D.N.Y. 2002); Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 52 Fed. R. Serv. 3d 168, 171–73 (E.D. La. 2002) (ordering the production of defendant's backup tapes under one of two proposed protocols); Kaufman v. Kinko's Inc., No. Civ.A. 18894-NC, 2002 WL 32,123,851, at *2 (Del. Ch. Apr. 16, 2002) (explaining its granting a motion to compel production of e-mails retrievable from defendant's backup system, the Delaware court stated that "[u]pon installing a data storage system, it must be assumed that at some point in the future one may need to retrieve the information previously stored"); Renda Marine, Inc. v. United States, 58 Fed. Cl. 57, 62 (2003) (ordering the production of backup tapes that were the subject of plaintiff's original FED. R. CIV. P. 34 request, as well as other subsequently-created backup tapes); *In re* CI Host, Inc., 92 S.W.3d 514, 516–17 (Tex. 2002) (affirming the trial court's order for the production of back-up tapes, which plaintiffs had requested under TEX. R. CIV. P. 193(2)(b), noting that Rule 193(2)(b) "permits discovery of electronic recordings, data, and data compilations").

69. Webopedia, *Legacy Application*, at http://www.webopedia.com/TERM/l/legacy_application.html (last visited Feb. 27, 2005).

70. *Id.*

71. *See* REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, at 11 (describing legacy data as "information that is no longer used and only maintained on an obsolete system, making it expensive and burdensome to restore and provide").

72. *See* Feldman & Kohn, *supra* note 49, at 55 ("*Residual data* is information that appears to be gone, but is still recoverable from the computer system. It includes 'deleted' files still extant on a disk surface and data existing in other system hardware such as buffer memories of printers, copiers and fax machines."). Residual data have been analogized "to data on crumpled

requests for deleted data, since residual data may consist of old deleted data stored in "slack space."[73] Lastly, system data consist of information recorded by a computer regarding a "variety of routine transactions and functions, including password access requests, the creation or deletion of files and directories, maintenance functions, and access to and from other computers, printers, or communication devices."[74] Parties suspecting spoliation might—and often should—request system data to conduct investigatory efforts.

The aforementioned categories of data share a common feature concerning the reasonableness of their accessibility. Comments recently submitted to the Civil Rules Advisory Committee pointed to legacy, backup, and fragmented data (which can include residual data) as examples of data that in many circumstances will be not be reasonably accessible and therefore should be subject to discovery requests only upon judicial order and a showing of good cause.[75] Whether the amended Rules further open the door for requests of these data, or make their discovery more difficult, the problem of remotely accessible forms of data only promises to increase as

---

newspapers used to pack shipping boxes." Hedges, *supra* note 33, at 4 (quoting THE MANUAL FOR COMPLEX LITIGATION §11.446 (Judge Stanley Marcus et al. eds., 4th ed. 2004)).

73. File slack space is "the space that exists from the end of a file to the end of the last cluster" it occupies on a hard drive. Jack Seward & Daniel A. Austin, *E-Sleuthing and the Art of Electronic Data Retrieval: Uncovering Hidden Assets in the Digital Age: Part II*, AM. BANKR. INST., Mar. 2004, at 54, *available at* http://www.e-evidence.info/seward2.pdf. "Computer files are created in changing lengths depending on their size [and] it is seldom that the file size will match the size of the available cluster to which it is assigned." *Id.*

74. Hedges, *supra* note 33, at 4.

75. *See, e.g.*, Letter from Hon. Ronald J. Hedges to Peter McCabe, Secretary, Committee on Rules of Practice & Procedure 2–5 (Feb. 8, 2005) (criticizing the potentially benign effect of the good cause standard), *available at* http://www.uscourts.gov/rules/e-discovery/04-CV-169.pdf; Letter from Thomas Y. Allman to Peter McCabe, Secretary, Committee on Rules of Practice & Procedure 3–4 (Dec. 28, 2004) (providing comments on Proposed Civil Rule Amendments, Including Electronic Discovery), *available at* http://www.uscourts.gov/rules/e-discovery/04-CV-007.pdf; Letter from Microsoft Corp. to Peter McCabe, Secretary, Committee on Rules of Practice & Procedure 6–9 (Dec. 16, 2004) (providing comments on Proposed Civil Rule Amendments, Including Electronic Discovery), *available at* http://www.uscourts.gov/rules/e-discovery/04-CV-001.pdf ; *see also* Part III.D, on tier two discovery.

technological advances continue to replace older systems and programs.

c. Instant messaging logs

Instant messaging ("IM") represents another source of electronic documentation whose significance has grown in recent years due to the expanded ability to capture IM sessions.[76] Public IM is perhaps the more well-known type of IM, but increasingly business enterprises are establishing corporate IM programs that enable employees to chat with one another via IM conversations.[77]

IM works in the following manner: a user downloads IM software, enabling her to send nearly instantaneous messages to other software users who are online at the same time.[78] The IM server essentially notifies the user that other "friends" are online and logged into the server.[79] When one user contacts another and the recipient accepts, the server links the two directly, thus removing itself from the transmission of information.[80] Even though the server links users directly to one another, the conversation is nevertheless maintained on the IM service provider's server.[81]

---

76. OVERLY, *supra* note 2, at 19.

77. *See* Dmitry Shapiro, *Instant Messaging and Compliance Issues: What You Need To Know*, (May 27, 2004), *at* http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci967281,00.html.

78. *See generally* Deborah H. Juhnke & David P. Stenhouse, *Instant Messaging: What You Can't See Can Hurt You (in Court)*, Computer Forensics Inc. (2004) (describing how instant messaging functions), *at* http://www.forensics.com/pdf/Instant_Messenger_Programs.pdf; *see also* Federal Deposit Insurance Corporation, *FDIC Financial Institution Letters: Guidance on Instant Messaging* (FDIC Financial Institution Letters, July 2004) ("IM products available on the Internet are unofficially used in many organizations. There are two ways that IM products enter the workplace. The first is referred to as Server Proxy, in which messages pass through the IM vendor's computer and are forwarded to the user. The second is by Server Broker, in which messages are passed to the IM vendor only to initiate the communication between users, who then communicate directly with each other."), *at* http://www.fdic.gov/news/news/financial/2004/fil8404a.html.

79. Juhnke & Stenhouse, *supra* note 78.

80. *Id.*

81. *See* Jeff Tyson, *How Instant Messaging Works*, HOW STUFF WORKS, *at* http://computer.howstuffworks.com/instant-messaging.htm (last visited Feb. 27, 2005). How long the conversations are stored on the IM provider's server will vary according to the provider's business practices. *See id*; *see also* Michael Gartenberg, *Being Careful with IM Use*, COMPUTER WORLD

In the case of corporate IM, the conversation is often captured on the enterprise's server and thus easily subject to a discovery request if believed to be reasonably calculated to lead to the discovery of admissible evidence.[82] With public IM, the user's hard drive does not generally log conversations because the IM software transmits the messages to the external IM provider's server.[83] However, businesses increasingly use software designed to capture such conversations to monitor and log employee messages.[84] Additionally, new applications, such as the "Google Desktop Search," promise to make the discovery of instant messages and browser cache files[85] significantly easier than in the past.[86]

(May 27, 2002), *at* http://www.computerworld.com/printthis/2002/0,4814, 71447,00.html.

82. Ongoing investigations into the objectivity of stock assessments by Wall Street analysts illustrate how content relayed on corporate intranets could prove to be relevant to a claim. *See* Noam Cohen, *Word for Word / Mixed Messages; Swimming With Stock Analysts, or Sell Low and Buy High . . . Enthusiastically*, N.Y. TIMES, May 5, 2002, §4 (providing excerpts from e-mail messages sent from and to an analyst at the center of an investigation by New York Attorney General Eliot Spitzer), 2002 WLNR 4046668. Despite the potential relevancy of instant messaging conversations, the hearsay rule may be a barrier to the admissibility of statements made. Although the investigation primarily concerned the exchange of e-mail messages, one could easily imagine some of the intra-corporate correspondence occurring via instant messaging. If the firm had software in place to capture these hypothetical conversations, their content could find its way into the hands of opposing counsel. For hearsay hurdles to the admissibility of e-mail and other internet-related evidence, see *infra* Part VI.E.1(b).

83. *See* Juhnke & Stenhouse, *supra* note 78, at 2.

84. Software such as "IM Auditor" allows network administrators to map instant message conversations, link screen names to actual users, and log conversations going to and coming from the instant messaging server. *See* Peter Sayer, *Who's Monitoring Your Instant Messages?* (Feb. 5, 2002), *at* http://www.pcworld.com/reviews/article/0,aid,82764,src,ov,00.asp.

85. "Caching" is the "process of storing popular or frequently visited Web sites" on the computer's RAM in order to expedite the retrieval of information from memory rather than the internet. OVERLY, *supra* note 2, at 31–32.

86. For more information regarding the Google Desktop Search, see Danny Sullivan, *A Closer Look at Privacy & Desktop Search* (Oct. 14, 2004), *at* http://www.searchenginewatch.com/searchday/article.php/3421651, and Google Desktop, About Google Desktop Search, *at* http://desktop.google.com/about.html (last visited Feb. 9, 2005).

d. Temporary files

Temporary files are those that "are created for purposes of a particular computer session and then automatically deleted when that session is completed."[87] Many programs, such as word processing programs, create temporary files any time a user opens a new document.[88] These temporary files store editing information (e.g. cutting and pasting), as well as other types of information pertaining to the document.[89] Once the program saves the document to disk, the program deletes the temporary information.[90] However, if there is a system failure, if the program closes without saving, or if power is lost, the temporary files will remain and may reveal copies of documents not otherwise obtainable.[91]

e. Mirror disks

Mirror disks often complement a network's primary hard disk and serve as a backup for important systems.[92] Such disks are typically arranged so that every time a program saves information to the primary disk, the program also stores that information on the mirror disk.[93] Thus, they become a potential source of apparently lost electronically stored information.[94] A responding party with an established mirror system who tries to claim that certain documents are irretrievable due to a system "crash" can be thwarted by pointing to the presence of the information on the mirror drive.[95] One court recently found that mirror disks are particularly useful in allowing an expert to conduct a thorough examination of an opposing party's hard drive using sophisticated off-location equipment.[96]

---

87. OVERLY, *supra* note 2, at 21–22.
88. *Id.* at 22.
89. *Id.*
90. *Id.*
91. *Id.*
92. *See id.* at 22–23.
93. *Id.* at 23.
94. *See id.*
95. *Id.*
96. *See* United States v. Alexander, No. 04-2005-BC, 2004 WL 2,095,701 (E.D. Mich. Sept. 14, 2004). In *Alexander*, the defendant was criminally charged with receiving obscene pictures over the Internet. *Id.* at *1. The defendant requested that the government provide him with a mirror disk to allow his expert to conduct an examination in his own laboratory, including an analysis of whether defendant knowingly received the contested images. *Id.* at

f. Additional electronic storage devices

Internet cache files or computer users' cookie files may also prove to be discoverable electronically stored information.[97] Such files could provide a requesting party with information on when a user visited particular Internet sites, or if a party uses employee-monitoring software. This software tracks a variety of actions employees take while using their computers, providing relevant information regarding either internet usage or document creation and editing.[98]

C. Distinguishing "Document" From "Electronically Stored Information" and Other Proposed Changes to Federal Rule of Civil Procedure 34(a)

The proposed amendment to FRCP 34(a) carves out a category for electronically stored information.[99] One of the major reasons for the proposed distinction is that the term "documents" does not adequately encompass or describe electronically stored information.[100] The Advisory Committee and courts have drawn numerous distinctions between paper and electronic documents,[101] and the discovery of each, including both quantitative and qualitative differences.[102] Indeed, the differences have resulted in

---

*9. Because it was possible that the mirror disk contained relevant dates, times, and circumstances surrounding the receipt of obscene pictures, the court ordered its production. *Id.*

97. *See, e.g.*, Giardina v. Lockheed Martin Corp., No. Civ.A. 2-1030, 2003 WL 1,338,826 (E.D. La. Mar. 14, 2003) (ordering defendant to respond to an interrogatory request for a list of non-work related Internet sites visited by employees in a department of plaintiff's employer throughout a specified time period).

98. *See* OVERLY, *supra* note 2, at 33.

99. *See* REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 24–25 (proposed amendment to Rule 34(a)(1)).

100. *See id.* at 15.

101. The author recognizes that "documents" refers not only to paper documents, but also includes drawings, graphs, charts, and phonorecords. The logic behind the distinction between some of the sub-categories listed as documents, on the one hand, and electronically stored information, on the other, will be explored in Part II.C.1.

102. *See* NINTH CIR. ADVISORY BD., *supra* note 10, at 1–2; REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, at 2–3; Corinne L. Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257, 259–62 (2000); Hedges, *supra* note 33, at 1–2.

fundamentally altered forms of communication through which individuals exchange information and ideas:

> 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 . . . thus multiplying the volume of documents. . . . [U]nlike most paper-based discovery, archived e-mails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes which have become obsolete.[103]

Electronically stored information itself is dynamic in the sense that it is incomprehensible when separated from the system that created it; therefore, understanding it depends on the environment in which it is displayed. Moreover, electronically stored information lasts longer than paper documents and is more easily altered.[104] It also contains meta data that are usually not visible to the average user, including information about the document itself.[105] In addition, electronically stored information is unique in that it may become obsolete depending on the survival of the technology that created it in the first place.[106] Lastly, electronic information often reveals details about the techniques used to record, store, and code data.[107]

1. The Scope of Proposed Federal Rule of Civil Procedure 34(a)

Proposed Amended FRCP 34(a) defines electronically stored information expansively to avoid limitation to existing technologies.[108] Thus, electronically stored information, as

---

103. Thompson v. United States Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 97 (D. Md. 2003) (quoting Byers v. Ill. State Police, No. 99 C 8105, 2002 WL 1,264,004, at *10 (N.D. Ill. June 3, 2002).

104. OVERLY, *supra* note 2, at 3–4; *see* NINTH CIR. ADVISORY BD., *supra* note 10, at 1.

105. *See* NINTH CIR. ADVISORY BD., *supra* note 10, at 2; *see also* Hedges, *supra* note 33, at 4 (noting that meta data may be within the scope of discovery, though it is not routinely used for business purposes).

106. *See* NINTH CIR. ADVISORY BD., *supra* note 10, at 2.

107. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1007614, at *12 (S.D.N.Y. May 16, 2002) (likening such disclosures to trade secrets in the business context).

108. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 29 (proposed amendment to Rule 34(a)).

contemplated by the new rule, most certainly includes e-mail[109] as well as a broad range of other data and information.[110] To date, the consensus is that virtually all forms of electronically stored information, including instant messaging, web blogs, and cache files, are now—or should be—subject to FRCP 34(a) requests.[111] Other legal organizations, such as the American Bar Association, have proposed changes to their civil discovery guidelines that are in accordance with the Civil Rules Advisory Committee's expansive view of electronically stored information.[112] Finally, the proposed amendment's aim is to place the discovery of electronically stored information on "equal footing" with the discovery of documents.[113] As a result, commentators describe the discovery rules as "media neutral" in that they apply to documents regardless of the medium in which they exist, be it paper or electronic.[114] Although the two

109. *Id.* app. at 28 (proposed amendment to Rule 34(a)). Indeed, courts have already confirmed that e-mails are discoverable sources of evidence. *See, e.g.*, Collette v. St. Luke's Roosevelt Hosp., No. 99 CIV.4864(GEL), 2002 WL 31,159,103, at *8 (S.D.N.Y. Sept. 26, 2002); MHC Inv. Co. v. Racom Corp., 209 F.R.D. 431, 433 (S.D. Iowa 2002); Tulip Computers Int'l v. Dell Computer Corp., No. CIV.A. 00-981-RRM, 2002 WL 818,061, at *7 (D. Del. Apr. 30, 2002).

110. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 29 (proposed amendment to Rule 34(a)).

111. For a discussion of how courts have treated the discoverability of these types of electronically stored information, see *supra* Part II.B.4(a)–(f).

112. *See* AMERICAN BAR ASS'N, AMENDMENTS TO CIVIL DISCOVERY STANDARDS (2004) (recommending that the courts consider the following as discoverable data: e-mail, word processing documents, spreadsheets, presentation documents, graphics, animations, images, audio, video recordings, audiovisual recordings, and voicemail, in addition to platforms such as databases, networks, systems, servers, archives, backup systems, storage media, laptops, personal computers, Internet data, personal digital assistants, handheld wireless devices, mobile telephones, paging devices, and audio systems); *see also* NINTH CIR. ADVISORY BD., *supra* note 10 (stating electronic documents normally include information intentionally entered and saved by a computer user); federal case law cited, *supra* note 4 (setting forth how courts have interpreted documents to include various types of electronic information); Hedges, *supra* note 33 (listing computer data that may be within scope of discovery); Scheindlin & Rabkin, *supra* note 10 (excluding information stored without a user's knowledge).

113. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 28 (proposed amendment to Rule 34(a)).

114. Hedges, *supra* note 33, at 29 (citing THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 8 (Jonathon M.

categories of discoverable information differ, the amended rules look beyond these differences in order to promote the free-flow exchange of information necessary to resolve disputes.[115]

Despite the broad definition afforded to electronically stored information, some ambiguities persist. For instance, it is not immediately clear from the text of the amended version whether electronically stored information will be confined to information created intentionally, or whether other data collections, such as dynamic databases that constantly change in response to user queries, are discoverable.[116] Moreover, judicial rulings on the discoverability of electronic databases will add clarity to the scope of Proposed Amended FRCP 34(a). To date, at least one district court has made clear that FRCP 34 requests for databases concern only those compilations already in existence.[117] Another court emphasized that the manipulability of a database does not entitle a requesting party to have access to its electronic form.[118]

Redgrave et al. eds., 2004).

115. The proposed Amended Rule's broad reach is also in accordance with "the American civil process which 'puts a premium on disclosure of facts to ascertain the truth as the means of resolving disputes.'" Super Film of Am., Inc. v. UCB Films, Inc., 219 F.R.D. 649, 654 (D. Kan. 2004) (quoting Uniden Am. Corp. v. Ericsson Inc., 181 F.R.D. 302, 306 (M.D.N.C. 1998)).

116. *See, e.g.*, MYLES LYNK & RICK MARCUS, DISCOVERY SUBCOMMITTEE REPORT ON ELECTRONIC DISCOVERY 10–11 (2003), *at* http://www.kenwithers.com/rulemaking/report041403.pdf.

117. *See* Paramount Pictures Corp. v. Replay TV, CV 01-9358, 2002 WL 32,151,632, at *2 (C.D. Cal. May 30, 2002) ("A party cannot be compelled to create, or cause to be created, new documents solely for their production. Federal Rule of Civil Procedure Rule 34 requires only that a party produce documents that are already in existence." (citing Alexander v. FBI, 194 F.R.D. 305, 310 (D.D.C. 2000)). Notably, however, the Northern District of Illinois ordered a plaintiff to hand over to defendant a database created during discovery based on materials provided by the defendant. *See* Portis v. City of Chicago, No. 02 C 3139, 2004 WL 1,535,854, at *5 (N.D. Ill. July 7, 2004) (requiring the parties to share the expenses incurred by plaintiff in creating the database).

118. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1,007,614 (S.D.N.Y. May 16, 2002). In *Jones*, inmate plaintiffs sought electronic databases containing information on prison incident reports, medical problems, disciplinary records, and other data. *Id.* at *3. The plaintiffs wanted to analyze the data to show a causal link between the practice of double-celling and increased incidence of disease and violence among inmates, which could not be established through individual testimony. *See id.* Nevertheless, the court denied the request because the plaintiffs not only failed to show that the

a. The surviving meaning of "data or data compilations in any medium"

The proposed wording of FRCP 34(a) has been described as "problematic,"[119] and indeed has left the rule open to some degree of interpretation. If approved, the amended rule will declare:

> Any party may serve . . . a request (1) to produce and permit the party making the request . . . to inspect, copy, test, or sample *any designated electronically stored information or any designated documents* (including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations in any medium from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect, copy, test, or sample any designated tangible things. . . .[120]

One reading of the proposed rule would treat electronically stored information and documents as distinct categories, with the parenthetical referring to documents only.[121] However, this interpretation would mean that "documents" still includes "images," "sound recordings," and "data or data compilations in any

---

statistical analyses were feasible and likely to produce results, but the request would have required affirmative action on the part of the producing party to instruct the plaintiffs on how the data were organized and encoded. *Id.* at *7. Both *Jones* and *Paramount Pictures* signal a departure from past judicial responses that were more favorable to requests that required a responding party to compile electronic data. *See, e.g.*, Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 CIV. 2120, 1995 U.S. WL 649,934, at *3 (S.D.N.Y. Nov. 3, 1995) (requiring responding party to compile electronic data depending on plaintiff's need for the information and the cost to the defendant); Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1258–59 (E.D. Pa. 1980) (requiring plaintiff to re-run a program that assembled and printed sales data onto computer-readable media after defendants offered to pay related costs); *see also* Lisa M. Arent et al., *E-Discovery: Preserving, Requesting & Producing Electronic Information*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 131, 156–57 (2002) (discussing *Anti-Monopoly* and *National Union*).

119. Gregory P. Joseph, *Proposed Electronic Discovery Rules* 1, 8 (2004), *at* http://www.uscourts.gov/rules/e-discovery/04-CV-066.pdf.

120. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 24–25 (proposed amendment to Rule 34(a)) (emphasis added).

121. *See* Joseph, *supra* note 119, at 8.

medium"—all of which clearly include electronic information.[122] This reading of the amended rule blurs the distinction between documents and electronically stored information.[123] On the other hand, if the parenthetical includes both "electronically stored information" and "documents," then the goal of creating an explicit distinction between the two categories appears unmet.

The Advisory Committee's notes to proposed FRCP 34(a) muddy the attempt at clarification, and seem to suggest that the Committee intended the all-inclusive interpretation described above. The Committee notes that the phrase, "data or data compilations in any medium" was added to FRCP 34(a) in 1970 to authorize discovery of data compilations in anticipation of the growing use of computerized information.[124] It further states that the phrase includes "any databases currently in use or developed in the future."[125] Given that electronically stored information has already been described as "any type of information that can be stored electronically,"[126] it is clear that both "data" and the "databases" included therein constitute electronically stored information.

Lastly, the Committee notes that "documents" does not adequately conceptualize electronically stored information, and therefore the new category avoids the "need to stretch [the] word [document] to encompass such discovery." Yet, the Committee goes on to state that, "document" production requests "should be understood to include electronically stored information unless discovery in the action has clearly distinguished between [that] information and 'documents.'"[127] Thus, if "document" requests

122. *Id.*

123. *See id.*

124. FED. R. CIV. P. 34(a) advisory committee's notes (1970). Indeed, the Notes to the 1970 Amendment to Rule 34 explained that, "[i]n many instances . . . [the] respondent will have to supply a print-out of computer data," implying that a hard copy was sufficiently equivalent to an electronic one so as to satisfy the requirements of production. *Id.*

125. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 28 (proposed amendment to Rule 34(a)).

126. *Id.*

127. *Id.* For judicial action in this area, see Mosaid Techs. Inc. v. Samsung Elecs. Co., No. CIV. A. 01-CV-4340, 2004 WL 2,550,306 (D.N.J. July 7, 2004). There, the plaintiff moved for discovery sanctions after defendant refused to produce e-mails. *Id.* at *1. Defendants claimed that plaintiff did not specify "e-mail" in its definition of "document" during discovery. *Id.* at *2.

continue to be all-inclusive, then the Committee seems to obliterate the need for a distinction in terminology.

b. Implications for distinguishing between documents and electronically stored information

The guidance (or misguidance) of the Advisory Committee raises the question of whether responding parties should review and produce electronically stored information, even if the propounding party does not specifically request it. The Committee Notes answer this inquiry affirmatively,[128] but not all courts have required parties to produce electronically stored information where it has not been directly requested.[129] Courts in the Southern and Eastern Districts of New York have interpreted their Local Rule 26.3(c)(2) to include electronically stored information in the definition of "document", which seems to be in accordance with the Advisory Committee's suggested interpretation of the term, despite the ambiguous wording of the proposed amendment.[130]

In federal courts outside of New York, the issue appears to focus not so much on whether certain types of electronically stored information fall within the gambit of "document," but more on parties' obligation to disclose the existence of electronically stored information to propounding parties and the specificity of requests in terms of production form.[131] To offer a glimpse of what is occurring at the state level, a Texas court in *In re Lowe's Companies, Inc.*[132] stated in dicta that, "a party cannot be compelled to produce . . . that

However, in part because defendant had requested e-mails from the plaintiff, the court found that defendant "knew, or should have known, those e-mails were discoverable" because of their own reliance on e-mails and due to the obvious realities of modern litigation. *Id.* at *3.

128. *See* REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 28 (proposed amendment to Rule 34(a)).

129. *See infra* Part II.D.

130. Joseph, *supra* note 119, at 9; *see also* S.D.N.Y. & E.D.N.Y. LOCAL CT. R. 26.3(c)(2) (2004) ("Document. The term 'document' is defined to be synonymous in meaning and equal in scope to the usage of this term in Federal Rule of Civil Procedure 34(a), including, without limitation, electronic or computerized data compilations.").

131. For further discussion of the circumstances under which federal courts have required the disclosure and/or production of information in electronic format, see *infra* Part II.D.1.

132. 134 S.W.3d 876 (Tex. App. 2004).

which it has not been requested to produce."[133] Furthermore, the court applied Texas Rule of Civil Procedure 196.4 to conclude that, "to obtain discovery of information that exists in electronic form, the requesting party must specifically request production of electronic data and specify the form in which it is to be produced."[134]

c. A suggested modification to proposed Federal Rule of Civil Procedure 34(a)

Criticisms of Proposed Amended FRCP 34(a) aside, it might be beneficial to consider an alternative framework for expressly incorporating modern manifestations of electronically stored information into the Federal Rules of Civil Procedure. The proposed approach creates a separate category to accommodate the significant differences between electronic and paper discovery. However, the mere addition of a new type of material to FRCP 34(a) perpetuates reliance on a categorical framework designed in 1970, before technology had fully transformed electronically stored information into today's predominant form of information storage and communication. In some respects, the challenges posed by attempting to squeeze electronically stored information into the current framework of FRCP 34 are analogous to the difficulty faced when attempting to fit a square peg into a round hole. Building off of the concept that the federal discovery rules are media neutral, it would seem more appropriate to streamline rather than expand the categories of information that parties may request under FRCP 34(a). Reformulating FRCP 34(a) to encompass an all-inclusive category of designated *information* would appear to better achieve the purpose of capturing both paper and electronically-stored material, with FRCP 34(b) guiding the form in which parties must produce such information.[135] In conclusion, if the Advisory Committee is going to

133. *Id.* at 880 n.7.

134. *Id.* The propounding party merely made a request for documents relating to injury claims against the defendant; therefore, the responding party did not need to produce any electronic data, including the database at issue. *See id.* at 879.

135. Of course, parties would still be encouraged to identify potentially relevant information in their opponent's possession through interrogatories and depositions and to specify the particular types of electronically stored information they wished to see produced in their FED. R. CIV. P. 34(a) requests. *See, e.g.*, Arent et al., *supra* note 118, at 169 (noting the utility of

amend FRCP 34(a), the most pragmatic way to do so is to group the various types of information conceptualized in the terms "document" and "electronically stored information" under one, all-inclusive umbrella.[136]

2. Obligation to Produce for Inspection, Copying, Testing and Sampling

Another proposed change to FRCP 34(a) concerns requests for testing and sampling of electronically stored information. The current FRCP 34(a) states, "[a]ny party may serve on any other party a request . . . to inspect and copy[] any designated documents . . . [and] to inspect and copy, test, or sample any tangible things which

---

interrogatories in obtaining preliminary information regarding a party's computer system, "including hardware, software, software applications, back-ups, e-mail and voicemail administration, and similar issues."). Hon. Scheindlin and Jeffrey Rabkin proposed a similar change to Federal Rule of Civil Procedure 34 that would re-phrase the Rule as follows: "Any party may serve on any other party a request . . . to . . . copy any designated documents *or any designated data* (including writings, drawings, graphs, charts, photographs, phonorecords, and *electronically-stored information*)." Scheindlin & Rabkin, *supra* note 10, at 372–73 (emphasis in original). The proposal would thus "eliminate the need to define 'documents' to include 'data compilations'," but would maintain a distinction between "data" and "documents" in order to create an opportunity to develop separate bodies of case law regarding the two categories. *Id.* at 373. While this approach carries the advantage of giving judiciaries flexibility in dealing with issues such as privilege, proprietary interests, duty to preserve, and possession, as they relate to electronic evidence specifically, it still places a burden on propounding parties to make the obscure distinction between a traditional "document" and writings or recordings contained in "data."

136. The UK-based Litigation Support Technology Group ("LiST") has similarly proposed a new definition for "document" ("anything in which information of any description is recorded") and an eventual move to the use of the term "item" instead of document:

> It is the drafters' ultimate intention to move away from "document" as the accepted term . . . and introduce the term "item", the definition of which will include "document" . . . as well as "database record", "email folder", "CD-ROM", "videotape", etc. It is felt that this term better encapsulates the different type, size and class of anything in or on which information can now be recorded.

Litigation Support Technology Group (LiST), *Practice Direction—The Use of Technology in Civil Proceedings* 2, 2 n.5 (Society for Computers and Law (UK) May 28, 2004), *at* http://www.kenwithers.com/rulemaking/pd052804.pdf.

constitute or contain matters within the scope of Rule 26(b). . . ."[137] Whereas the current rule does not clearly authorize the opportunity to test or sample documents, the proposed FRCP 34(a) makes explicit the opportunity for a requesting party "to test or sample materials . . . in addition to inspecting or copying them."[138]

Inspection requests vary somewhat in electronic discovery from paper discovery because they tend to be more time-sensitive and often require an intrusion into an opponent's operations. For example, a request to inspect computers or storage media may require the responding party to refrain from using that computer system, or other tangible items, until the inspection has occurred, thus disrupting routine operations.[139] Consequently, courts will most likely deny unfettered requests for direct access to inspect and copy electronically stored information.[140] Rather, courts will typically

---

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

138. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 29 (committee note on proposed amendment to Rule 34(a)). The proposed language reads, "Any party may serve on any other party a request . . . to inspect, copy, test, or sample any designated electronically stored information or any designated documents. . . ." *Id.* app. at 24.

139. *See, e.g.*, R.S. Creative, Inc. v. Creative Cotton, Ltd., 89 Cal. Rptr. 2d 353, 356 (1999) (imposing sanctions on plaintiff for deleting files despite a stipulation that "computers and diskettes would not be operated or touched . . . until defendants' computer expert could examine them").

140. As the court in *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003), noted:

> The Advisory Committee Notes to Rule 34(a) support this interpretation. Commenting on data compilations, the Committee stated, "[W]hen the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data." FED. R. CIV. P. 34(a) advisory committee's note (1970 amend.). Like the other discovery rules, Rule 34(a) allows the responding party to search his records to produce the required, relevant data. Rule 34(a) does not give the requesting party the right to conduct the actual search. While at times—perhaps due to improper conduct on the part of the responding party—the requesting party itself may need to check the data compilation, the district court must "protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs."

Id.; *see also* Med. Billing Consultants, Inc. v. Intelligent Med. Objects, Inc., No. 01 C 9148, 2003 WL 1,809,465, at *2 (N.D. Ill. Apr. 4, 2003) (denying a motion to compel an expert's inspection of opponent's computer equipment

limit requests to the inspection and copying of a product that is the result of a respondent's "translation of the data into a reasonably usable form."[141] Moreover, copying requests will most likely be limited by a standard of reasonableness and a balancing of the privacy interests of the opponent party and the need for the information.[142]

3. The Impact of Requests for Electronically Stored Information on the Requirement of Control

FRCP 34(a) also limits discovery requests to documents or tangible things "which are in the possession, custody or control of the party upon whom the request is served."[143] This portion of FRCP 34(a) has been interpreted to mean that a party may be considered in control of documents or electronically stored information even if not in possession of the information, so long as the producing party has retained "any right or ability to influence the person in whose possession the documents lie."[144] Thus, if two parties are conducting

---

because the requesting party failed to show that additional relevant information would be found on the equipment); Bethea v. Comcast, 218 F.R.D. 328, 330 (D.D.C. 2003) ("As indicated by this court and other courts, a party's suspicion that another party has failed to respond to document requests fully and completely does not justify compelled inspection of its computer systems.").

141. *Ford Motor Co.*, 345 F.3d at 1316–17 (finding that the district court abused its discretion in allowing the plaintiff "unlimited, direct access" to defendant's databases, but indicating that "some kind of direct access might be permissible in certain cases"). In *First USA Bank v. PayPal, Inc.*, 76 Fed. Appx. 935, 936 (Fed. Cir. 2003), the court ordered direct inspection of a former chief executive officer's laptop under an approved search protocol that permitted electronic discovery consultants "to create a forensic copy of the computer's hard drive and identify any potentially relevant documents . . . if such documents were found and identified, . . . [the former CEO] would [be allowed] . . . to create a privilege log."

142. *See, e.g.*, Dikeman v. Stearns, 560 S.E.2d 115, 117 (Ga. Ct. App. 2002) (denying defendant's request for a complete copy of a hard drive that contained documents relating to plaintiff because the request was "overbroad, oppressive, and annoying").

143. FED. R. CIV. P. 34(a). The requesting party also has the burden of demonstrating that the opposing party has the requisite control. *See also* Super Film of Am., Inc. v. UCB Films, Inc., 219 F.R.D. 649, 653 (D. Kan. 2004) (stating that before the plaintiff has "to produce documents, . . . the court must determine [whether the plaintiff] has the right, authority, or ability to obtain the requested documents").

144. *See Super Film of Am., Inc.*, 219 F.R.D. at 651 (citing Lone Star Steakhouse & Saloon, Inc. v. Liberty Mut. Ins. Group, No. 02-1185-WEB,

business in a manner in which there is significant overlap in operations or an inherent relationship between the two parties, this may justify a finding of control under FRCP 34(a).[145] In the arena of electronically stored information, e-mails and other documents in the possession of business partners intimately connected to transactions with a litigant are likely to be considered discoverable.[146]

The requirement of control (or "possession" or "custody") is difficult to apply to some types of electronically stored information since only specialized computer programs are capable of identifying and locating it.[147] Moreover, although a party is not obligated to produce documents not in its control, if the documents sought are "known to have been in the party's possession, custody, or control" at some time in the past, the party must nevertheless explain their disposition.[148]

D. Forms of Production: Proposed Amendments to Federal Rule of Civil Procedure 34(b)

The form in which a party produces documents is more critical in electronic discovery than in paper discovery, due to the various forms in which electronically stored information may exist and the varying amounts of information which may be obtained from the electronic document depending on its form. Judicial management of electronic discovery disputes has made clear the need for guidelines concerning specificity of production requests and a default form of production in the absence of specific requests.[149]

2003 WL 21,659,662, at *2 (D. Kan. June 4, 2003)).

145. *Id.* at 654 (noting "[c]ontrol may be established where the corporations in question share a common ownership or management structure").

146. *See, e.g., id.* at 655–56.

147. Scheindlin & Rabkin, *supra* note 10, at 380.

148. *Super Film of Am., Inc.*, 219 F.R.D. at 651. Scheindlin & Rabkin propose defining the terms, "possession, custody or control" to exclude information intentionally discarded prior to anticipation of litigation. Scheindlin & Rabkin, *supra* note 10, at 381. Merging this suggestion with the approach of the *Super Film* court would result in requiring parties to at least disclose that the documents were at some time in their "possession, custody or control" and to provide an explanation as to where that information is now, if known.

149. *See, e.g.*, N. Crossarm Co. v. Chem. Specialties, Inc., No. 03-C-415-C, 2004 WL 635,606, at *1 (W.D. Wis. Mar. 3, 2004) (stating that "neither the letter nor the spirit of Rule 34 mandates that a party is *entitled* to production in its preferred format" in denying plaintiff's motion to compel production of e-

Electronically stored information may be produced in forms ranging from conventional paper or hard copy format to electronic formats such as document images and documents in native format.[150] As such, parties need to be aware of the possible forms in which relevant information may be requested, as well as the various media on which digital documents may be provided (including CD-ROM, disk, and other electronic devices). Commentators have suggested that requests for electronically stored information in native file format should also inquire into the programs used to generate the relevant information, the programs' developers, any modifications of the programs, and the location of the programs.[151] Finally, the forms in which electronically stored information may be produced are significant, not only due to their variety, but also due to the varying degree of manipulation that is possible depending on the form of production employed.

Currently, a FRCP 34(a) request for the production of "documents" entitles the propounding party to *disclosure* of electronically stored information, but not necessarily to *production* of that information in electronic format.[152] Many courts have held

---

mail in electronic format after defendant already provided 65,000 pages of e-mail in hardcopy).

150. *See supra* Part II.B.1(b), for a description of native file review and production and a comparison to document images.

151. OVERLY, *supra* note 2, at 24. Obtaining this information prior to production may be crucial in determining whether a party should seek production in electronic format. An important consideration for the requesting party may be whether it has the resources to interpret the opponents' data if produced in electronic form. A Third Circuit district court recently ordered production in electronic format, but stopped short of requiring the responding party to provide technical assistance to the propounding party in understanding the data produced. *See In re* Plastics Additives Antitrust Litig., No. 03-2038, 2004 U.S. Dist. LEXIS 23989, at *48–49 (E.D. Pa. Nov. 29, 2004) ("[D]efendants shall not be required to make available 'documentation and computer personnel' to help plaintiffs understand that data.... Although the parties may privately agree to provide technical assistance to one another, this Court will not impose such an obligation on either party as a matter of course.").

152. *See, e.g.*, *N. Crossarm Co.*, 2004 WL 635,606, at *1; *see also* Zhou v. Pittsburgh St. Univ., No. 01-2493-KHV, 2003 WL 1,905,988, at *2 (D. Kan. Feb. 5, 2003). In *Zhou*, the court ordered a party to "disclose all data compilations, computerized data and other electronically-recorded information . . . that reflect the salaries of faculty working within [d]efendant's music department from Fall semester 1997 through Spring semester 2000"

that hard copies are a sufficient form of production unless the requesting party *specifies* otherwise before the opposing party produces any information.[153] The proposed rule encourages the requesting party to specify the form in which electronically stored information should be produced.[154] If no such request is made, or if the parties do not agree and the judge does not order a particular form, then the responding party may produce either in the form in which the information is ordinarily maintained or in an electronically searchable form.[155]

1. The "As Ordinarily Maintained" Form of Production

The proposed amendment to FRCP 34(b) is analogous to the current rule, in that the responding party must produce electronically stored information "in a form in which it is ordinarily maintained."[156] Even without the amended rule, some jurisdictions have adopted a similar approach for electronically stored information and require that it be produced in a manner that would be expected in the regular course of business.

---

after defendant produced handwritten salary recommendations to plaintiff. *Id.* The court interpreted Federal Rule of Civil Procedure 34 to mean that a responding 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." *Id.*

153. There may be a trend away from hard copy production of electronic documents, however. *See, e.g.*, NINTH CIR. ADVISORY BD., *supra* note 10, at 5 (proposed local rule 3) (stating that "[e]lectronic documents *shall* be produced in electronic form (including meta data)" (emphasis added)); *In re* Plastics Additives Antitrust Litig., 2004 U.S. Dist. LEXIS 23989, at *48 (agreeing with defendants that both parties, not just defendants, should be required to produce transactional data in electronic format "to the extent reasonably feasible"). *But see N. Crossarm Co., Inc.*, 2004 WL 635606, at *1 ("[I]f a party produces its electronic information in a hard copy format that mimics the manner in which that information is stored electronically, then that party has not disobeyed Rule 34.").

154. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 26 (proposed amendment to Rule 34(b)).

155. *Id.* app. at 27 (proposed amendment to Rule 34(b)). Judicial orders thus far have included ordering the production of requested data "in a readily understandable electronic format," accompanied by any necessary technical assistance. Paramount Pictures Corp. v. Replay TV, No. CV 01-9358 FMC (Ex), 2002 WL 32151632, at *2 (C.D. Cal. May 30, 2002).

156. REPORT OF CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 27 (proposed amendments to Rule 34(b)).

A telling example of this approach occurred in *In re Honeywell International, Inc. Securities Litigation.*[157] In that case, Honeywell's financial auditor produced hard-copies of over one thousand documents, but plaintiffs sought electronic versions since that was the form in which the documents were maintained in the ordinary course of business.[158] Specifically, plaintiffs contended that they could not discern which attachments matched the workpapers produced in hard copy since this was not the form in which the workpapers were kept in the course of business.[159] Ultimately, the court ordered production in electronic form because the auditor did not provide plaintiffs "with an adequate means to decipher how the documents are kept in the usual course of business."[160]

Whether production of electronically stored information in commonly accepted image formats, such as PDF (portable document format) or TIFF,[161] meets the "as ordinarily maintained" requirement is debatable. Although a document image perfectly replicates its hard copy counterpart, document reviewers of such images lose the advantage of circumstantial observations, such as where a party stored information in relation to other documents and files.[162]

2. The "Electronically Searchable" Form of Production

If a party elects not to produce electronically stored information in the form in which it is ordinarily maintained, the information must be produced in an electronically searchable format.[163] The producing

157. No. M8-85 WHP, 2003 WL 22,722,961 (S.D.N.Y. Nov. 18, 2003).

158. *Id.* at *1.

159. *Id.* Tangentially, meta data likely would have played an important role in allowing plaintiffs to recognize which attachments corresponded to workpapers had those workpapers been produced electronically. *See supra* Part II.B.1, on meta data.

160. *In re Honeywell Int'l Inc.*, 2003 WL 22,722,961, at *2.

161. TIFF stands for "Tagged Image File Format" and is a graphics file format created in the 1980's to be the standard image format across multiple computer platforms. *See* Definition of TIFF, *at* http://www.sharpened.net/glossary/definition.php?tiff (last visited Jan. 20, 2005). Improvements have been made to the original TIFF format, and there are now around 50 variations of it. *Id.*

162. A review of document images, for example, would not reveal whether a "smoking gun" memorandum was tucked conspicuously behind unrelated files in a drawer or whether the document was filed amidst numerous other relevant documents.

163. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at

party may prefer this latter choice if the volume of documents requested is significant.[164] Through the use of meta data, most batches of electronic documents can be converted into a searchable format, including databases sorted by file type.[165]

Searchable formats may vary in type. Text-searchable materials, for instance, may prove most useful to propounding parties and are already acceptable under FRCP 34(b).[166] However, not all discoverable electronically stored information is text-searchable. Non-textual material, including compressed or encrypted files, graphics files, and digitized audio files, cannot be easily searched and typically require one-by-one review for relevance.[167]

The proposed rule's allowance for production of documents in electronically searchable format raises the question of whether such production may substitute for other efforts by the producing party, such as the creation of an index.[168] This may depend on whether "electronically searchable" refers to native format only or also includes document images. As discussed in Part B.1, the existence of meta data in native format files allows for searching and indexing capabilities, among others. On the other hand, document images are searchable, to a limited degree, through application software known as optical character recognition ("OCR").[169] How searchable the

---

27 (committee note on proposed amendment to Rule 34(b)(ii)).

164. *See, e.g.*, Zakre v. Norddeutsche Landesbank Girozentrale, No. 03 Civ. 0257(RWS), 2004 WL 764,895, at *1 (S.D.N.Y. Apr. 9, 2004) (holding that "[i]n light of the Sedona Principles and *In re Lorazepam*, and in particular of the Federal Rules of Civil Procedure, [defendant] is not obligated to provide more than a searchable CD-ROM," where defendant had already produced over 200,000 e-mails in a text-searchable format to plaintiffs).

165. *See supra* Part II.B.1, for a more thorough discussion of how meta data functions to enable the searching and organizing of large amounts of electronically stored information.

166. *See Zakre*, 2004 WL 764,895, at *1.

167. *See* OVERLY, *supra* note 2, at 46.

168. For example, in *Zakre*, the court held that the defendant did not need to produce a document index because the plaintiffs could "'search the documents on their own.'" 2004 WL 764,895, at *1 (quoting *In re* Lorazepam & Clorazepate Antitrust Litig., 300 F. Supp. 2d 43, 47 (D.D.C. 2004)).

169. *See What Do You Need to Know About OCR?*, SCAN SOFT, [hereinafter *What Do You Need to Know About OCR?*] *at* http://support.caere.com/ocr/ (last visited Nov. 19, 2004). OCR programs read the text contained in an image and convert it to ACSII (American Standard Code for Information Interchange), a set of codes used to represent letters, numbers, a few symbols, and control characters. "ASCII," COLUMBIA ENCYCLOPEDIA (6th ed. 2003),

electronically stored information needs to be to meet this FRCP 34(b) production form requirement remains to be explored.

3. The "One Form" Requirement

The proposed FRCP 34(b) will require parties to produce electronically stored information in only one form, unless there is good cause to order production in an additional form.[170] In the past, district courts have been split with respect to requiring the electronic production of information if the information has previously been submitted in hard copy. More recently, however, courts have taken the "one form" approach.[171] This approach appears to be in accordance with current discovery rules, which place the burden of

---

http://education.yahoo.com/reference/encyclopedia/entry?id=2979. With ASCII, a seven-digit (or seven-bit) binary number can represent one of 128 distinct codes. *Id.* Once the conversion takes place, users may save the conversion as a word processing file, which is subject to manipulation and searching. *See What Do You Need to Know About OCR?*, *supra*. Nevertheless, searching capability is sometimes limited by the accuracy of the conversion, and functionality is limited to searching because meta data is still not available to provide information about the file's creation, or identity and timing of authorship. *Id.*; *see* O'Reilly & Derting, *supra* note 17 (noting that printable end product does not include embedded data). OCR software captures 85% or less of the searchable text in a document, compared to 100% accuracy with the original source file. O'Reilly & Derting, *supra* note 16, at 5. The difference between creating a litigation document database from OCR-searchable document images and field databases derived from native files is that field databases offer full Boolean search capability. *Id.* Boolean searches interpret all characters as combinations of "ones" and "zeros" and eliminate any chance for error. *See, e.g.*, Webopedia, *Boolean Logic*, *at* http://www.webopedia.com/TERM/B/Boolean_logic.html (last modified Aug. 5, 2004); *see also* Scheindlin & Rabkin, *supra* note 10, at 333–35 (explaining how computers transform and store information in binary form).

170. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 31 (proposed amendment to Rule 34(b)) ("One such ground might be that the party seeking production cannot use the information in the form in which it was produced.").

171. *Compare* Williams v. Owens-Illinois, Inc., 665 F.2d 918, 932–33 (9th Cir. 1982) (holding that the district court did not abuse its discretion in denying a request for computer tapes where the requesting party already had all information from tapes on wage cards), *with* Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV.2120, 1995 WL 649,934, at *2 (S.D.N.Y. Nov. 3, 1995) ("[P]roduction of information in 'hard copy' documentary form does not preclude a party from receiving that same information in computerized/electronic form.").

specifying the form of production on the requesting party.[172] It also reinforces an underlying principle of civil procedure that the Federal Rules should be applied in the manner most likely to "secure the just, speedy, and inexpensive determination of every action."[173] Nevertheless, those courts that have not adopted the strict one form approach will still only require additional production if the propounding party can establish that the original form of production was insufficient.[174]

In *Marcin Engineering, LLC v. Founders at Grizzly Ranch, LLC*, the court applied the one form approach under the current Federal Rules of Civil Procedure.[175] In that case, the district court of Colorado refrained from ordering the electronic production of plaintiff's work, which had previously been produced in hard copies.[176] Defendant claimed that plaintiff "intentionally withheld" computer data that was relevant and material to defendant's claims, even though the "withheld" data had previously been produced in hard copies.[177] Because defendant waited five months after the discovery cut-off date to assert this deficiency, the court did not order electronic production.[178] Thus, whether a party is dilatory in asserting defects with the form of production might be one factor a court considers in deciding if good cause exists to order production in an additional form.

Whether there is good cause to order an additional form of production may also hinge on the degree to which an original

---

172. *See* FED. R. CIV. P. 34(b).

173. *Id.* 1.

174. *E.g.*, McNally Tunneling Corp. v. City of Evanston, No. 00C6979, 2001 U.S. Dist. LEXIS 20394, at *14–15 (N.D. Ill. Dec. 10, 2001) (finding that the defendant's statement, "'the electronic version of [plaintiff's] schedules will better allow the [defendant] . . . to understand the reasons for the delays encountered by [plaintiff] on this project,'" did not adequately explain why the already-produced hard copies were insufficient).

175. 219 F.R.D. 516 (D. Colo. 2003).

176. *Id.* at 523.

177. *Id.* at 521. Moreover, although Grizzly Ranch used the definition of "document" contained in Federal Rule of Civil Procedure 34, which includes "computer data or other data compilation from which information can be obtained or translated," the actual discovery request only asked the plaintiff to produce its "files," a term that was undefined and did not necessarily include "computerized versions of preliminary and superseded work product." *Id.* at 523.

178. *See id.* at 523–24.

production failed to satisfy the requesting party's discovery needs. Several courts have made it clear that mere speculation is insufficient to justify electronic production when hard copies have already been produced.[179] In *Stallings-Daniel*, for example, an employment discrimination plaintiff suspected that her employer had altered certain e-mails before producing them.[180] Yet, the plaintiff presented nothing more than scant circumstantial evidence to support her theory, and the court was unwilling to order an electronic investigation based on mere speculations.[181] Even if more evidence exists to substantiate the need for production in electronic form, this

> [D]oes not mean that any information that would be discoverable in paper form must automatically be discoverable, on the same terms and conditions, and without consideration of additional issues, in electronic form. . . . Particularly when it comes to balancing the costs and benefits of providing discovery, the balance may well differ depending on the form of the information.[182]

Case law does suggest that where the electronic version of data in question proves to be both relevant and easier to manipulate, production in electronic form, in addition to paper form, may be ordered.[183] It also suggests that the one form standard would not preclude parties from agreeing to alter the form of production mid-way through discovery.[184]

---

179. *See, e.g.*, Stallings-Daniel v. N. Trust Co., No. 01 C 2290, 2002 WL 385,566 (N.D. Ill. Mar. 12, 2002).

180. *Id.*

181. *Id.* The plaintiff tried to show that in a previous discrimination suit her employer had possibly committed discovery abuse and therefore there may have been abuse in the case of her discovery request. *Id.* However, the court noted that the prior case was before a different judge, who did not necessarily conclude there was any abuse, and the documents at the focus of plaintiff's concern were not produced by the same individual as in the prior case. *Id.*

182. Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1,007,614, at *6–7 (S.D.N.Y. May 16, 2002) (noting that electronic production of the database at issue would not only require significant effort in the way of instructing the requesting parties as to how to use the database, but it would disclose confidential information about the way in which the defendant maintained, stored, and classified information).

183. *See id.* at *13 (noting that even where the burden of the proposed discovery is substantial, it does not forbid disclosure if the benefits outweigh those costs).

184. *See In re* Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437 (D.N.J.

E. The Use of Depositions and Interrogatories in the Discovery of Electronically Stored Information

Depositions and interrogatories provide parties with valuable opportunities to learn about the structure, form, and content of their opponents' electronically stored information. As such, a party should preferably use these discovery tools before it drafts an electronic discovery request to apprise itself of potentially discoverable and relevant information.

FRCP 30 governs depositions and can prove to be a useful tool for litigants engaging in electronic discovery. Depositions of information technology (IT) personnel serve as an ideal starting point in the discovery process.[185] Moreover, FRCP 30(b)(6) allows a party to capture more than one person with a deposition request, which can be useful in the context of electronic discovery if a party is unsure of who may be in possession of relevant electronically stored information.[186] Courts have upheld parties' requests for electronically stored information in depositions, including

---

2002). In *In re Bristol-Myers Squibb Securities Litigation*, the plaintiffs agreed at the commencement of litigation to pay $0.10 per page for defendant's photocopying costs. *Id.* at 439. Later, plaintiffs not only discovered that the defendants were producing many more documents than originally anticipated, but also discovered that the defendants had been electronically scanning the documents for their purposes and "blowing back" those same documents in hard copy for plaintiffs. *Id.* Although defendants were willing to give the plaintiffs the remaining documents in electronic format, they sought one-half of the scanning costs. *Id.* at 440. The court did not order plaintiffs to pay for their share of the scanning costs, but only for the nominal cost of the discs on which the information was duplicated, since plaintiffs originally agreed only to cover the cost of paper discovery. *Id.* at 444.

185. *See, e.g.*, Seward & Austin, *supra* note 73, at 52 (noting that depositions may be useful in finding out the types of computer systems, equipment, and software an opponent uses, as well as the location of data and back-up and deletion practices).

186. *See* FED. R. CIV. P. 30(b)(6). Rule 30(b)(6) states:

> A party may in the party's notice and in a subpoena name as the deponent a public or private corporation or a partnership or association or governmental agency and describe with reasonable particularity the matters on which examination is requested. In that event, the organization so named shall designate *one or more officers, directors, or managing agents, or other persons* who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify.

Id. (emphasis added).

information regarding unique software programs.[187]

Interrogatories provide parties with the opportunity to probe their opponents for information raised in a deposition or that otherwise appears relevant to a claim or defense.[188] Currently, FRCP 33(d) permits a responding party to answer an interrogatory by specifying the business records "from which the answer may be derived" and to give the serving party a reasonable opportunity to "examine, audit or inspect such records."[189] The proposed amendment to FRCP 33(d) would include electronically stored information in the definition of business records.[190] Thus, an answer to an interrogatory involving a review of business records should also include a search of electronically stored information and permit the responding party to answer by providing access to that information.[191] The proposed changes to FRCP 33(d) would allow a responding party to substitute access to electronically stored information for an answer only if the burden of deriving the answer would be substantially the same for either party.[192] Courts are cognizant of interrogatories' utility in providing an opportunity for parties to learn about the sources of their opponents' electronically

187. *See, e.g.*, R.S. Creative, Inc. v. Creative Cotton, Ltd., 89 Cal. Rptr. 2d 353, 355–56 (Ct. App. 1999). In a breach of contract action, the deposing party defined "document" in the notice of deposition to include "computer tapes, discs and any information stored in a computer." *Id.*; *see also* York v. Hartford Underwriters Ins. Co., No. 01-CV-590-B(J), 2002 WL 31,465,306, at *3–4 (N.D. Okla. Nov. 4, 2002) (ordering defendant to designate a person to testify during deposition as to specified matters surrounding defendant's software program, but granting defendant's request for a protective order concerning certain proprietary information).

188. OVERLY, *supra* note 2, at 57.

189. FED. R. CIV. P. 33(d).

190. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, app. at 29 (proposed amendment to Rule 34(b)) ("A companion change is made to Rule 33(d), making it explicit that parties choosing to respond to an interrogatory by permitting access to responsive records may do so by providing access to electronically stored information.").

191. *Id.* at 14. Courts already appear to be permitting parties to substitute access to electronically stored information in response to interrogatories. *See, e.g.*, United States v. Rachel, 289 F. Supp. 2d 688, 693 (D. Md. 2003) (holding that a Rule 33(d) interrogatory request was adequately addressed, in part, by the production of numerous computer diskettes).

192. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, at 14. This is not so much a proposed change, as it is a formal application of the current rule to electronically stored information.

stored information and encourage their use.[193]

The proposed amendment to FRCP 33(d) reflects a departure from the committee's approach to amending FRCP 34(a). While the new FRCP 34(a) would carve out a separate category for electronically stored information,[194] the modified FRCP 33(d) would instead include this type of information in the definition of a record.[195]

F. Incorporation of Electronically Stored Information in Other Discovery and Evidentiary Matters

Uniform treatment of electronically stored information in discovery, evidentiary, and other litigation-relevant rules is an ideal objective in creating a cohesive approach to using and producing such information in litigation. To this end, it is useful to examine the application of other rules that deal with electronically stored information. For example, the United States Court of Federal Claims, defines the term "records" to include electronically stored information.[196] That same court ordered producing parties to provide electronic records in the format in which they are typically used so long as the producing party offered the opposing party directions on how to access and use the information.[197] Another example occurred in the application of the Freedom of Information Act to e-mails requested in the course of litigation.[198] In that case, a district court ordered defendants to disclose factual, non-deliberative information

193. *See* Jones v. Goord, No. 95 CIV. 8026(GEL), 2002 WL 1,007,614, at *16 (S.D.N.Y. May 16, 2002) ("Nothing prevented plaintiffs from seeking, either informally . . . or formally by interrogatory, further information about the computer databases available from [defendant].").

194. *See* REPORT OF THE CIVIL RULE ADVISORY COMM., *supra* note 3, at 15.

195. *See id.* at 14.

196. *See, e.g.*, Jicarilla Apache Nation v. United States, 60 Fed. Cl. 413, 414 (2004) (including in the definition of "record," for purposes of a Protective Order, the following types of information: computation, computer or network activity log, data, database, e-mail, file, image, machine readable material, meta data, printout, spreadsheet, voicemail, webpage, "regardless of physical or electronic format or characteristic").

197. *See id.* at 416 ("If the requesting party is unable to access or use or is denied direct access to an electronic record, it may request that the responding party provide a paper version of or underlying source data for the electronic record.").

198. *See* Judicial Watch, Inc. v. United States Dep't of Justice, 337 F. Supp. 2d 183 (D.D.C. 2004).

contained in e-mails that was not inextricably intertwined with otherwise protected information.[199] In doing so, the court was interpreting e-mail to fall within the definition of the term, "documents," used in the segregable information requirement of the Act.[200]

1. The Business Records and Public Records Exceptions to the Hearsay Rule

Given the Civil Rules Advisory Committee's proposed inclusion of electronically stored information in the definition of business records for purposes of interrogatories,[201] the business records and public records exceptions to the hearsay rule of evidence warrant a similar consideration. Federal Rule of Evidence (FRE) 803(6) provides for an exception to the admissibility of hearsay where a party seeks to introduce a "memorandum, report, record, or data compilation . . . if kept in the course of a regularly conducted business activity."[202] Legal scholars widely accept that "all modern forms of digital data collection"[203] are included within this exception, so long as the record maintains trustworthiness.[204] Unlike the proposed changes to FRCP 33 and 34, no comparable changes have been officially proposed by the Advisory Committee on Evidence Rules. However, some academic consideration of whether the rule should address the manipulation of electronic records has taken place.[205]

---

199. *Id.* at 187.

200. *See id.* at 185.

201. REPORT OF THE CIVIL RULES ADVISORY COMM., *supra* note 3, at 14.

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

203. DAVID P. LEONARD & VICTOR J. GOLD, EVIDENCE: A STRUCTURED APPROACH 224 (2004); *see also* Hardison v. Balboa Ins. Co., 4 Fed. Appx. 663, 669–70 (10th Cir. 2001) (finding no abuse of discretion where the district court held computer-generated printouts to be admissible under the business records exception to the hearsay rule. The appellate court noted that the foundation does not need to be laid by the record's author, but rather can be established by "anyone who demonstrates sufficient knowledge of the record keeping system that produced the document.").

204. LEONARD & GOLD, *supra* note 203, at 226.

205. *See, e.g.*, Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J.L. & TECH. 161 (2000); Daniel R. Murray & Timothy J. Chorvat, *Stepping Up to the Next Level: From the UETA to the URE and Beyond*, 37 IDAHO L. REV. 415 (2001);

In *Linnen v. A.H. Robins Co.*,[206] the plaintiffs requested that a blanket order for all e-mail sent among defendant employees be deemed admissible under the business records exception to the hearsay rule.[207] The court did not appear to question the assertion that e-mail fit within the definition of "business records," but rather denied the request based on the fact that the evidentiary ruling was better reserved for trial.[208] However, a different court denied a similar request under other circumstances on the basis that e-mails were not shown to be business records.[209]

Increased discovery and use of electronically stored information also carries implications for the public records exception contained in FRE 803(8). In several cases, federal district courts have held that government documents obtained from reliable Internet sources fit within the public records exception.[210] In one case, the court

---

Herbert M. Strassberg, *Computerized Business Records Can be Treated More Equitably at Trial by the United States Adopting Parts of the New Canadian System*, 9 SW. J. L. & TRADE AM. 221 (2002).

206. No. 97-2307, 1999 WL 462,015 (Mass. Super. Ct. June 16, 1999).

207. *Id.* at *7.

208. *Id.*

209. *See* New York v. Microsoft Corp., No. CIV A. 98-1233(CKK), 2002 WL 649,951, at *2 (D.D.C. Apr. 12, 2002). There, the court addressed plaintiffs' contention that an e-mail was admissible as a "record of regularly concluded activity":

> While Mr. Glaser's email may have been "kept in the course" of RealNetworks regularly conducted business activity, Plaintiffs have not, on the present record, established that it was the "regular practice" of RealNetworks employees to write and maintain such emails. Indeed, the complete lack of information regarding the practice of composition and maintenance of such emails invokes the final clause of Rule 803(6), which permits exclusion of the evidence where "the method or circumstances of preparation indicate lack of trustworthiness."

Id. at *2 (citation omitted).

210. *See, e.g.*, EEOC v. E.I. Du Pont de Nemours & Co., No. Civ. A. 03-1605, 2004 WL 2,347,559 (E.D. La. Oct. 18, 2004); United States *ex rel.* Dingle v. BioPort Corp., 270 F. Supp. 2d 968, 971 (W.D. Mich. 2003); Chapman v. S. F. Newspaper Agency, No. C 01-02305 CRB, 2002 WL 31,119,944, at *2 (N.D. Cal. Sept. 20, 2002) (holding that a computer printout of a page from the United States Postal Service's Web site came from a sufficiently reliable source to be an admissible public record under Rule 803(8)). *But see* St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999) (holding that "voodoo information taken from the Internet" was insufficient to withstand a motion to dismiss because "[n]o

admitted a printout from the U.S. Census Bureau Web site after the producing party provided enough evidence to authenticate the document.[211] Although the opposing party tried to argue that a printout from the Internet is "inherently unreliable,"[212] the court retorted that "'[p]ublic records and government documents are generally considered not to be subject to reasonable dispute,' and '[t]his includes public records and government documents available from reliable sources on the Internet.'"[213] Underlying the court's decision was an unwillingness to give a blanket characterization of unreliability to all information stored on computers and the Internet, given that the vast majority of information is now electronically-stored.[214]

2. The Best Evidence Rule and Authentication

FRE 1001, 1002, 1003, and 1004 constitute the federal version of the "best evidence rule"[215] and FRE 901 deals with authentication of documents.[216] Both areas of evidence law carry implications for the discovery and production of electronically stored information. For example, what constitutes an original when the content of a writing is at issue? Moreover, what steps must be taken to authenticate either a hard copy version of electronically stored information, or electronic information itself?[217]

a. Writing or recording

For purposes of FRE 1001, writings and recordings "consist of letters, words, or numbers, or their equivalent, set down by

---

web-site is monitored for accuracy" and "this so-called Web provides no way of verifying the authenticity" of information on which the plaintiff wished to rely).

211. *E.I. Du Ponte De Nemours & Co.*, 2004 WL 2,347,559, at *1 (stating that the printout contained the domain address from which the image was printed and a print date).

212. *Id.*

213. *Id.* (citing *Dingle*, 270 F. Supp. 2d at 971).

214. *See id.*

215. *See* FED. R. EVID. 1001–1004.

216. *Id.* 901.

217. This Part presents only a brief overview of the applicability of the Federal Rules of Evidence to electronically stored information. For a thorough discussion of authentication and the best evidence rule, please see *infra* Part VI.B.1 & E.

handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."[218] Thus, the Rule already explicitly recognizes at least some forms of electronically stored information. Yet, the same problems arise here as those discussed in Part C with respect to relying on data compilation to encompass all forms of electronically stored information. To date, courts have applied FRE 1001–1004 broadly to encompass electronically stored information.

b. The requirement of an "original"

FRE 1001 defines an original as a "writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. . . . If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."[219] The Advisory Committee's pertinent note goes on to state that, "[i]n most instances, what is an original will be self-evident and further refinement will be unnecessary . . . [P]racticality and usage confer the status of original upon any computer printout."[220] However, the Committee references a 1965 case, and much has transpired in the technological world since that time.[221] While a printout may still meet the requirement of an original, courts will likely need more information to authenticate that printout.[222] Moreover, admissibility does not guarantee high probative value, and the other party to the

218. FED. R. EVID. 1001.

219. *Id.*

220. *Id.* 1001 advisory committee's note, ¶ 3.

221. *See id.* (citing Transp. Indem. Co. v. Seib, 132 N.W.2d 871, 875 (Neb. 1965)).

222. *Infra* Part VI, provides a full analysis of this topic. Assuming the author admits sending and receiving certain messages, it appears that the most common form of authenticating printouts of e-mails is to simply call the author as a foundational witness. *See, e.g.*, J.P. Morgan Chase Bank *ex rel.* Mahonia Ltd. v. Liberty Mut. Life Ins. Co., No. 01 Civ. 11523(JSR), 2002 WL 31,867,731, at *4 (S.D.N.Y. Dec. 23, 2002) (determining that e-mails authored by senior bank officials were admissible based on the testimony of one official as to the e-mails' contents); Kearley v. State, 843 So. 2d 66, 70 (Miss. Ct. App. 2002) (allowing authentication via a rape victim's testimony that she had received and printed the contested e-mails).

litigation may challenge admissibility with evidence that tends to show the printout's unreliability or inaccuracy.[223]

As demonstrated above, courts already apply the Federal Rules of Evidence to electronically stored information according to the Rules' direct acknowledgement of data, recordings, and other compilations.[224] When the content of a writing is at issue, FRE 1002 requires the admission of the original writing.[225] Nonetheless, FRE 1003 and FRE 1004 permit the admission of duplicates where (1) the original has been lost or destroyed; (2) is unobtainable; (3) is in possession of the opponent; or (4) is not closely related to the contested issue, unless there is a dispute over the original's authenticity, or it would be unfair to admit a duplicate.[226] What constitutes an admissible duplicate in the context of electronically stored information will vary depending on the type of information at issue.[227]

Authentication of electronically stored information is more complex than authentication of paper documents due to the increased manipulability of electronically stored information.[228] For evidence to be admissible, the offering party must show "evidence sufficient to support a finding that the matter in question is what its proponent claims."[229] Requests for admissions represent one tool for authenticating a document.[230] To prove the authenticity of electronically stored information, for example, a proponent may submit a hard copy printout, along with information regarding authorship, ownership of a particular e-mail address or domain name,

---

223. *See* OVERLY, *supra* note 2, at 170.

224. *E.g., id.* 1001(3) ("If data are stored in a computer or similar device, any printout or other output readable by sight . . . is an 'original.'"); FED. R. EVID. 1001(4) ("A 'duplicate' is a counterpart produced by . . . mechanical or electronic re-recording. . . .").

225. *Id.* 1002.

226. *Id.* 1003, 1004.

227. *See, e.g.*, United States v. Capanelli, 257 F. Supp. 2d 678, 681 (S.D.N.Y. 2003) (applying FED. R. EVID. 1001–1003 in ruling that, not withstanding the destruction of the digital chip originals, recordings produced from a digital chip were admissible duplicates).

228. *See* OVERLY, *supra* note 2, at 58 ("Because of their nature it is frequently difficult to authenticate electronic documents.")

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

230. OVERLY, *supra* note 2, at 58–59.

creation date, and subsequent revisions.[231] Alternatively, the proponent may elect to copy electronic files to "write-once, read many" media[232] and prove the authenticity of the files stored therein.[233] Other methods of authentication may include audit trails, encryption authentication, and transmission via an intermediary.[234] Lastly, a printout of a computerized public record will also meet the requirements of FRE 901, so long as a witness can authenticate it with evidence that the record "is from the public office where items of this nature are kept."[235]

G. Conclusion

Much has changed since the advent of electronic discovery, though much has remained the same. Electronic discovery itself is not new;[236] rather, the novelty lies in the speed with which technology has evolved and the subsequent expansion of its use in litigation. Such rapid and drastic changes in the digital landscape have forced federal courts to account for technological advances and

---

231. *Id.* at 59; *see, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002) (finding that printouts from a Web site and attached to the declaration of plaintiff's CEO were authentic and admissible because they were declared to be "true and correct copies of pages printed from the Internet" and printed by or under the direction of the CEO).

232. Such media include the popular CD-R, which allows a user to copy files onto a CD-ROM. Once the files are copied onto the disk, they are considered "read-only" and cannot be altered. OVERLY, *supra* note 2, at 59.

233. *Id.*; *cf.* State v. Cook, 777 N.E.2d 882, 887 (Ohio Ct. App. 2002) (holding that the trial court properly admitted data generated from a mirror image of defendant's hard drive after hearing expert testimony because "there [was] no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive."). Although this is a state court case, Ohio's Rule of Evidence 901 mimics its federal counterpart. *See id.*

234. OVERLY, *supra* note 2, at 161–65. Audit trails are essentially computer files that record usage, user login information, user location, and user activities. *Id.* at 162.

235. FED. R. EVID. 901(b)(7). For instance, in *United States v. Meienberg*, 263 F.3d 1177, 1180–81 (10th Cir. 2001), a government witness satisfied Rule 901(b)(7)'s authentication requirement by testifying that the computer printouts were a record of all firearm approval numbers issued by the Colorado Bureau of Investigations to defendant's business.

236. *See, e.g.*, SEC v. Beacon Hill Asset Mgmt. LLC, No. 02CIV8855LAKHBP, 2004 WL 1,746,790, at *14 (S.D.N.Y. Aug. 3, 2004) ("For more than thirty years, Fed. R. Civ. P. 34(a) has included data stored on electronic media as being subject to a Rule 34 request. The fact that the data has not been printed out does not mean that the document does not exist.").

apply broadly applicable discovery rules to the situation at hand. One could argue that the Federal Rules of Civil Procedure should be left unaltered, given the apparent ability of courts to adapt to technological changes. Yet, consistency lends a degree of certainty to the litigation process, and modifying the Rules of Civil Procedure to directly address some of the peculiarities of electronic discovery may be preferable to adapting an older set of guidelines to a vastly different and dynamic subject area.

It is important to clarify the various types of information that are subject to discovery in order to increase certainty in electronic discovery. In addition, it is critical to recognize the advantages and disadvantages associated with the various forms in which electronic discovery may materialize. While this area of law will inevitably grow as technological strides are made, the lessons courts draw from applying the discovery process to electronically stored information as it exists today will undoubtedly be useful in the future.