**THE INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION**
**70th Annual Conference**
**Savannah, Georgia**
**September 25-28, 2005**

# "E-DISCOVERY: A PROBLEM OF E-NORMOUS PROPORTIONS?"

**By: Douglas C. Haney – City Attorney, Carmel, Indiana**

## I INTRODUCTION

## II. ELECTRONIC DATA: WHAT IS IT, WHERE IS IT AND WHY IS IT DIFFERENT?

### A. E-Data – What Is It?

1. "E-data" is data that has been created, transmitted or stored in digital form on a computer.

2. E-data includes:

   a. "Active data" - e-data in current use and normally found on computer hard-drives, data-bases and servers.

   b. "Inactive data" - e-data that must be returned to "active" status before it can be read.

   c. "Contextual data" - e-data created by the computer and that records computer system usage, including web-sites visited and documents sent.

   d. "Metadata" - e-data created by the computer or a computer program that records the "who, what, when and where" of an e-document, including document edits and comments.

### B. E-Data – Where Is It?

1. E-mail (in-house & third party)
2. Word-processing documents
3. Spread sheets
4. Back up files
5. Pagers/Answering machines
6. Fax machines/Printers
7. Home computers/Laptops
8. Voice mail
9. World Wide Web
10. On and off-site storage files
11. Hard and floppy disks
12. CD-rom's/Cassettes/Cartridges
13. DVD's/Memory sticks
14. Address books/Task notes/Calendars
15. Quarantined files
16. Discarded computers/Software
17. Zip/Jaz disks/Thumbnails
18. Palm Pilots/Blackberries
19. Power Point presentations
20. Audio/Audio-visual recordings
21. Chat rooms/Bulletin boards
22. GPS data files/Credit cards
23. Digital pictures
24. Third party retailers/Cable providers

C. E-Data: Why Is It Different?

1. Volume, Duplicity and Dispersion

a. A municipality with 500 employees will generate about five million e-documents each year.

b. Two 10-GB hard drives can hold the equivalent of one million pages of documents.

c. E-documents are duplicated and re-transmitted many times over.

d. E-documents are sent to, received from and stored in numerous locations, many of which may be unknown to the e-document author.

2. A Dynamic, Fragile and Deceptive Medium

a. Unlike paper documents, which can sit undisturbed for decades, digital data is fluid, constantly subject to loss or modification through overwriting or disposal.

b. Some metadata can be lost or altered simply by re-booting a computer or by running a computer maintenance program.

c. E-documents seem more "casual" than paper documents, which encourages angry, unsubstantiated and brutally candid statements that would never be reduced to writing.

d. It can be difficult to ensure the integrity and verify the authorship of e-documents.

3. An Indestructible and Unforgiving Medium

a. E-data has "vampire" attributes, and can be "brought back to life" by a forensic examiner.

b. Destroying every trace of an e-document is very difficult. E-data can even be recovered from a computer disk that is broken or burned in half.

c. Metadata can disclose relationships and patterns that are completely hidden in the "paper world."

d. Metadata can often trace e-document alteration or destruction efforts to their source, with devastating results.

4. Obsolescence and Oversight

a. E-data cannot be read (by humans) outside of the structure and environment in which it was created.

b. E-documents can be inadvertently lost by oversight when old computer drives are discarded and old passwords are forgotten.

c. E-data becomes more difficult and costly to re-create and read as technology evolves beyond that which created it.

5. Increased Search Time and Cost

a. The enormous amount of e-documents that are created each year makes their search, storage and management costly.

b. E-data is often jumbled together on back-up tapes in no logical, secure or easily searchable manner.

c. Confidential and privileged information is stored side-by-side with discoverable information, or even in slack spaces inside a discoverable e-document.

d. The cost of the outside computer technicians, specialty software, staff time and business disruptions needed to recover inactive e-data can be significant.

e. The legal review of e-documents prior to their production or use at trial can be time-consuming, and the risk of privilege waiver significant.

## III. ELECTRONIC DATA: WHAT IS DISCOVERABLE?

A. Since Fed.R.Civ.P. 34(a) was amended in 1970 to add "data compilations from which information can be obtained" to the definition of "document," relevant and non-privileged e-data has almost universally been deemed discoverable.

B. Fed.R.Civ.P. 26(b) is available to address unreasonably burdensome e-discovery requests and Fed.R.Civ.P. 26(c) can be used to shift some e-document production costs to the requestor.

C. Several federal[1] and state[2] courts have published their own local e-discovery rules.

[1] Federal courts that have adopted local e-discovery rules include the Eastern & Western Districts of Arkansas, the District of Wyoming, the District of Delaware, the District of New Jersey, the District of Kansas and the Middle District of Florida.

[2] State courts that have adopted local e-discovery rules include California, Illinois, Maryland, Mississippi, New Jersey and Texas.

D. State and local governments may have a separate and distinct obligation to retain and disclose e-documents under their state's "access to public records" law.

1. For example, Indiana's Access to Public Records Act[3] defines "public record" to include any writing or other material created, received, retained, maintained or filed by or with a public agency, *including "*electronically stored data." These public e-records must be retained until their destruction is approved by a county "commission on public records." Any "reckless or knowing" violation of this record retention law is a *felony*.

2. In addition to possible criminal prosecution, compliance with state record retention laws is vitally important because courts facing inadvertent e-document spoliation have held that "intent" is irrelevant when destroyed e-documents were required to be retained by law or regulation. Such destruction can lead to sanctions.[4]

E. According to one author, there may be over 2,500 e-record retention laws scattered amongst the fifty states.[5]

## IV. NEW E-DISCOVERY RULES ARE COMING!

### A. Proposed Changes To The Federal Rules of Civil Procedure

In 2004, the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States proposed changes to the Federal Rules of Civil Procedure. These changes, *which deal almost exclusively with e-discovery*, prompted over 250 written comments and three (3) days of live testimony. They are awaiting final action and could take effect on *December 1, 2006*. These proposed rules, as they relate to e-discovery, are summarized below:

1. Proposed Rule 26(a): The duty of disclosure will specifically include "electronically stored information."

2. Proposed Rule 26(b)(2)(B): Absent a showing of "good cause," a party will not be required to produce e-documents that are not "reasonably accessible because of undue burden or cost." In cases where production for "good cause" is required, cost-shifting may be ordered.

3. Proposed Rule 26(b)(5)(B): A procedure will be established for parties to follow when claiming that they inadvertently produced privileged or otherwise protected e-documents.

---

[3] I.C. 5-14-3-2 (2003).

[4] See, e.g., *Byrnie v. Town of Cromwell, 343 F.3d 93 (2nd Cir. 2001)* and the cases cited therein. Also note that a government attorney who discloses *too many* e-documents, including those containing confidential information or metadata, can violate both state law and ethical obligations. See, e.g., Indiana Code 5-14-3-10; *New York State Bar Association Committee on Professional Ethics*, Opinion No. 782 (12-08-04).

[5] *The Negligent Spoliation of Electronic Information: Practical Advice For Successfully Preserving Digital Data, Dean A. Gonsowski; www.flosinc.com/resources/pdf Files/200310 – preserving – data. pdf, at fn.19.*

4. Proposed Rules 26(f) and 16(b); Form 35: Parties will be required to discuss e-discovery issues, including the production and preservation of e-information and inadvertent privilege waivers, early in the case. These e-discovery discussions must be reported to the court.

5. Proposed Rules 33(d) and 34(a) & (b): A requesting party will be able to specify the form in which e-information will be produced, subject to objection. Unless agreed to by the parties or ordered by the court, a party will only have to produce "e-data" in one form.

6. Proposed Rule 37(f): A "safe harbor" will be created to protect parties from sanctions for failing to produce e-documents that are lost due to the routine operation of their computer system. However, this "safe harbor" will not be available to a party who violates a preservation order or who fails to take "reasonable steps" to preserve e-data.[6]

7. Proposed Rule 45: The ability to obtain "electronically stored information" by subpoena will be expressly affirmed.

B. Other E-Discovery Rules and Guidelines

The American Bar Association and several other professional groups have recently published their own proposed e-discovery rules, standards and guidelines. Some of them are summarized below:

1. *The Sedona Principles*,[7] prepared in 2004 as part of The Sedona Conference℠ Working Group Series, set out fourteen (14) "principles" for e-document production as the "best practice" in this area of discovery. Among other things, these principles encourage: (a) the early resolution of e-discovery issues, (b) clearly worded e-document requests, (c) a good faith effort to preserve e-documents, while recognizing that the preservation of every potentially relevant byte of e-data is unreasonable, (d) cost-shifting in appropriate cases and (e) a common sense approach to spoliation sanctions. The *Sedona Principles* is a good place for attorneys to find a concise overview of e-discovery issues.

2. *The Sedona Guidelines*[8] represent the second major publication in The Sedona Conference℠ Working Group Series, and is a companion piece to *The Sedona Principles*. *The Sedona Guidelines* offer well-reasoned suggestions to follow when developing an e-document management and retention policy. Suggestions include the implementation of a reasonable e-records management policy that is flexible, tailored to the specific corporate and legal needs and responsibilities of the organization, and establishes both an e-records destruction cycle and a means to put a "hold" on e-records destruction. The *Sedona Guidelines* is a "must-read" for attorneys seeking to create a new e-records policy or to amend an existing policy to better meet the needs, exigencies and subtleties of our digital world.

---

[6] This "reasonable steps" determination will apparently not consider the harm that e-document spoliation causes an opposing party.

[7] *The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production, The Sedona Conference, Sedona, Arizona (January, 2004).*

[8] *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, The Sedona Conference, Sedona, Arizona (September, 2004).*

3. ABA Revised Electronic Discovery Standards[9]

The ABA Electronic Discovery Task Force has proposed numerous revisions to its Civil Discovery Standards that are designed to address e-discovery issues. These revisions specifically remind attorneys of their obligation to advise clients of e-document preservation issues so as to avoid spoliation claims. They also identify the various e-data and e-data platforms that exist, the need to specify the format in which e-data is to be produced, the need for cost shifting (when appropriate) and the need for counsel, at their initial discovery conference, to discuss and agree upon e-discovery protocols and privilege issues.

## V. THE CREATION OF AN E-RECORDS RETENTION POLICY

### A. Step One

Meet with the heads of your administrative and IT departments to:

i. Develop a detailed understanding of your computer system.
ii. Understand your e-record management and destruction policies and practices.
iii. Obtain a list of all e-record custodians and e-record storage locations.

### B. Step Two

Review relevant statutes, case law and commentaries to understand your client's legal duties and responsibilities regarding the preservation and production of e-documents and e-data.

### C. Step Three

Develop a written e-record retention policy that:

1. Makes it clear that all e-documents and e-data on municipal computers or created by a municipal employee on "work time" is property of the municipality.

2. Complies with all applicable laws (IRS, DOL, EPA, state public records laws).

3. Tags all e-documents with metadata that will allow them to be identified and searched by file.

4. Segregates privileged and confidential e-documents from other e-documents and limits their re-transmission to non-secure sites or to sites that may result in a privilege waiver.

5. Requires all e-records to remain in a usable format during their normal retention period.

6. Provides for the retention and preservation of e-data pursuant to specific protocols.

7. Provides for the routine destruction of e-documents according to a specific timetable and subject to review and safeguard protocols.

[9] *ABA Electronic Discovery Task Force, Final Revised Amendments To Civil Discovery Standards: Report 103B (August, 2004)*

8. Designates a POC to answer e-document policy questions.

9. Designates a POC to receive "tips" and investigate possible incidents of improper e-document destruction.

10. Designates Rule 30(b)(6) e-records custodians and e-discovery administrators.

11. Designates procedures to follow when replacing obsolete computer hardware/software.

12. Provides guidance to employees as to what e-documents must be retained pursuant to your policy.

13. Provides for continued employee education and testing to ensure a complete understanding of your e-record retention policy.

14. Mandates policy compliance audits and employee discipline for policy violations.

15. Establishes detailed procedures and specific responsibilities for imposing a "litigation hold" on all e-documents relevant to a claim. This "litigation hold" procedure should:

    a. Identify the e-documents that may be relevant to a claim or that may lead to the discovery of relevant e-documents.

    b. Provide for the transmission (and periodic re-transmission) of the "litigation hold" to all employees and others who may have possession of or control over affected e-documents.

    c. Identify the e-records custodian and e-discovery administrator who will be personally responsible for your organization's compliance with the "litigation hold."

    d. Establish the procedure that will be used to identify, search for and harvest potentially responsive e-documents, to include:

        i) Placing a hold on all "key player" computer usage, over-writing, back-up, maintenance, computer upgrades and other activities or actions that could alter, damage or destroy e-data until a "mirror image"[10] is taken of their computer hard drives.

        ii) Developing a protocol for the e-records custodian to follow to ensure that:

            - e-document chain of custody logs are properly kept,
            - the e-custodian knows how and when she is able to receive, destroy and alter e-data,
            - the e-custodian retains all e-documents created after the "litigation hold" on separate media;

[10] A "mirror image" is an exact copy of a computer hard drive (including unallocated spaces and hidden partitions). It is write-protected, compressed and encrypted to verify its image integrity.

iii) Developing a protocol for the e-discovery administrator to use so that he can make informed and consistent decisions regarding e-documents and the taking of "mirror images" of those computer hard drives that may contain e-documents subject to the "litigation hold."

16. Require all document preservation efforts taken in response to a "litigation hold" to be fully and properly documented.

## VI. THE DANGERS OF E-RECORD SPOLIATION

A. Improper e-discovery conduct has been sanctioned in every federal circuit and in many state courts.

B. The duty to save responsive e-documents (in all formats) begins as soon as litigation is "reasonably anticipated," *or sooner* if required by law or regulation.

C. Courts have *imposed spoliation sanctions not only for intentional e-record destruction*, but also for the *negligent* destruction of e-documents *without* a showing of "bad faith."[11] Even "*purposeful sluggishness*" in preserving and producing e-data has been sanctioned.[12]

D. In *Zubulake V*,[13] the court found it "insufficient" for respondent's counsel to have simply alerted employees that a "litigation hold" existed. Once the "litigation hold" was in effect, counsel had a *further duty* to take *affirmative steps* to monitor her client's compliance with its e-data preservation obligations. In the court's view, these steps should have included:

1. Periodically re-issuing the "litigation hold" notice;

2. Periodically reminding all "key players" of their duty to preserve e-documents;

3. Directing the client to produce copies of all relevant e-documents; and,

4. Working with the client's IT personnel to ensure that all applicable back-up media were identified, stored and preserved.

---

[11] See, e.g., *Southern States Rack and Fixture, Inc. v. Sherwin-Williams Co., 318 F.3d 592 (4th Cir. 2003).*

[12] See, e.g., *United States v. Philip Morris, 327 F. Supp. 2d 21 (D.D.C. 2004);Zubulake v. UBS Warburg, LLC., No. 02 Civ. 1243 (SAS) (S.D.N.Y. Oct. 22, 2003); Metro Opera Ass'n. v. Local 100, Hotel & Restaurant Employees Int'l. U., 212 F.R.D. 178 (S.D.N.Y. 2003); Residential Financing Corp. v. DeGeorge Financial Corp., 306 F.3d 99 (2d Cir. 2002);Prudential Insurance Co. of America Sales Practices Litigation, 169 F.R.D. 598 (D.N.J. 1997).*

[13] *Zubulake v. UBS Wartburg LLC, No. 02 CIV.1243(SAS), 2004 WL 1620866 (S.D.N.Y. 2004).*

E. Courts have broad discretion in deciding whether and how to sanction a party for e-document spoliation, depending on the facts of the case. Spoliation sanctions have included:

- Additional discovery with cost shifting;[14]
- Fines imposed on the attorney/client;[15]
- The preclusion of an expert, evidence or a defense;[16]
- An evidentiary presumption;[17]
- An adverse inference jury instruction;[18]
- Dismissal of the action or entry of default judgment;[19] and,
- Contempt of court.[20]

F. I strongly recommend that you read *Zubulake I, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake III, 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake IV, 220 F.R.D. 212 (S.D.N.Y. 2003);* and, *Zubulake V, supra*, as well as *McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001); Rowe Entertainment, Inc., v. Wm. Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y.), aff'd 53 Fed.R.Serv. 3d 296 (S.D.N.Y. 2002),* and the cases, guidelines and resources cited therein. They should give you a good idea of what the courts will be reading when deciding whether your e-data preservation and production efforts were up to snuff.

G. Finally, as if things were not tense enough for attorneys in the world of e-discovery, several jurisdictions now recognize the tort of "negligent spoliation of evidence."[21]

## VII. SERVING AND RESPONDING TO E-DISCOVERY

### A. Your Spoliation Letter

1. Your spoliation letter should specifically demand the preservation of all electronic documents, including all metadata and contextual data, that may either be relevant to your claim or defense or that may lead to the discovery of such evidence.

2. Make sure that your letter is detailed enough to allow your opponent to identify and locate possibly relevant e-data.

3. A sample "spoliation letter"[22] is included as Attachment A.

---

[14] *GTFM v. Wal-Mart, 49 Fed. R. Serv.3d 219 (S.D.N.Y. 2000).*

[15] *See, e.g., US v Philip Morris USA, F. Supp.2d (D.D.C. July 21, 2004) ($2.75 Million sanction); In Re Prudential Insurance Co. of America Sales Practices Lit, 169 F.R.D. 598 (D.N.J. 1997) ($1 Million sanction).*

[16] *See,e.g., Trigon Ins. Co. v. U.S., 204 F.R.D. 277 (E.D. Va. 2001); Thompson v. H.U.D., 219 F.R.D. 93 (D.Md. 2003); Konstantopoulos v. Westvaco Corp., 112 F.3d 710 (3d. Cir. 1997).*

[17] *See,e.g., Advanta Care Health Partners v. Access IV, No. CO3-04496 JF, 2004 WL 1837997 (N.D. Cal. 2004).*

[18] *See,e.g., Coleman (Parent) Holdings, Inc. v. Morgan Stanley, Inc., 2005 WL 67071 (Fla. Ctr. Ct., Mar.1, 2005); QZ0, Inc. v. Moyer, 358 S.C. 246 (2004).*

[19] *See,e.g., Rambus, Inc. v. Infineon, 220 FRD 264 (E.D. Va 2004).*

[20] See, e.g., *Trigon Ins. Co., supra.; Landmark Legal Foundation v. E.P.A., 2003 WL 21715678 (D.D.C., July 24, 2003).*

[21] See, e.g., *Holmes v. Amerex Rent-A-Car, 710 A.2d 846 (D.C. App., 1998); Callahan v. Stanley Works, 703 A.2d 1014 (N.J. Super. 1997).*

B. Their Spoliation Letter

1. As soon as you receive a spoliation letter, immediately identify all "key persons" and records custodians relative to the subject matter of the letter.

2. Promptly send out your "litigation hold" notice, defining therein the categories of e-data that must be preserved in unaltered form and suspending all use and maintenance of electronic equipment that may contain such e-data. Consider sending this "litigation hold" notice to selected third parties as well. Have the "litigation hold" notice signed for by all "key persons" and all responsible e-document custodians and e-discovery administrators. A sample "litigation hold" acknowledgment form is included as Attachment B.

3. Designate the specific persons who will be responsible for ensuring that all e-documents are identified and preserved. Utilize a written preservation checklist and e-document log.

4. After you have issued your "litigation hold," ensure that all regular computer maintenance overwriting has *actually* stopped and that all "key employees" have *actually* ceased their electronic activities until a "mirror image" is obtained of their hard drives.

5. Consider retaining electronics experts to assist you with your e-discovery searches, filtering, categorization and preservation. They can create an "un-biased" chain of custody log, utilize "cutting edge" data storage, transmission, search, organization and presentation technologies, and more easily adjust their electronic strategies to changing circumstances than most in-house IT crews.

   a. Read *Best Practices For The Selection Of Electronic Discovery Vendors: Navigating the Vendor Proposal Process*,[23] for excellent insights into the process of e-expert selection.

   b. Be careful with the e-experts you retain:

      (i) Their notes and e-mails may be discoverable.
      (ii) Their spoliation of e-evidence will expose you to sanctions.
      (iii) Hire experts initially as "consulting experts." See: Fed.R.Civ.P. 26(b)(4)(B).

[22] This is a "bare-bones" document. In complex cases, spoliation letters can run four (4) pages or more in length.
[23] *Best Practices For The Selection Of Electronic Discovery Ventors: NavagatingThe Vender Proposal Process, The Sedona Conference, Sedona, Arizona (July, 2005).*

c. Use your e-experts to:

(i) Help you prepare discovery requests and responses;
(ii) Assist you at pre-trial conferences;
(iii) Identify the types of e-data you have in your possession or control;
(iv) Locate potentially responsive e-data;
(v) Forensically capture and preserve responsive e-data;
(vi) Search potentially responsive e-data by text, phrase, time period, etc.;
(vii) Filter out privileged or highly confidential e-data (and spam);
(viii) Prepare e-data for your legal review;
(ix) Prepare responsive e-data for production;
(x) Help you prepare your witnesses for deposition and trial;
(xi) Help you prepare for deposition and trial; and,
(xii) Testify at trial.

6. Consider purchasing software "tools" to assist you.

- Forensic tools: (i.e. "Pro-Discover"; "EnCase").
- Litigation support tools: (i.e. "Concordance"; "Summation").
- Trial presentation tools: (i.e. "Trial Director"; "Sanction").

7. Gather Your E-Records Support Team

a. Make sure everyone on the team knows each other, their POC's and chain of command, and their authority, duties and responsibilities as regards the preservation, gathering, searching, filtering, organizing, maintaining and reviewing of computer hardware, software and/or individual e-documents.

b. Keep a complete record of all e-discovery compliance actions and costs, as well as written chain-of-custody logs.

C. Your Rule 26(f) Discovery Conference

In any litigation that involves significant e-data, the parties (and their IT experts) should schedule an early discovery conference to:

1. Determine what e-documents exist and where they are located.
2. Determine what experts/software will be needed to access and format the e-documents.
3. Determine what steps will be taken to retain and preserve e-documents, and a chain of custody protocol.

4. Determine a methodology for e-document searches (search words, name/date ranges, 10% samplings) and the scope of the searches (no back-up tapes or fragments).

5. Determine a protocol to deal with the inadvertent waiver of privilege:

    a. "Call/Claw Back" agreement;
    b. "Quick Peek" agreement;
    c. Review of e-data by a neutral expert.

6. Agree on an e-document production format (native, PDF, TIFF).

D. The Rule 26(c) Preservation Order

Absent proof of a party's intent to destroy e-data, the issuance of a broad e-data preservation order, or allowing direct access to an opponent's computer system, is rarely appropriate.

E. The Cost-Shifting Arrangement

1. If possible, reach an agreement as to who pays for what e-discovery production costs.

    a. Absent unique circumstances, the producing party should pay the cost of obtaining, reviewing and producing "active" e-documents.

    b. Courts have begun to move away from the traditional rule that each party bears its own discovery costs when it comes to the production of "inactive" e-documents.

    c. Which party pays the costs of e-discovery may now depend on:

        i) The extent to which an e-discovery request was tailored to identify relevant information;

        ii) The availability of the requested information from other sources;

        iii) The total cost of production compared to the amount in controversy;[24]

        iv) The total cost of production compared to the resources available to each party;

        v) The relative ability of each party to control e-document production costs and its incentive to do so;

        vi) The importance of the issues at stake in the litigation; and,

        vii) The relative benefits to the parties of obtaining the e-information.[25]

[24] For some idea of how e-discovery costs can quickly escalate, consider that: Forensic images cost $600-$700 per 4GB drive; data filtering by file/date costs $5,000-$6,000 per 4GB drive and the management of potentially relevant e-documents costs $2,500-3,000 per 4GB drive. To this total add the cost of an expert spending 2-3 hours per 4GB drive, plus attorney review time, plus computer down, time, plus storage costs and business interruption. OUCH!

F. Interrogatories (Fed. R. Civ. P. 33)

Your initial interrogatories should seek to identify all of your opponent's potentially relevant e-information and how to get it. You should ask your opponent to identify, at a minimum:

1. Its computer system configuration;
2. Its back-up, storage and retrieval procedures;
3. Its firewalls, access procedures and limitations;
4. Whether its computer system can be remotely accessed;
5. Its internet provider;
6. Its e-mail program;
7. All electronic equipment used by its "key players" during the period at issue;
8. All of its e-data locations;
9. All of its e-records custodians and systems administrators; and,
10. All of its access codes and encryption particulars.

G. Depositions (Fed. R. Civ. P. 30)

Early in the case, you may want to depose your opponent's IT and administrative personnel.[26] This will help you determine the "who, what, when, where and how" of your opponent's e-document creation, storage and destruction system (its written policies *and* its actual practices). An abbreviated deposition topic summary sheet is included as Attachment C.

H. Requests To Inspect (Fed. R. Civ. P. 34)

In appropriate cases, you may want to seek permission for your forensic expert to view and analyze your opponent's actual computer system.

I. Requests For Production (Fed. R. Civ. P. 34)

1. One of the most common mistakes made in requests for the production of e-documents is to fail to describe in sufficient detail the e-data requested and the format in which you want it produced.

2. Do not forget to request the policies, manuals and other documents that govern your opponent's computer use and e-document creation, storage and destruction, in addition to the e-documents that specifically relate to the subject matter of your dispute.

---

[25] See, e.g., *Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); McPeek v. Ashcroft 202 F.R.P. 31 (D.D.C. 2001) and Rowe Entertainment Inc. v. William Morris Agency, 205 F.R.D. 421; aff'd. 53 Fed R. Serv. 3d 296 (S.D.N.Y. 2002).* See also, *Wiginton v. CB Richard Ellis, Inc., 2004 WL 1895122 (N.D. Ill. 2004); Multi Technology Services, LP v. Verizon Southwest, 2004 WL 1553480 (N.D. Tex. 2004); Thompson v. H.U.D., 219 F.R.D. 93 (D.Md. 2003);Kormendi v. Computer Associations International, No.02 CIV 2996 (LAK) (DFE), 2002 WL 31385832 (S.D.N.Y. Oct. 21, 2002).*

[26] Also consider deposing third parties who may have copies of relevant e-data. (Fed.R.Civ.P. 30).

## VIII. THE INTRODUCTION OF E-DOCUMENTS AT TRIAL

### A. Admissibility Is The Key

Obtaining e-documents and e-document experts is all well and good, but of limited value to your client if the evidence they can provide is not admissible in court. Like all documents and testimony offered for the truth of the matter stated,[27] admissible e-evidence must be authentic, reliable and trustworthy.

### B. Daubert, Frye and Expert Testimony

In 1923, the District of Columbia Court of Appeals issued its decision in *Frye v. United States*.[28] In *Frye,* the court established a "test" for the admissibility of scientific evidence that was based upon a determination of whether the scientific principle or discovery upon which an expert's testimony is based has been sufficiently established to have gained "general acceptance" in the applicable scientific field. This *Frye* "general acceptance" test soon became the standard used by courts across the nation, and stood unassailable for almost fifty (50) years.

However, the 1970's saw many new types of forensic evidence emerge and seek judicial approval. In 1975, the Federal Rules of Evidence also took effect.[29] Faced with a groundswell of new scientific "theories," some courts and commentators began to decry them as so-called "junk science." Others welcomed these new scientific discoveries, and began to criticize the *Frye* test as being too conservative and unnecessarily deferential to the scientific community's willingness to embrace and accept scientific advancements.

---

[27] Of course, many e-documents are used as demonstrative evidence, which requires a different and normally less onerous foundation. Essentially, a witness need only testify that he is familiar with the matter at issue and that the demonstrative evidence (i.e. computer graphics) fairly and accurately represents same.

[28] *Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).*

[29] The Federal Rules of Evidence took effect on July 1, 1975.

In 1991, the Ninth Circuit issued its decision in ***Daubert v. Merrell Dow Pharmaceuticals, Inc.***[30] This civil tort case turned on the admissibility of expert testimony that was based upon a re-analysis of certain epidemiological data. This re-analysis caused the plaintiff's expert to conclude that Merrill Dow's morning sickness medication caused birth defects. The Ninth Circuit ruled that this evidence should be excluded under the ***Frye*** test, because the plaintiff's expert had not submitted his data re-analysis for peer review nor published his findings in a scientific journal so that it could be scrutinized and accepted by others in the field. On appeal, the United States Supreme Court held that the ***Frye*** test was too rigid for the evaluation of scientific testimony, and that the new Federal Rules of Evidence, specifically Rule 702, was the appropriate standard to use in such evaluations.[31] The Court held that, under Rule 702, a trial judge, when determining whether the reasoning or methodology underlying a pro-offered expert opinion was scientifically valid and properly applied to the case facts (and therefore sufficiently "reliable" to be admitted into evidence) should consider, amongst others, the following factors:

1. Whether the scientific theory or technique at issue can (and has) been tested;
2. Whether the theory/technique has been subject to peer review and publication;
3. The known or potential error rate of the theory/technique;
4. The existence (and use) of testing/analysis standards and controls; and,
5. Whether the theory/technique has gained widespread acceptance within the relevant scientific community.[32]

The ***Daubert*** Court stressed that, under Rule 702, this judicial inquiry should be "flexible," with the overarching goal being the determination of the scientific validity, and thus the evidentiary relevance and reliability, of the proffered evidence.

---

[30] 951 F.2d 1128 (9th Cir. 1991).

[31] Fed. R. Evid. 702 states as follows: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

[32] *Daubert v. Merrill Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Following *Daubert*, the federal courts replaced *Frye's* "general acceptance" test with the more flexible standard set forth in Rule 702. However, *Daubert* received a decidedly lukewarm reception in state courts. To date, less than half of the states have adopted the *Daubert* standard.[33] Another one-third, including California, Florida, Illinois and New York, have expressly or effectively retained the *Frye* test.[34] The rest of the states have either adopted their own "hybrid" test or have not squarely decided this issue.[35]

Given the above, when you decide upon your e-discovery approach, and especially if you are in a *Frye* jurisdiction, ensure that any e-experts you retain have the proper credentials and utilize a scientific methodology in reaching their conclusions that will pass muster when it comes time to take the stand.

C. E-document Admissibility Issues

1. In order to enter an e-document into evidence for the truth of the matter stated, its proponent must show that it:

   a. is "relevant;"
   b. Is "authentic;"
   c. Is not inadmissible "hearsay;" and,
   d. Has probative value that outweighs its potentially prejudicial, confusing or cumulative nature.

2. Objections to the authenticity of an e-document often include claims that:

   a. It was altered after its creation;[36]
   b. The computer program that generated it is not reliable; and/or,
   c. The purported author is not the true author.

3. Objections as to authenticity can normally be overcome by the introduction of evidence indicating the reliability of the computer program, metadata that tracks the e-document back to its author, chain-of-custody logs and proof of computer drive image integrity and/or expert testimony that reduces the possibility that the e-document was altered by spoofers, Trojan Horse programmers or other electronic interlopers. Faced with this evidence, most courts will rule that these objections go to the weight, not the admissibility, of e-evidence.

---

[33] By my count, the states that follow the *Daubert* standard are: Alaska, Arkansas, Connecticut, Delaware, Hawaii (limited), Iowa (limited), Kentucky, Louisiana, Maine, Montana, Nevada, New Mexico, North Carolina, Ohio, Oklahoma, Rhode Island, South Carolina (limited), South Dakota, Tennessee, Texas, Vermont, West Virginia and Wyoming.

[34] By my count, the states that still apply the *Frye* test are: Arizona, California, Florida, Illinois, Idaho, Indiana, Kansas, Maryland, Michigan, Minnesota, Mississippi, Nebraska, New York, North Dakota, Pennsylvania and Washington.

[35] "Hybrid" tests appear to be used in Colorado, Georgia, Oregon, Utah and Wisconsin.

[36] See, e.g., *U.S. v. Tank, 200 F.3d 627 (9th Cir. 2000) (Internet chat room logs admitted. Argument that they could have been "altered" goes to weight, not admissibility).*

4. The "reply letter" and "consistent action" doctrines can also be used to authenticate e-mail whenever an e-mail reply contains the original message in its body or a person takes actions consistent with her e-mail message.

5. Hearsay[37] objections can be handled as follows:

   a. *It's not hearsay.* The hearsay rule was created to prevent unreliable out-of-court statements *by humans* from being considered for the truth of the matter stated. To the extent e-records contain only *electronically generated data* that has never been "touched" by a human, they are not hearsay. A machine has no conscience, no ulterior motives, and no possibility of making a "mistake" unless it is tampered with or not functioning properly. Absent evidence of these problems, computer-generated e-records, once properly authenticated, should survive a "hearsay" challenge because they are not hearsay.[38] Such records are also not hearsay to the extent they contain an admission by a party-opponent.[39]

   b. *It's admissible under a hearsay exception.* While computer stored documents that were created or altered by humans are hearsay if they are being offered for the truth of the matter asserted, they are admissible under one or more of the following hearsay exceptions:

      i. *Business records (Fed. R. Evid. 803(6) & (7))*. Computer records can often be admitted as "business records" if they were created and maintained as part of a routine procedure and in a manner that strongly suggests their accuracy. Evidence of the absence of an entry in a business e-record is also admissible.

      ii. *Public Records (Fed. R. Evid. 803 (8), (9) & (10))*. E-documents that constitute official records and reports prepared and maintained by public offices and agencies to prove their activities, or that concern matters observed under a legal duty or obligation, can be admitted as "public records." E-documents that record vital statistics maintained by public officials in the course of their duties are also admissible under this hearsay exception. Evidence of the absence of an entry in a "public record" is admissible as well.

      iii. *Present Sense Impression/Excited Utterance (Fed. R. Evid. 803(1) & (2)*). Electronic statements made while the author was perceiving an event or condition, or made while under stress or excitement from such event or condition, are admissible as "present sense impressions" or as "excited utterances."

      iv. *Recorded Recollection (Fed. R. Evid. 803(5))*. An electronic memorandum concerning a matter about which a witness once had knowledge can be read into evidence as a "recorded recollection."

---

[37] See, Fed. R. Evid. 801(c).

[38] See, e.g., *Telewizia Polska USA v. Echostar Satellite Corp., 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004) (Internet Archives web page "snapshot" was not hearsay, as it merely showed what had been on the website); U.S. v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000) (E-mail was admitted over authentication and hearsay objections).*

[39] See, Fed. R. Evid. 801(d)(2).

6. Best Evidence Rule[40] objections can be handled by reminding the court that e-data, in its native or "original" form, consists of a jumble of 0's and 1's. To present e-data to the trier of fact in its "original" form would render it meaningless. Perhaps recognizing this, Fed. R. Evid. 1001(3) defines an "original" as including a computer print-out shown to accurately reflect e-data stored in the computer. In jurisdictions that do not follow the Federal Rules of Evidence, practicality and common usage should confer the status of "original" on e-documents printed in paper form.

7. Objections claiming that computer print-outs are "evidence summaries" can be countered by arguing that, just because computer print-outs transform millions of bytes of digital data into a format humans can read, this does not turn them into "summaries" admissible only upon compliance with Rule Fed. R. Evid. 1006. That Rule only applies to computer print-outs that merely summarize other independent e-data.

8. As the case law regarding e-discovery is still fluid, and the court (and you) may still be learning this highly technical area of law, it is prudent to offer as much direct and circumstantial evidence as you can that shows your e-documents to be accurate, reliable and trustworthy. This is one time when you might want to pile it on a little thick, so as to exorcize any remaining "junk science" concerns and to provide the court (and any reviewing court) with a complete record in support of the admissibility of your e-evidence.

## VIII. CONCLUSION

[40] See, Fed. R. Evid. 1002.

ATTACHMENT A

*CERTIFIED MAIL, RETURN RECEIPT REQUESTED*

*RE: Request to Retain And Preserve Digital Data*

*Dear _____:*

*I represent the City of _____ ("City"). On _____, 2005, the City received your letter dated _____, alleging that _____ (the "Claim"). You threaten litigation if this matter is not resolved to your client's satisfaction.*

*Under these circumstances, and because the information relevant to your claim may have been prepared, transmitted and/or stored digitally, you are hereby requested to retain and preserve in unaltered form all digital data and documents that may be relevant to the subject matter of the Claim, or that may lead to the discovery of such data and/or documents (the "Digital Data"). Digital Data includes, but is not limited to, digital files, programs, spreadsheets, metadata and residual data, as well as on-line and stored data regardless of format, and all other electronically created, received, transmitted or retained data and documents wherever located.*

*Please do not engage in any rotation, alteration and/or destruction of any electronic media that could result in the alteration or loss of Digital Data. Please do not dispose of any electronic media storage devices that may contain Digital Data. Please do not run any automated purging programs that may affect any Digital Data.*

*This Request is on-going and remains in effect until a final and non-appealable resolution of the Claim by and between the City and your client has been obtained.*

*If you have any questions regarding this Request, please contact the undersigned immediately at _____.*

ATTACHMENT B

ELECTRONIC DOCUMENT HOLD NOTICE # 00925

Matter # 0031-05 : City v. Ima Klutz ; Fall on Monon Trail on 08-28-05.

Records To Be Held: All Monon Trail Maintenance Logs from 01-01-00 through 08-30-05

All Monon Trail Police/Ambulance/911 calls from 01-01-00 through 08-30-05

All Constituent Complaints about Monon Trail from 01-01-00 through 08-30-05

All City records regarding the Monon Trail from 08-01-05 through 08-30-05

All City records regarding Ima Klutz, regardless of date

1. I have read and understand this Electronic Document Hold Notice.

   Yes ☐ No ☐

2. I have or may have records subject to this Electronic Document Hold Notice.

   Yes ☐ (*Do not access these documents without prior City Attorney approval]*
   No ☐

3. I agree to preserve these records in their present form until the City Attorney informs me in writing that this Electronic Document Hold has been lifted as to these records.

   Yes ☐ No ☐

4. Other individuals, computer systems or electronic medias that may contain or have knowledge of information or documents relating to this matter are: _____.

5. _____.

Signed _____ Date _____

*This document is not a public record. It is a privileged communication and/or attorney work product.*

ATTACHMENT C

1. Computer System Configuration

   a. Describe the types of computer system(s) used in your business.

   b. Identify the types of software used on your computer system(s).

   c. Identify by name and title the person(s) responsible for the operation, maintenance and back-up of your computer system(s).

   d. Does [name of key players] have a home computer, PDA, cell phone, fax machine (etc.), they use for business purposes?

   e. Are passwords or encrypted files used on your computer system(s)?

      - Describe how files are protected.
      - Identify who can provide access codes

   f. Has your company modified the way it uses its computers within the past year? to comply with discovery requests? on account of this lawsuit?

   g. _____

2. E-Data Back-up and Retention

   a. Are files ever deleted from your computer system(s)?
      - How, when and by whom?

   b. Are your computer system(s) backed up?
      - Do you follow a procedure when backing-up your computer system(s)?
      - Describe the back-up program(s) used.

   c. Are archival back-ups ever created?
      - What files have been archived?
      - Where and by whom are they maintained?

   d. Have you modified your backup procedures in the last year? to comply with discovery requests? on account of this lawsuit?

   e. Describe any disaster recovery plans in place at your company during [relevant time period].

   f. Have your disaster recovery plans been changed in the last year? to comply with discovery requests? on account of this lawsuit?

   g. _____

3. System Maintenance and Access

   a. Are utility or network maintenance programs ever used on your computer(s)?
      - Which program(s)?
      - Has any program been used to permanently "wipe" any computer files within the last year?
      - Has any program been used to de-fragment, optimize or compress drives within the last year?

   b. Does anyone outside of your company have access to your computers?

   c. Are your office computers secured? How?

   d. Has your company computer hardware/software been upgraded or replaced in the past year?

   e. Do you use third parties to search, transmit, store or retrieve your electronic data?

   f. _____

4. E-Data Authentication

   a. Are individual computer files purged when an employee transfers departments or leaves your company?

   b. Are computer passwords/access codes revoked or re-used when an employee transfers departments or leaves your company?

   c. When employee workstations are reassigned:

      - Are hard drives wiped or re-formatted for a new user?
      - Are hard drives backed-up before a new user begins to use the system?

   d. Describe how used or obsolete computer equipment and software is disposed of.

   e. Describe how, if at all, used computer disks and drives are treated before their disposal.

   f. Has your company used outside contractors to upgrade its computer hardware/software?

   g. Are changes or modifications made to your company's computer hardware/software recorded or logged in some manner?

   h. _____

5. Other Areas of Inquiry

   a. _____
   b. _____