204 Leading Through the Electronic Discovery Quagmire (Part 1): Nuts & Bolts Best Practices

Patrick Oot
Director of Electronic Discovery & Senior Counsel
Verizon Legal Department

Sonya L. Sigler
General Counsel
Cataphora, Inc.

Miriam M. Smolen
Associate General Counsel
Fannie Mae

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).
Materials may not be reproduced without the consent of ACC.
Reproduction permission requests should be directed to Julienne Bramesco at ACC: 202/293-4103, ext. 338; bramesco@acca.com

Faculty Biographies

Patrick Oot

Patrick L. Oot is director of Electronic Discovery and Senior Counsel at Verizon in Arlington, Virginia. He has extensive experience in discovery practices including commercial litigation, regulatory filings, and antitrust matters. Mr. Oot is charged with advising Verizon business units on electronic discovery while developing new technologies with the goal of increasing cost-efficiency. In 2006, Mr. Oot was nominated for the Verizon Excellence Award for playing a key role in the successful completion of Verizon's response to the Department of Justice's Second Request for Documents in its acquisition of MCI. He has also testified as Verizon's 30(b)(6) witness for discovery-related inquiries in other matters.

Currently, Mr. Oot is a member of the advisory board for The Georgetown University Law Center CLE Program's Advanced E-discovery Institute. He is also a member of the advisory board for an independent search and retrieval science consortium. Mr. Oot actively participates in the sedona conference's working groups; focusing on best practices for selecting search and retrieval technology and e-mail management systems. He is a member of the International Legal Technology Association. He speaks regularly at legal conferences including and general counsel round tables across the country.

Mr. Oot received both his B.A. and J.D. from Syracuse University and his LL.M. from Georgetown University Law Center.

Sonya L. Sigler

Sonya Sigler is the vice president, business development & general counsel at Cataphora, Inc. She actively works on intellectual property matters including negotiating and drafting various Internet, technology, software licensing and other agreements. She has over ten years of experience in business relationship management through her role as in-house counsel and as a business development and legal consultant to start-ups such as Treasure Media, RealCommunities and IDO Systems, as well as established companies such as Sony and Intuit.

Ms. Sigler worked as an attorney at Sega supporting the business development, product development, marketing, and finance groups, as well as Sega Studios in Los Angeles. More recently, Sonya worked at Intuit, where she evaluated and negotiated agreements and licenses for Intuit's industry-leading financial software products, Quicken, Quicken Mortgage, and QuickBooks.

She writes articles and speaks frequently on the subjects of electronic discovery, intellectual property, and other topics. She is a member of the ACC, the ABA, and the sedona conference working Group 1 on electronic document retention and production. Past board work has included the Women in Interactive Entertainment Association, women in technology advisory board and the Nova Vista Symphony.

Ms. Sigler holds B.A. from UC Berkeley a J.D. from Santa Clara University.

Miriam M. Smolen

Miriam Smolen serves as associate general counsel in the office of corporate compliance for Fannie Mae, in Washington, DC. In that role, she has assessed legal and regulatory risk for business operations and created and implemented business specific compliance plans, implemented the code of business conduct to prevent conflict of interest and other violations, and developed fraud prevention and detection processes to deter mortgage fraud. Her responsibilities also include conducting internal investigations, and responding to government investigations. Her expertise includes electronic evidence retention and production.

Previously, Ms. Smolen was an assistant U.S. attorney with the U.S. Attorney's Office in the District of Columbia, and served a detail with the Department of Justice computer crime and intellectual property section. She investigated and tried dozens of violent crime, narcotics, and financial fraud cases, including multi-million dollar embezzlements from government agencies and labor unions, health care fraud, and computer crime. She specialized in health care fraud and intellectual property and computer crime cases, serving as the health care fraud coordinator and chair of the health care fraud task force, and as the computer and telecommunications coordinator for the D.C. U.S. Attorney's Office. Prior to joining the U.S. Attorney's Office, Ms. Smolen was an associate with Latham and Watkins in Washington DC and clerked for the Honorable Stanley S. Harris, United States District Court, District of Columbia.

She has received numerous Justice Department Special Achievement Awards and was awarded the Department of Health and Human Services Integrity Award for prosecution of Medicaid fraud. She has been a frequent lecturer for the National Medicaid Fraud Control Units, the National Association of Attorney's General, and the ABA on health care fraud issues, and on investigation and prosecution of white-collar cases for numerous law enforcement training groups.

She received her B.A. from University of California, Berkeley and her J.D., from Boalt Hall School of Law, University of California Berkeley.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

ACC 2006 Annual Meeting
San Diego, CA
204 Leading Through the Electronic Discovery Quagmire (Part 1): Nuts & Bolts Best Practices

Monday, October 23, 2006 2:30 PM - 4:00 PM

Some Resources:

1. "The Electronic Discovery Handbook: Forms, Checklists, and Guidelines" by Sharon D. Nelson, Bruce A. Olson and John W. Simek (Published by ABA Law Practice Management Section)

2. ***Association of Corporate Counsel ("ACC") Virtual Library***
(Free to Members, and includes: 1) "Sample Electronic Discovery Interrogatories and Requests for Production of Documents;" 2) InfoPak on "Records Retention;" and 3) "Ten Tips for Electronic Discovery."

3. FileNet's ***"Compliance Roadmap"*** Includes: 1) ROI Calculator; 2) Whitepapers & Podcasts; and 3) Records Management Guide.
(Free, and should be available through website: www.filenet.com)

4. ***"Leveraging Content Analytics to Reduce E-Discovery Risks and Costs"***
(Free Whitepaper available through www.KahnConsultingInc.com)

5. Vendor Newsletters, such as Cataphora's "Discussions"
(www.cataphora.com)

6. The Sedona Conference Website (Free, Research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. www.thesedonaconference.org)

7. Discovery Resources
(Free, electronic discovery resources http://www.discoveryresources.org/)

DISCOVERY OF DIGITAL INFORMATION

Ronald J. Hedges, U.S.M.J.
Martin Luther King, Jr., Federal Building and Courthouse
50 Walnut Street
Newark, New Jersey 07101
Judge_Ronald_Hedges@njd.uscourts.gov

September 27, 2004

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

NOTICE

In August of 2004, proposed amendments to the Federal Rules of Civil Procedure addressing electronic discovery were published. Here is a "capsule" summary of the proposals and the rule-making process:

> Disseminating the package of proposals in legal newspapers and posting the nearly-200 page report of the Judiciary's Advisory Committee on Civil Rules starts a six-month period for public comment. Publication also begins a long process that could see the amendments take effect by December 1, 2006. The proposed amendments will be available on the Judiciary's website at www.uscourts.gov.
>
> The changes generally seek to modernize existing rules language to explicitly mention electronic discovery and require the parties to talk about any issues relating to disclosure or discovery early in the lawsuit.
>
> Among the proposed amendments is one that relieves a party from retrieving and producing electronic information that is not reasonably accessible, including information in disaster-recovery back-up tapes, in response to a discovery request.
>
> Another amendment sets out procedures putting a hold on the use of privileged information inadvertently produced until the court has had an opportunity to rule on the underlying issue.
>
> Under a proposed 'safe harbor' provision, a party may not be sanctioned under the rules if electronic information has been lost or destroyed as a result of the routine operation of the party's computer system - such as information lost when back-up tapes are recycled - if the party took reasonable steps to preserve the information after it knew the information to be relevant.
>
> All public comment will be considered by the Advisory Committee on Civil Rules, and be included with its recommendations, anticipated in the spring of 2005, to the Judicial Conference Committee on Rules of Practice and Procedure.
>
> If approved by the committee, the amendments would be considered by the Judicial Conference at its September 2005 meeting, and forwarded to the Supreme Court. The high court's adoption of new amendments then would be sent to Congress and, if meeting no objections, would take effect December 1, 2006. [Vd. 36, No. 7, The Third Branch 6 (July 2004)].

The proposed amendments are summarized in greater detail in an article by Ken Withers of the Federal Judicial Center titled, "Two Tiers and a Safe Harbor: Federal Rulemakers Grapple with E-Discovery," and published in The Federal Lawyer 29 (Sept. 2004), and in "Call for Comments on New E-discovery Rules," Vol. 4, No. 9, Digital Discovery & e-Evidence 1 (Sept. 2004). Much more to follow.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

TABLE OF CONTENTS

DISCOVERY OF DIGITAL INFORMATION[1]

I. WHAT DOES "DIGITAL INFORMATION" ENCOMPASS?

A. What is digital (or electronic) discovery:

> Electronic discovery refers to the discovery of electronic documents and data. Electronic documents include e-mail, web pages, word processing files, computer databases, and virtually anything that is stored on a computer. Technically, documents and data are 'electronic' if they exist in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. Electronic discovery is often distinguished from 'paper discovery,' which refers to the discovery of writings on paper that can be read without the aid of some devices. [The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery at 1 [Sedona Conference Working Group Series Jan. 2004) (hereinafter "The Sedona Principles"].

B. Is digital information different?

> Computer files, including e-mails, are discoverable. *** . However, the Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of e-mail files. Several commentators have noted important differences between the two. ***. Chief among these differences is the sheer volume of

[1]For sources of information on digital discovery, see Digital Discovery & e-Evidence, a monthly publication of Pike & Fischer, Inc., and the unofficial web site created by Ken Withers of the Federal Judicial Center at http://www.kenwithers.com. See also, for helpful "primers" on various aspects of electronic information, the two-part series of articles in the July and August, 2002 issues of The Federal Lawyer and the articles in the June 2004 issue of For the Defense.

Texts may also be of assistance: M. Arkfeld, Electronic Discovery and Evidence (Law Partner Publishing: 2004); J. Feldman, Essentials of Electronic Discovery (Glasser Legal Works: 2003).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> electronic information. 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 email. Additionally, computers have the ability to capture several copies (or drafts) of the same e-mail, thus multiplying the volume of documents. All of these e-mails must be scanned for both relevance and privilege. Also, unlike 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. Thus, parties incur additional costs in translating the data from the tapes into useable form. One commentator has suggested that given the extraordinary costs of converting obsolete backup tapes into useable form, the requesting party should be required to show that production will likely result in the discovery of relevant information. [Byers v. Illinois State Police, 2002 U.S. Dist LEXIS 9861, *31-33 (N.D. Ill. May 31) (citations omitted)[2]].

C. The Sedona Principles[3] include definitions, as described in Vol. 3, No. 4, Digital Discovery & e-Evidence 10 (April, 2003):

> Understanding technical terms is the first hurdle to overcome in mastering electronic evidence. To that end, the Sedona Principles are accompanied by a glossary of words and phrases. Here are the Sedona definitions of some of the less familiar terms.

---

[2]"There are many ways in which producing electronic documents is qualitatively and quantitatively different from producing paper documents." The Sedona Principles at 3. "[B]road categories of differences" include volume and duplicability, persistence, changeable content, obsolescence, and dispersion and search ability. Id. at 3-5.

[3]The Sedona Principles are available at http:/www.thesedonaconference.org. A 2004 "Annotated Version" is available from Pike & Fisher, Inc.

The American Bar Association has also been active in the area of electronic discovery. In 1999, its House of Delegates adopted "Civil Discovery Standards," two of which addressed electronic discovery (available at http://www.abanet.org/litigation/taskforces/standards. html). In August of 2004, the House of Delegates amended the Civil Discovery Standards "to supplement existing rules and address practical aspects of the electronic discovery process." Report, 2004 Amendments to the Civil Standards Relating to Electronic Discovery. The amendments are available at http://www.abanet.org/leadership/2004/annual/daily/journal/103B.doc.

Distributed Data: Distributed Data is that information belonging to an organization which resides on portable media and non-local devices such as home computers, laptop computers, floppy disks, CD-ROMS, personal digital assistants ('PDAs'), wireless communication devices (e.g., Blackberry), zip drives, Internet repositories such as e-mail hosted by Internet service providers or portals, web pages, and the like. Distributed data also includes data held by third parties such as application service providers and business partners.

Forensic Copy: A Forensic Copy is an exact bit-by-bit copy of the entire physical hard drive of a computer system, including slack and unallocated space.

Legacy Data: Legacy Data is information the development of which an organization may have invested significant resources to and that has retained its importance, but has been created or stored by the use of software and/or hardware that has been rendered outmoded or obsolete.

Metadata: Metadata is information about a particular data set which describes how, when and by whom it was collected, created, accessed, and modified and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and is unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed. (Typically referred to by the not highly informative 'shorthand' phrase 'data about data,' describing the content, quality, condition, history, and other characteristics of the data.)

Residual Data: Residual Data (sometimes referred to as 'Ambient Data') refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in the file slack space; and (3) data within files that have functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

Migrated Data: Migrated data is information that has been moved from one database or format to another, usually as a result of a change from one hardware or software technology to another.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

D. The Manual for Complex Litigation (Fourth Edition)[4] assumes that, "[f]or the most part," digital or electronic information will be "generated and maintained in the ordinary course of business." However,

> Other data are generated and stored as a byproduct of the various information technologies commonly employed by parties in the ordinary course of business, but not routinely retrieved and used for business purposes. Such data include the following:
>
> .Metadata, or 'information about information.' ***
>
> .System data, or information generated and maintained by the computer itself. The computer records 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.
>
> .Backup data, generally store offline on tapes or disks. Backup data are created and maintained for short-term disaster recovery, not for retrieving particular files, databases, or programs. These tapes or disks must be restored to the system from which they were recorded, or to a similar hardware and software environment, before any data can be accessed.
>
> .Files purposely deleted by a computer user. Deleted files are seldom actually deleted from the computer hard drive. The operating system renames and marks them for eventual overwriting, should that particular space on the computer hard drive be needed. The files are recoverable only with expert intervention.
>
> .Residual data that exist in bits and pieces throughout a computer hard drive. Analogous to the data on crumpled newspapers used to pack shipping boxes, these data are also recoverable with expert intervention.
>
> Each of these categories of computer data may contain information within the scope of discovery. The above categories are listed by order of potential relevance and in ascending order of cost and burden to recover and produce. [Manual, §11.446].

[4] Hereinafter "Manual." Published in 2004.

E. In Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003), the court discussed electronic data storage media. Here are the descriptions of those media, as summarized in Vol. 3, No. 6, Digital Discovery & e-Evidence 6 (June, 2003):

> Here are the full descriptions of electronic data storage media, taken from the Zubulake decision. The listings are in order from most to least accessible; citations have been omitted.
>
> **.Active, online data:** Online storage is generally provided by magnetic disk. It is used in the very active stages of an electronic record's life–when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds. Examples of online data include hard drives.
>
> **.Nearline data:** This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape. Examples include optical disks.
>
> **.Offline storage/archives:** This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Offline storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to offline media involves manual intervention and is much slower than online or nearline storage. Access speed may be minutes, hours or even days, depending on the access – effectiveness of the storage facility. The principle difference between nearline data and offline data is that offline data lacks 'the coordinated control of an intelligent disk subsystem,' and is, in the lingo, JBOD ('Just a Bunch Of Disks').
>
> **.Backup tapes:** A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> transfer speeds also vary considerably. ... The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks. As a result, [t]he data on a backup tape are not organized for retrieval of individual documents or files [because] ... the organization of the data mirrors the computer's structure, not the human records management structure. Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.
>
> **.Erased, fragmented or damaged data:** When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters. ... As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk. Such broken-up files are said to be 'fragmented,' and along with damaged and erased data can only be accessed after significant processing.

F. Conclusion? "The complexity and rapidly changing character of technology for the management of computerized materials may make it appropriate for the judge to seek the assistance of a special master or neutral expert, or call on the parties to provide the judge with expert assistance, in the form of briefings on the relevant technological issues." Manual, §11.446; see The Sedona Principles, Comment 10.c ("In certain circumstances, a court may find it beneficial to appoint a 'neutral' person (e.g., a special master or court-appointed expert) who can help mediate or manage electronic discovery issues").

II. WHEN TO BEGIN TO "THINK DIGITAL"

A. Rule 11(a) requires that, "[e]very pleading, written motion, and other paper shall be signed by at least one attorney of record ***."

B. Rule 11(b) provides that,

> [b]y presenting to the court *** a pleading, written motion, or other paper, an attorney *** is certifying that, to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances,–
>
> (1) it is not being presented for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation;
>
> (2) the claims, defenses, and other legal contentions therein are warranted by existing law or by a nonfrivolous argument for the extension, modification, or reversal of existing law or the establishment of new law;
>
> (3) the allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery; and
>
> (4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on a lack of information or belief.

C. The language of Rule 11 "stresses the need for some prefiling inquiry into both the facts and the law to satisfy the affirmative duty imposed by the rule. The standard is one of reasonableness under the circumstances." Advisory Committee Note to 1983 amendment to Rule 11. Rule 11 "continues to require litigants to 'stop-and-think' before initially making legal or factual contentions." Advisory Committee Note to 1993 amendment to Rule 11(b) and ©).

D. Why is knowledge of information in electronic format needed at earliest stage of litigation?[5]

---

[5]For a discussion of how to "map out a straightforward plan for electronic discovery response," both at the commencement of litigation and for discovery purposes, see V. Llewllyn & E. Green, (Implementing a Response Plan," For the Defense 21 (June 2004): see also N.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

1. Ensure that there is an "off switch" for any deletion of data.

2. Comply with Rule 11.[6]

3. Prepare for Rule 26(f) conference.

4. Prepare for Rule 26(a)(1) disclosures.

E. Data Preservation:[7] A responsibility shared by attorney and client. In Zubulake v. UBS Warburg LLC, 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. July 20) ("ZubulakeV"), sanctions were imposed on the defendant for failing to preserve e-mail. In imposing sanction, Judge Scheindlin stated:

> Counsel failed to communicate the litigation hold order to all key players. They also failed to ascertain each of the key players' document management habits. By the same token, UBS employees – for unknown reasons – ignored many of the instructions that counsel gave. This case represents a failure of communication, and that failure falls on counsel and client alike.
>
> At the end of the day, however, the duty to preserve and produce documents rests on the party. Only that duty is made clear to a party, either by court order or by instructions from counsel, that party is on notice of its obligations and acts at its own peril. Though more diligent action on the part of counsel would have mitigated some of the damage caused by UBS's deletion of e-mails, UBS deleted the e-mails in defiance of explicit instructions not to [*48-49].

See "Zubulake V Places Onus of E-discovery More Fully on Counsel," Vol. 4, No. 8, Digital Discovery & e-Evidence 1 (Aug. 2004); D. Gonsowski, "Zubulake V Spoliation Comes Home to Roost," Vol. 4, No. 8, Digital Discovery & e-Evidence 3 (Aug. 2004). Zubulake V has been described "as a platform to set forth certain basic guidelines that outside and in-house counsel should follow in the presentation and production of electronic records." J. Rosenthal, "Practical Implication of Zubulake V," Vol. 4, No. 9, Digital Discovery & e-Evidence 4 (Sept. 2004).

F. Note that databases prepared by or at the direction of counsel may be work product and yet discoverable. See Portis v. Chicago, 2004 US. Dist. LEXIS 12640 (N.D. Ill. July 7).

Lawson & D. Regard, "Assessing Your Case from a Data Standpoint: Key Considerations and Questions," Vol. 4, No. 8, Digital Discovery & e-Evidence 6 (Aug. 2004).

[6] Of course, an attorney should inquire into the validity of digital information. In Jiminez v. Madison Area Technical College, 321 F.3d 652 (7 Cir. 2003), the court of appeals affirmed the imposition of Rule 11 sanctions on the plaintiff and her attorney. The plaintiff had produced "a number of inflammatory letters and e-mails allegedly written by various colleagues and supervisors" and made reference to these in her racial discrimination complaint. The district court concluded in a Rule 11 hearing that the letters and e-mail were "obviously fraudulent."

[7] "[O]nce a party reasonably anticipates litigation, it has a duty to suspend any routine document purging system that might be in effect and to put in place a litigation hold to ensure the preservation of relevant documents - failure to do so constitutes spoliation." Rambus, Inc. v. Infineon Technologies AG, 220 F.R.D. 264, 281 (E.D. Va. 2004); see Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

II. DIGITAL INFORMATION AND RULE 26(f)

A. Why should discovery of electronic information be considered as early as possible? Here is what the Manual says:

> Computerized data have become commonplace in litigation. The sheer volume of such data, when compared to conventional paper documentation, can be staggering. A floppy disk, with 1.44 megabytes, is the equivalent of 720 typewritten pages of plain text. A CD-ROM, with 650 megabytes, can hold up to 325,000 typewritten pages. One gigabyte is the equivalent of 500,000 typewritten pages. Large corporate computer networks create backup data measure in terabytes, or 1,000,000 megabytes; each terabyte represents the equivalent of 500 billion typewritten pages of plain text.
>
> Digital or electronic information can be stored in any of the following: mainframe computers, network servers, personal computers, hand-held devices, automobiles, or household appliances; or it can be accessible via the Internet, from private networks, or from third parties. Any discovery plan must address issues relating to such information, including the search for it and its location, retrieval, form of production, inspection, preservation, and use at trial.
>
> * * *
>
> There are several reasons to encourage parties to produce and exchange data in electronic form:
>
> .discovery requests may themselves be transmitted in computer-accessible form–interrogatories served on computer disks, for example, could then be answered using the same disk, avoiding the need to retype them;
>
> .production of computer data on disks, CD-ROMs, or by file transfers significantly reduces the costs of copying, transport, storage, and management–protocols may be established by the 11 parties to facilitate the handling of documents from initial production to use in depositions and pretrial procedures to presentation at trial;
>
> .computerized data are far more easily searched, located, and organized than paper data; and
>
> .computerized data may form the contents for a common document depository (see section 11.444).
>
> The goal is to maximize these potential advantages while minimizing the potential problems of incompatibility among various computer systems, programs, and data, and minimizing problems with intrusiveness, data integrity, and information overload." [Manual, §11.446].

B. Rule 26(f) requires the parties to confer:

> Conference of Parties; Planning for Discovery. Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:
>
> (1) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;
>
> (2) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;
>
> (3) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and
>
> (4) any other orders that should be entered by the court under Rule 26©) or under Rule 16(b) and ©).
>
> The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. A court may

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> order that the parties or attorneys attend the conference in person. If necessary to comply with its expedited schedule for Rule 16(b) conferences, a court may by local rule (I) require that the conference between the parties occur fewer than 21 days before the scheduling conference is held or a scheduling order is due under Rule 16(b), and (ii) require that the written report outlining the discovery plan be filed fewer than 14 days after the conference between the parties, or excuse the parties from submitting a written report and permit them to report orally on their discovery plan at the Rule 16(b) conference.

C. The Rule 26(f) conference is the first opportunity to discuss electronic information with adversaries.[8] Some district courts require the subject to be addressed:

1. Eastern and Western Districts of Arkansas Local Civil Rule 26.1:

> The Fed. R. Civ. P. 26(f) report filed with the court must contain the parties' views and proposals regarding the following:
>
> * * *
>
> 4. Whether any party will likely be requested to disclose or produce information from electronic or computer-based media. If so:
>
> a. whether disclosure or production will be limited to data reasonably available to the parties in the ordinary course of business;
>
> b. the anticipated scope, cost and time required for disclosure or production of data beyond what is reasonably available to the parties in the ordinary course of business;
>
> c. the format and media agreed to by the parties for the production of such data as well as agreed procedures or such production;
>
> d. whether reasonable measures have been taken to preserve potentially discoverable data from alteration or destruction in the ordinary course of business or otherwise;
>
> e. other problems which the parties anticipate may arise in connection with electronic or computerbased discovery.

2. District of Delaware Default Standard for Discovery of Electronic Documents:" [9]

> **1. Introduction.** It is expected that parties to a case will cooperatively reach agreement on how to conduct e-discovery. In the event that such agreement has not been reached by the Fed. R. Civ. P. 16 scheduling conference, however, the following default standards shall apply until such time, if ever, the parties conduct e-discovery on a consensual basis.
>
> **2. Discovery conference.** Parties shall discuss the parameters of their anticipated e-discovery at the Fed. R. Civ. P. 26(f) conference, as well as at the Fed. R. Civ. P. 16 scheduling conference with the court, consistent with the concerns outlined below. More specifically, prior to the Rule 26(f) conference, the parties shall exchange the following information:
>
> - A list of the most likely custodians of relevant electronic

[8] State court rules have also begun to discuss electronic information. See Mississippi Rule of Civil Procedure 26, as amended by Supreme Court of Mississippi Court Order 15 effective May 29, 2003; Texas Rule of Civil Procedure 196.4, which provides:

> To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot - through reasonable efforts - retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

[9] This default standard is not incorporated in local rules. Instead, it "is available for use by the Court and by parties engaged in litigation"in the District." Ad Hoc Committee for Electronic Discovery of the U.S. District Court for the District of Delaware, http://www.ded.uscourts.gov/Announce/HotPage22.htm. See, for a discussion of the standard, K. Brady, "District of Delaware Establishes Default Standard for Discovery of E-data," Vol. 4., No. 8, Digital Discovery and e-Evidence 10 (Aug. 2004).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

materials, including a brief description of each person's title and responsibilities (see ¶ 6).

- A list of each relevant electronic system that has been in place at all relevant times and a general description of each system, including the nature, scope, character, organization, and formats employed in each system. The parties should also include other pertinent information about their electronic documents and whether those electronic documents are of limited accessibility. Electronic documents of limited accessibility may include those created or used by electronic media no longer in use, maintained in redundant electronic storage media, or for which retrieval involves substantial cost.

- The name of the individual responsible for that party's electronic document retention policies ('the retention coordinator'), as well as a general description of the party's electronic document retention policies for the systems identified above (see ¶ 6).

- The name of the individual who shall serve as that party's 'e-discovery liaison' (see ¶ 2).

- Provide notice of any problems reasonably anticipated to arise in connection with e-discovery.

To the extent that the state of the pleadings does not permit a meaningful discussion of the above by the time of the Rule 26(f) conference, the parties shall either agree on a date by which this information will be mutually exchanged or submit the issue for resolution by the court at the Rule 16 scheduling conference.

3. E-discovery liaison. In order to promote communication and cooperation between the parties, each party to a case shall designate a single individual through which all e-discovery requests and responses are made ('the e-discovery liaison'). Regardless of whether the e-discovery liaison is an attorney (in-house or outside counsel), a third party consultant, or an employee of the party, he or she must be:

- Familiar with the party's electronic systems and capabilities in order to explain these systems and answer relevant questions.

- Knowledgeable about the technical aspects of e-discovery, including electronic document storage, organization and format issues.

- Prepared to participate in e-discovery dispute resolutions.

The court notes that, at all times, the attorneys of record shall be responsible for compliance with e-discovery requests. However, the e-discovery liaisons shall be responsible for organizing each party's e-discovery efforts to insure consistency and thoroughness and, generally, to facilitate the e-discovery process.

4.Timing of e-discovery. Discovery of electronic documents shall proceed in a sequenced fashion.

- After receiving requests or document production, the parties shall search their documents, other than those identified as limited accessibility electronic documents and produce responsive electronic documents in accordance with Fed. R. Civ. P. 26(b)(2).

- Electronic searches of documents identified as of limited accessibility shall not be conducted until the initial electronic documents search has been completed. Requests for information expected to be found in limited accessibility documents must be narrowly focused with some basis in fact supporting the request.

- On-site inspections of electronic media under Fed. R. Civ. P. 34(b) shall not be permitted absent exceptional circumstances, where good cause and specific need have been demonstrated.

5. Search methodology. If the parties intend to employ an electronic search to locate relevant electronic documents, the parties shall disclose any restrictions as to scope and method which might affect their ability to conduct a complete electronic search of the electronic documents. The parties shall reach agreement as to the method of searching, and the words, terms, and phrases to be searched with the assistance of the respective e-discovery liaisons, who are charged with familiarity with the parties' respective systems. The parties also shall reach agreement as to the timing and conditions of any additional searches which may become necessary in the normal course of discovery. To minimize the expense, the parties may consider limiting the scope of the electronic search (e.g., time frames, fields, document types).

6. Format. If, during the course of the Rule 26(f) conference, the parties cannot agree to the format for document production,

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

electronic documents shall be produced to the requesting party as image files (e.g., PDF or TIFF). When the image file is produced, the producing party must preserve the integrity of the electronic document's contents, i.e., the original formatting of the document, its metadata and, where applicable, its revision history. After initial production in image file format is complete, a party must demonstrate particularized need for production of electronic documents in their native format.

7. Retention. Within the first thirty (30) days of discovery, the parties should work towards an agreement (akin to the standard protective order) that outlines the steps each party shall take to segregate and preserve the integrity of all relevant electronic documents. In order to avoid later accusations of spoliation, a Fed. R. Civ. P. 30(b)(6) deposition of each party's retention coordinator may be appropriate.

The retention coordinators shall:

- Take steps to ensure that e-mail of identified custodians shall not be permanently deleted in the ordinary course of business and that electronic documents maintained by the individual custodians shall not be altered.

- Provide notice as to the criteria used for spam and/or virus filtering of e-mail and attachments, e-mails and attachments filtered out by such systems shall be deemed non-responsive so long as the criteria underlying the filtering are reasonable.

Within seven (7) days of identifying the relevant document custodians, the retention coordinators shall implement the above procedures and each party's counsel shall file a statement of compliance as such with the court.

8. Privilege. Electronic documents that contain privileged information or attorney work product shall be immediately returned if the documents appear on their face to have been inadvertently produced or if there is notice of the inadvertent production within thirty (30) days of such.

9. Costs. Generally, the costs of discovery shall be bone by each party. However, the court will apportion the costs of electronic discovery upon a showing of good cause.

10. Discovery disputes and trial presentation. At this time, discovery disputes shall be resoled and trial presentations shall be conducted consistent with each individual judge's guidelines. [footnote omitted].

3. District of Kansas Electronic Discovery Guidelines:[10]

1. Existence of electronic information. With respect to the discovery of electronic information, prior to the Faddier, Civ.P. 26(f) conference, counsel should become knowledgeable about their clients' information management systems and their operation, including how information is stored and retrieved. In addition, counsel should make a reasonable attempt to review their clients' electronic information files to ascertain their contents, including archival, backup, and legacy data (outdated formats or media).

2. Duty to disclose. Disclosures pursuant to Fed.R.Civ.P. 26(a)(1) must include electronic information. To determine what information must be disclosed pursuant to this rule, counsel shall review with their clients the clients' electronic information files, including current files as well as back-up, archival, and legacy computer files, to determine what information may be used to support claims or defenses (unless used solely for impeachment). If disclosures of electronic information are being made, counsel shall also identify those individuals with knowledge of their clients' electronic information systems who can facilitate the location and identification of discoverable electronic information.

3. Duty to notify. A party seeking discovery of computer-based information shall notify the opposing party of that fact immediately, and, if known at the time of the Fed.R.Civ.P. 26(f) conference, shall identify as clearly as possible the categories of information that may be sought.

4. Duty to meet and confer regarding electronic information.

During the Fed.R.Civ.P. 26(f) conference the parties shall confer regarding the following matters:

(a) Computer-based information in general. Counsel shall

[10] These guidelines are not included in local rules. Attorneys are directed to the guidelines by initial scheduling orders.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

attempt to agree on steps the parties will take to segregate and preserve computer-based information in order to avoid accusations of spoliation. Counsel shall also attempt to agree on the steps the parties will take to comply with the decisions and rules requiring the preservation of potentially relevant information after litigation has commenced.

(b) E-mail information. Counsel shall attempt to agree on the scope of e-mail discovery and e-mail search protocol.

©) Deleted information. Counsel shall attempt to agree on whether deleted information still exists, the extent to which restoration of deleted information is needed, and who will bear the costs of restoration.

(d) Back-up and archival data. Counsel shall attempt to agree on whether back-up and archival data exists, the extent to which back-up and archival data is needed, and who will bear the cost of obtaining such data.

(e) Costs. Counsel shall discuss the anticipated scope, cost, and time required for disclosure or production of data beyond what is reasonably available to the parties in the ordinary course of business, and shall attempt to agree on the allocation of costs.

(f) Format and media. Counsel shall discuss and attempt to agree on the format and media to be used in the production of electronic information.

(g) Privileged material. Counsel shall attempt to reach an agreement regarding what will happen in the event privileged electronic material or information is inadvertently disclosed.

4. District of New Jersey Local Civil Rule 26.1(b)(2):

The parties shall submit their Fed. R. Civ. P. 26(f) discovery plan containing the parties' views and proposals regarding the following:

***

(d) whether any party will likely request or produce computerbased or other digital information, and if so, the parties' discussions of the issues listed under the Duty to Meet and Confer in L. Civ. R. 26.1(d)(3) below ***.

5. District of New Jersey Local Civil Rule 26.1(d):

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

(2) Duty to Notify. A party seeking discovery of computerbased or other digital information shall notify the opposing party as soon as possible, but no later than the Fed. R. Civ. P. 26(f) conference, and identify as clearly as possible the categories of information which may be sought. A party may supplement its request for computer-based and other digital information as soon as possible upon receipt of new information relating to digital evidence.

(3) Duty to Meet and Confer. During the Fed. R. Civ. P. 26(f) conference, the parties shall confer and attempt to agree on 21 computer-based and other digital discovery matters, including the following:

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

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

6. District of Wyoming Local Civil Rule 26.1(d)(3):

(A) Duty to Notify. A party seeking discovery of computer-based

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> information shall notify the opposing party immediately, but no later than the Fed. R. Civ. P. 26(f) conference of that fact and identify as clearly as possible the categories of information which may be sought.
>
> (B) Duty to Meet and Confer. The parties shall meet and confer regarding the following matters during the Fed. R. Civ. P. 26(f) conference;
>
> (I) Computer-based information (in general). Counsel shall attempt to agree on steps the parties will take to segregate and preserve computer-based information in order to avoid accusations of spoilation;
>
> (ii) E-mail information. Counsel shall attempt to agree as to the scope of e-mail discovery and attempt to agree upon an e-mail search protocol. This should include an agreement regarding inadvertent production of privilege e- mail messages.
>
> (iii) Deleted information. Counsel shall confer and attempt to agree whether or not restoration of deleted information may be necessary, the extent to which restoration of deleted information is needed, and who will bear the costs of restoration; and
>
> (iv) Back-up data. Counsel shall attempt to agree whether or not back-up data may be necessary, the extent to which back-up data is needed and who will bear the cost of obtaining back-up data.

D. Rule 26(f) affords the opportunity to, among other things:

1. Inquire into what information adversaries have in electronic format and how expensive production will be.[11]

2. Inquire into who is most knowledgeable about an adversary's electronic information systems.

3. Discuss preservation of electronic data.[12] What the Manual says about preservation orders:

> Before discovery starts, and perhaps before the initial conference, consider whether to enter an order requiring the parties to preserve and retain documents, files, data, and records that may be relevant to the litigation. Because such an order may interfere with the normal operations of the parties and impose unforseen burdens, it is advisable to discuss with counsel at the first opportunity about the need for a preservation order and, if one is needed, the scope, duration, method of data preservation, and other terms that will best preserve relevant matter without imposing undue burdens. A blanket preservation order ay be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations. In addition, a preservation order will likely be ineffective if it is formulated without reliable information

[11] In In Re Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437 (D.N.J. 2002), class action plaintiffs agreed to pay for paper copies of documents that, unknown to them, were available in a less expensive electronic format. As a commentator has stated, "[l]itigants ought not place a cart blanche order for something without knowing what is available and what potential cost may inhere. Conversely, the responding party has some responsibility to explain what is available and to present reasonable alternatives to the requesting party." A. Blakley, ed., Electronic Information 62-63 (Federal Bar Ass'n : 2002). Thus, parties might consider how electronic records "could be rendered mutually searchable by electronic means." In re Lorazepam & Clorazepate Antitrust Litigation, 300 F. Supp. 2d 43, 47 (D.D.C. 2004).

[12] "A party's obligation to preserve evidence that may be relevant to litigation is triggered once the party has notice that litigation may occur." Renda Marine, Inc. v. United States, 58 Ct. Cl. 57, 60 (2003) (rejecting government's reliance on records retention policy inconsistent with duty to preserve evidence and ordering government to produce back-up tapes). "The duty to presume material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation. ***. If a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence." Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001).

See, for a discussion of when the duty to preserve attaches in the context of a records retention policy and the effect of an adverse inference instruction for spoliation, Stevenson v. Union Pacific Rr. Co., 354 F.3d 739, 745-51 (8 Cir. 2004). See, for a discussion of preservation of electronic records, Principle 5 and the comments thereto of The Sedona Principles. ABA Standard 29(a) also addresses the duty to preserve.

In Dodge, Warren & Peters Ins. Services, Inc. v. Riley, 130 Cal. Rptr. 2d 385 (Ct. App. 2003), an appellate court affirmed the issuance of an injunction to prevent the loss of digital information and to allow a court-appointed expert access to that information. For the consequences of violating an injunction to preserve information by reformatting hard drives and erasing backup tapes, see Landmark Legal Foundation v. EPA, 272 F. Supp. 2d 70, 85-87 (D.D.C. 2003).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

from the responding party regarding what data-management systems are already in place, the volume of data affected, and the costs and technical feasibility of implementation. The following are among the points to consider in formulating an effective data preservation order:

.Continued operation of computers and computer networks in the routine course of business may alter or destroy existing data, but a data preservation order prohibiting operation of the computers absolutely would effectively shut down the responding party's business operations. Such an order requires the parties to define the scope of contemplated discovery as narrowly as possible, identify the particular computers or network servers affected, and agree on a method for data preservation, such as creating an image of the hard drive or duplicating particular data on removable media, thereby minimizing cost and intrusiveness and the downtime of the computers involved.

.Routine system backups for disaster recovery purposes may incidentally preserve data subject to discovery, but recovery of relevant data from nonarchival backups is costly and inefficient, and a data-preservation order that requires the accumulation of such backups beyond their usual short retention period may needlessly increase the scope and cost of discovery. An order for the preservation of backup data obliges the parties to define the scope of contemplated discovery narrowly to minimize the number of backups that need to be retained and eventually restored for discovery purposes.

.A preservation order may be difficult to implement perfectly and may cause hardship when the records are stored in data-processing systems that automatically control the period of retention. Revision of existing computer programs to provide for longer retention, even if possible, may be prohibitively expensive. Consider alternatives, such as having parties duplicate relevant data on removable media or retaining periodic backups. Any preservation order should ordinarily permit destruction after reasonable notice to opposing counsel; if opposing counsel objects, the party seeking destruction should be required to show good cause before destruction is permitted. The order may also exclude specified categories of documents or data whose cost of preservation outweighs substantially their relevance in the litigation, particularly if copies of the documents or data are filed in a document depository * * * or if there are alternative sources for the information. The court can defer destruction if relevance cannot be fairly evaluated until the litigation progresses. As issues in the case are narrowed, the court may reduce the scope of the order. The same considerations apply to the alteration or destruction of physical evidence. [Manual, §11.442 (footnote omitted,[13]].

What test should a court apply in issuing a protective order? Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 138 n.8 (Ct. Cl. 2004):

> Other courts have held that the requirements for issuing an injunction must be satisfied before a preservation order may issue. ***. The court, however, believes that the more recent of these decisions ignore significant changes made to the Federal Rules of Civil Procedure since the 1960's, further establishing the case management powers of judges. In the court's view, a document preservation order is no more an injunction than an order requiring a party to identify witnesses or to produce documents in discovery. ***. While such pretrial and discovery orders take the basic form of an injunction (an order to do or not to do something), the decisional law suggests that, in issuing them, courts need not observe the rigors of the four-factor analysis ordinarily employed in issuing injunctions. ***. In the court's view, the same ought to hold true for preservation orders. In particular, contrary to defendant's claim, the court sees no reason for it to consider whether plaintiff is likely to be successful on the merits of its case in deciding whether to protect records from destruction. In the court's view, such an approach would be decidedly to put the cart before the horse.

Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433-34 (W.D. Pa. 2004):

> [W]e conclude that the four prong test typically applied to matters concerning injunctive relief is not a completely appropriate test to utilize when examining the need for a preservation order, particularly since proof of a probability of success in the litigation is not an appropriate consideration in the determination whether to order preservation of documents. To require such proof would be contrary to the dictates of the scope of discovery which permits discovery of all things, not privileged, that appear to be 'reasonably calculated to

[13]See, for examples of data preservation orders, the attached "Order Concerning Electronic Discovery Hearing," In re: Prempro Products Liability Litigation (E.D. Ark. Nov. 17, 2003), and Pueblo of Laguna v. United States, 60 Fed. Ct. 133, 141-43 (Ct. Cl. 2004).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

lead to discovery of admissible evidence.' Fed. R. Civ. P. 26(b)(1). In addition, the public interest is not a significant factor in the discovery process as discovery at its essence affects only the parties to the litigation, and additionally access to particularly sensitive items obtained in discovery can be limited by the court with the additional requirement of destruction or return to the opposing party after completion of an appeal. Considering these differences, adoption of the four part test used for injunctive relief is not appropriate in the judicial determination of motions seeking preservation orders.

The determination whether to issue a preservation order should properly include consideration of a court's power to oversee discovery and correct abuses. Additionally, where the preservation of evidence is alleged to be of utmost urgency because of an imminent threat to the integrity or existence of evidence, either by intentional or unintentional means, the guidance and approach utilized by courts in the granting of injunctive relief can assist a court in assessing the level of the threat to the evidence with regard to the magnitude and imminence of the danger. An evaluation of a motion for a preservation order therefore demands application of a separate and distinct test, which can be formulated by molding the factors used in granting injunctive relief with the considerations, policies and goals applicable to discovery.

While remaining consistent with the Federal Rules of Civil Procedure, but still addressing the need to perform the judicial duty to oversee and decide discovery disputes, this Court believes that a balancing test which considers the following three factors should be used when deciding a motion to preserve documents, things and land: 1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; 2) any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and 3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.

At the outset, in implementing this balancing test it is important to stress that the type of evidence will change from case to case and clearly the attendant circumstances of each case will dictate the necessity of the preservation order requested. The issues raised by a request for a preservation order require the trial court to exercise its discretion, and the factors set forth in the balancing test are only intended to assist the court by focusing on important areas which will arise in all such cases. Finally, it is important to note that the Court believes that a motion for a preservation order can be granted with regard to all items of evidence which are *discoverable* in accordance with Federal Rule of Civil Procedure 26(b)(1), without the necessity of establishing that the evidence will necessarily be relevant and admissible at trial. [footnotes omitted].

4. Address production of "confidential" information under a protective agreement or order.[14]

5. Address the consequences of inadvertent production of privileged materials.[15]

---

[14]For an example of a broad protective order in the digital discovery context, see Jicarilla Apache Nation v. United States, 60 Fed. Cl. 413, 414 (Ct. Cl. 2004). Note, however, that "[t]he mere fact that a document is a computer record or an electronic document does not warrant protection from disclosure." Holland v. GMAC Mortgage Corp., 2004 WL 1534179, *4 (D. Kan. June 30).

[15] Parties sometimes try to facilitate discovery by agreeing that the disclosure of a privileged document will not be deemed a waiver with respect to that document or other documents involving the same subject matter. Some courts, however, have refused to enforce such agreements." Manual, §11.431 (footnote omitted). Such agreements do have limits, as evidenced by the "Entry Regarding Inadvertently Disclosed Document," In re: Bridgestone/Firestone, Inc., Tire Products Liability Litigation (S.D. Ind. Oct. 10 2001)(attached).

See, with regard to inadvertent waiver of "electronic communication," the two-part article by F. Ruderfer, that appeared in the September and October, 2002 issues of Digital Discovery & e-Evidence. See also United States v. Rigas, 281 F. Supp. 2d 733 (S.D.N.Y. 2003), in which the government inadvertently produced to defense counsel a hard drive on which was unknowingly copied the entire computer network account of a government paralegal. In denying the defendants' request to retain the privileged information, the court took note of "three schools of thought" on waiver through inadvertent disclosure.

"[M]any parties to document-intensive litigation enter into so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents." Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (footnote omitted). A clawback (or "quick peek") agreement, however, "is not an option in many situations and must be carefully examined." J. Redgrave & E. Bachmann, "Ripples on the Shores of Zubulake," The Federal Lawyer 33 (Nov./Dec. 2003); see, with regard to concerns raised by clawback or quick peek agreements, Comment 10.d of The Sedona Principles

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

6. Learn areas of agreement/disagreement about "subjects on which discovery may be needed." Rule 26(f)(2).

7. Plan your discovery requests.

E. Thoughts from the Manual on what might be done by attorneys:

> The time and expense of discovery may sometimes be substantially reduced if pertinent information can be retrieved from existing computerized records. Moreover, production in computer-readable form of relevant files and fields (or even of an entire database) can reduce disputes over the accuracy of compilations made from such data and enable experts for both sides to conduct studies using a common set of data. On the other hand, accessing and using computer-generated evidence is subject to numerous pitfalls. * * *. The parties' computer experts should informally discuss, in person or by telephone, procedures to facilitate retrieval and production of computerized information; the attorneys can then confirm these arrangements in writing. [Manual, §32.432 (footnote omitted)[16]].

Another concern with clawback or quick peek agreements may be that these are not binding on nonsignatories. Will production of privileged materials under an agreement be deemed a waiver vis-a-vis a third party?

[16]ABA Standard 31 describes a number of items about electronic discovery that parties might discuss at the Rule 26(f) conference.

IV. DIGITAL INFORMATION AND RULE 26(a)(1)

A. Rule 26(a)(1) requires the automatic disclosure of, among other things:

> (A) the name and if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;
>
> (B) a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;
>
> ©) a computation of any category of damages claimed by the disclosing party, making available for inspection and copying as under Rule 34 the documents or other evidentiary material, not privileged or protected from disclosure, on which such computation is based, including materials bearing on the nature and extent of injuries suffered ***. [emphasis added].

B. Rule 26(a)(1) also introduces the concept of bifurcation of discovery. Rule 26(a)(1) requires disclosure of information that a party "may use to support its claims or defenses. " This is consistent with Rule 26(b)(1), which allows discovery "regarding any matter *** that is relevant to the claim or defense of any party." Attorneys should use the Rule 26(f) meeting to decide what the "claims or defenses" in a case are and the nature of Rule 26(a)(1) disclosure of electronic information.

C. Is the individual most knowledgeable about a party's electronic information systems subject to disclosure under Rule 26(a)(1)(A)?

D. Rule 26(a) allows a party to object to disclosure:

> These disclosures must be made at or within 14 days after the Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in the circumstances of the action and states the objection in the Rule 26(f) discovery plan. In ruling on the objection, the court must determine what disclosures–if any–are to be made, and set the time for disclosure.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

E. What the Manual says:

> Prediscovery disclosure avoids the cost of unnecessary formal discovery and accelerates the exchange of basic information to plan and conduct discovery and settlement negotiations. The judge should administer Rule 26(a)(1) to serve those purposes; disclosure should not place unreasonable or unnecessary burdens on the parties (and should not require disclosure of any information that would not have to be disclosed in response to formal discovery requests). In complex litigation, this rule may need modification or suspension. The scope of disputed issues and relevant facts in a complex case may not be sufficiently clear from the pleadings to enable parties to make the requisite disclosure. One purpose of Rule 26(f)'s required meeting of counsel is to identify issues and reach agreement on the content and timing of the initial disclosures. To the extent the parties cannot agree at their meeting, it sometimes helps to defer disclosure and fashion an order at the Rule 16 conference, defining and narrowing the factual and legal issues in dispute and establishing the scope of disclosure. This will require suspending, by stipulation or order, Rule 26(f)'s presumptive ten-day deadline for making disclosure. Although Rule 26(a)(1) defines certain information that must be disclosed, it does not limit the scope of prediscovery disclosure and exchange of information. The parties have a duty to conduct a reasonable investigation pursuant to disclosure, particularly when a party possesses extensive computerized data, which may be subject to disclosure or later discovery. The rule does not require actual production (except for damage computations and insurance agreements), but only identification of relevant information and materials. The judge may nevertheless direct the parties to produce and exchange materials in advance of discovery, subject to appropriate objections. Effective use of this device without excessive and unnecessary burdens on the parties can streamline the litigation. [Manual, §11.13 (footnote omitted)].

V. DISCOVERY

A. Digital discovery and the discovery rules:[17]

> The best approach to electronic discovery begins by recognizing how existing precedent and new technology interact. The rules governing discovery are, as noted above, broadly stated standards that require reasonableness in their application. As such, the rules governing discovery are *media neutral*, in that they apply to documents existing in all media–paper, electronic, or stone tablets. Due to their generality, however, the proper application of the rules only takes shape when one understands the specific context in which the rule is applied. For electronic discovery, this requires that the litigants and the courts understand how electronic documents work, and the costs and benefits of different approaches to discovery.
>
> The result is a process of *translation*: precedent from the world of paper discovery provides a starting point, composed of the legal rule and the application in the specific facts of the case. One can translate that precedent to the world of electronic discovery by asking whether the factual differences between the paper context and the electronic context are relevant to the rule. I f so, the precedent may not be a good model. If not, the paperbased precedent could be an adequate starting point for discovery in the electronic context. [The Sedona Principles at 8].

B. Basics

1. Back to the bifurcation of discovery: In addition to allowing discovery on any matter "relevant to the claim or defense," Rule 26(b)(1) allows discovery, [f]or good cause *** of any matter relevant to the subject matter involved in the action." The bifurcation was introduced by the 2000 amendment of Rule 26(b)(1) and, according to the Advisory Committee Note, "is designed to involve the court more actively in regulating the breadth of sweeping and contentious discovery." Unfortunately, as the Advisory Committee Note goes on to say, "[t]he dividing line between information relevant to the claims and defenses and that relevant only to the subject matter of the action cannot be defined with precision."

---

[17]Of course, a party may attempt to defer discovery until a dispostive motion is decided. See Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc. 2003 WL 1809465,*2 (N.D. Ill. April 4).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

2. The concept of proportionality.[18] This appears in Rule 26(b)(2), which provides, in pertinent part:

> The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (I) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26©).
>
> Rule 26(b)(2) "contemplates greater judicial involvement in the discovery process and thus acknowledges the reality that it cannot always operate on a self-regulating basis." Advisory Committee Note to 1983 amendments to Rule 26. "The objective is to guard against redundant or disproportionate discovery ***." Id. By 2000, the Advisory Committee "has been told repeatedly that courts have not implemented these limitations with the vigor that was contemplated." [GAP Report of Advisory Committee to 2000 amendment to Rule 26(b)(1). 192 F.R.D. 340, 390 (2000)].

[18]For an example of how Rule 26(b)(2) has been applied, see Patterson v. Avery Dennison Corp., 281 F.3d 576, 681-82 (7th Cir. 2002), in which the Seventh Circuit Court of Appeals affirmed the district court's refusal to compel the deposition of an officer of the defendant corporation: "[I]n light of the burdens that a deposition would have placed on the company, and Patterson's refusal to avail herself of other reasonably available means of discovery, and the relatively small amount in controversy ***," the district court was affirmed. Plaintiff's request for the deposition was triggered by one e-mail the corporate officer had sent.

See also, although making no specific reference to Rule 26(b)(2), Wright v. AmSouth Bancorportion, 320 F.3d 1198, 1205 (11 Cir. 2003). In Wright, the court of appeals held that the district court had not abused its discretion in denying the plaintiff's request for discovery into word processing files of five employees of the defendant over a two and one-half period. "Wright has not tried to identify particular items within the expansive request nor has he provided a theory of relevance that might narrow the scope of this request."

3. Rule 26(g) ("Signing of Disclosures, Discovery Requests, Responses, and Objections"):

> (1) Every disclosure made pursuant to subdivision (a)(1) or subdivision
>
> (a)(3) shall be signed by at least one attorney of record in the attorney's individual name, whose address shall be stated. An unrepresented party shall sign the disclosure and state the party's address. The signature of the attorney or party constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the disclosure is complete and correct as of the time it is made.
>
> (2) Every discovery request, response, or objection made by a party represented by an attorney shall be signed by at least one attorney of record in the attorney's individual name, whose address shall be stated. An unrepresented party shall sign the request, response, or objection and state the party's address. The signature of the attorney or party constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the request, response, or objection is:
>
> (A) consistent with these rules and warranted by existing law or a good faith argument for the extension, modification, or reversal of existing law;
>
> (B) not interposed for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation; and
>
> ©) not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation. If a request, response, or objection is not signed, it shall be stricken unless it is signed promptly after the omission is called to the attention of the party making the request, response, or objection, and a party shall not be obligated to take any action with respect to it until it is signed. ***.

4. Rule 34 ("Production of Documents and Things"):

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> (a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phone records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

What the Advisory Committee Note to the 1970 amendment to Rule 34 says about "documents:"

> The inclusive description of 'documents' is revised to accord with changing technology. It makes clear that Rule 34 applies to electronics data compilations from which information can be obtained only with the use of detection devices, and that when 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. The burden thus placed on respondent will vary from case to case, and the courts have ample power under Rule 26©) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs. Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.

In re: Ford Motor Co., 345 F.3d 1315 (11 Cir. 2003):

> Rule 34(a) does not grant unrestricted, direct access to a respondent's database compilations. Instead, Rule 34(a) allows a requesting party to inspect and to copy the product–whether it be a document, disk, or other device–resulting from the respondent's translation of the data into a reasonably useful form.
>
> *** 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 the preservation if his records, confidentiality of nondiscoverable matters, and costs.' [345 F.3d at 1316-17 (quoting Rule 34(a)[19]].

What the Manual says about production of computerized data under Rule 34:

> Conventional 'warehouse' productions of paper documents often were costly and time consuming, but the burdens and expense were kept in check by the time and resources available to the requesting parties to review and photocopy the documents. In a computerized environment, the relative burdens and expense shift dramatically to the responding party. The cost of searching and copying electronic data is insignificant. Meanwhile, the tremendously increased volume of computer data and a lack of fully developed electronic records-management procedures have driven up the cost of locating, organizing, and screening data for relevance and privilege prior to production. Allowing requesting parties access to the responding parties' computer systems to conduct their own searches, which is in one sense analogous to the conventional warehouse paper production, would compromise legally recognized privileges, trade secrets, and often the personal privacy of employees and customers. [Manual, §11.446 [20]].

---

[19] Might the Ford Motor court, rather than relying on Rule 34 and what could be argued is that rule's outmoded concept of "databases" from the 1970's, have reached the same result by undertaking a "proportionality" analysis under Rule 26(b)(2)?

[20] "When a party seeks to compel discovery, it first has the burden of demonstrating the relevance of the information to the lawsuit. *** . In the context of computer systems and computer records, inspection or seizure is not permitted unless the moving party can 'demonstrate that the documents they seek to compel do, in fact, exist and are being unlawfully withheld.' ***. 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." Bethea v. Comcast, 218 F.R.D. 328, 329-30 (D.D.C. 2003).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

B. Cost-bearing.

1. In 1998, the Advisory Committee proposed an amendment to Rule 34(b). The amendment would have added this sentence:

> On motion under Rule 37(a) or Rule 26©), or on its own motion, the court shall-if appropriate to implement the limitations of rule 26(b)(i)(iii)-limit the discovery or require the party seeking discovery to pay part or all of the reasonable expenses incurred by the responding part. [181 F.R.D. 18, 88- 89].

2. The intent of the Advisory Committee was to make "explicit the court's authority to condition document production on payment by the party seeking discovery of part or all of the reasonable costs of that document production if the request exceeds the limitations of Rule 26(b)(2)(i), or (iii). This authority was implicit in the 1983 adoption of Rule 26(b)(2) ***." 181 F.R.D. 18, 89-91 (1999).

3. The Judicial Conference did not approve the amendment. However, the power to shift costs remains implicit in Rules 26(b)(2) and 26©). See Manual, §11.433; 8 Wright, Miller & Marcus, Federal Practice and Procedure, §2008.1 at 27-28 (2004 pocket part).

For a decision which allowed a requesting party to have direct access to an adversary's database, see In re Honeywell Int'l, Inc., 2003 U.S. Dist. LEXIS 20602 (S.D.N.Y. Nov. 18) (allowing access to nonparty's audit work papers on findings that hard copies were not kept in normal course of business, "namely in electronic form," and that nonparty did not provide "adequate means to decipher how the documents are kept"). Honeywell and Ford Motor Co. are discussed in D. Gonsowski & D. Weber, "Unfettered Database Access in Discovery: Inherent Right on Sanction of Non-Compliance," Vol. 4, No. 4, Digital Discovery and e-Evidence 12 (Apr. 2004). See, for another decision which denied direct access to a database, Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc., 2003 WL 1809465,*2 (N.D. Ill. April 4)

Courts have now recognized that, when the "normal course of business" is for entities to maintain records in digital format, what is important for discovery purposes is not whether the records are indexed but whether the records are (or can be made) readable and searchable. Zakre v. Norddeutsche Landesbank Giorzentrale, 2004 WL 764895 (S.D.N.Y. Apr. 9); In re Lorazepam & Clorazepate Antitrust Litigation, supra, 300 F. Supp. 2d 43, 47 (D.D.C. 2004).

For an example of a successful (?) search, see Wiginton v. CB Richard Ellis, Inc., 2004 U.S. Dist. LEXIS 15722, *4-9 (N.D. Ill. Aug. 10).

VI. COST-BEARING: THREE APPROACHES

A. McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001) (Magistrate Judge John M. Facciola).

1. Background of case and discovery dispute:

> Plaintiff's complaint identifies two forms of retaliation. He first complains that, despite the confidentiality of the settlement agreement, his claims *** were known by the people with whom he worked and that he suffered humiliation and retaliation at their hands. He then complains that, after hiring counsel in July 1988 to pursue formal legal remedies beginning with EEO counseling, he suffered renewed retaliation efforts. ***.
>
> In responding to plaintiff's discovery, defendants have searched for electronic and paper documents. Since defendants have already searched for electronic records, they do not quarrel with their obligation to do so. During discovery, the producing party has an obligation to search available electronic systems for the information demanded. * * * Plaintiff, however, wants more. He wants to force DOJ to search its backup systems since they might yield, for example, data that was ultimately deleted by the user but was stored on the backup tape and remains there today.
>
> Defendants protest that the remote possibility that such a search will yield relevant evidence cannot possibly justify the costs involved. [202 F.R.D. at 32].

2. Judge Facciola's analysis of cost-bearing:

> There is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic and provide little guidance. The one judicial rationale that has emerged is that producing backup tapes is a cost of doing business in the computer age. ***. But, that assumes an alternative. It is impossible to walk ten feet into the office of a private business or government agency without seeing a network computer, which is on a server, which, in turn, is being backed up on tape (or some other media) on a daily, weekly or monthly basis. What alternative is there? Quill pens?

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Furthermore, making the producing party pay for all costs of restoration as a cost of its 'choice' to use computers creates a disincentive for the requesting party to demand anything less than all of the tapes. American lawyers engaged in discovery have never been accused of asking for too little. To the contrary, like the Rolling Stones, they hope that if they ask for what they want, they will get what the need. They hardly need any more encouragement to demand as much as they can from their opponent.

The converse solution is to make the party seeking the restoration of the backup tapes pay for them, so that the requesting party literally gets what it pays for. Those who favor a 'market' economic approach to the law would argue that charging the requesting party would guarantee that the requesting party would only demand what it needs. Under that rationale, shifting the cost of production solves the problem. ***.

But there are two problems with that analysis. First, a strict cost-based approach ignores the fact that a government agency is not a profit-producing entity and it cannot be said that paying costs in this case would yield the same 'profit' that other foregone economic activity would yield . ***. While the notion that government agencies and businesses will not have backup systems if they are forced to restore them whenever they are sued may seem fanciful, courts should not lead them into temptation.

Second, if it is reasonably certain that the backup tapes contain information that is relevant to a claim or defense, shifting all costs to the requesting party means that the requesting party will have to pay for the agency to search the backup tapes even though the requesting party would not have to pay for such a search of a 'paper' depository.

A fairer approach borrows, by analogy, from the economic principle of 'marginal utility'. The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the government agency search at its own expense. The less likely it is, the more unjust it would be to make the agency search at its own expense. The difference is 'at the margin.'

Finally, economic considerations have to be pertinent if the court is to remain faithful to its responsibility to prevent "undue burden or expense'. Fed. R. Civ. P. 26©). If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail. That is an awfully expensive needle to justify searching a haystack. It must be recalled that ordering the producing party to restore backup tapes upon a showing of likelihood that they will contain relevant information in every case gives the plaintiff a gigantic club with which to beat his opponent into settlement. No corporate president in her right mind would fail to settle a lawsuit for $100,000 if the restoration of backup tapes would cost $300,000. While that 38 scenario might warm the cockles of certain lawyers's hearts, no one would accuse it of being just.

Given the complicated questions presented, the clash of policies and the lack of precedential guidance, I have decided to take small steps and perform, as it were, a test run. Accordingly, I will order DOJ to perform a backup restoration of the e-mails attributable to *** [an individual's] computer during the period of July 1, 1988 to July 1, 1999. I have chosen this period because a letter from plaintiff's counsel to

DOJ, complaining of retaliation and threatening to file an administrative claim, is dated July 2, 1998, and it seems to me a convenient and rational starting point to search for evidence of retaliation. I have chosen email because of its universal use and because I am hoping that the restoration will yield both the e-mails *** [the individual] sent and those he received. The DOJ will have to carefully document the time and money spent in doing the search. It will then have to search in the restored e-mails for any document responsive to any of plaintiff's requests for production of documents. Upon the completion of this search, the DOJ will then file a comprehensive, sworn certification of the time and money spent and the results of the search. Once it does, I will permit the parties an opportunity to argue why the results and the expense do or do not justify any further search. [202 F.R.D. at 33-35 (citations omitted)[21]].

---

[21]What is quoted from here is "McPeek I." In "McPeek II," reported at 212 F.R.D. 33 20 D.D.C. 2003), the parties returned to Judge Facciola after the "test run" had been completed. Not surprisingly, '[t]he search having been done, the parties could not disagree more completely as to what the search revealed." 212 F.R.D. at 34.

During the test run, the defendant learned that only certain backup tapes were available. Rather than allow the plaintiff to search all the tapes, Judge Facciola relied on the principle that, "[t]he likelihood of finding relevant data has to be a function of the application of the common sense principle that people generate data referring to an event, whether e-mail or word

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

B. Rowe Entertainment, Inc. v. William 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) (Magistrate Judge James C. Francis).

1. Background of case and discovery dispute:

> Too often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter. As this case illustrates, discovery expenses frequently escalate when information is stored in electronic form.
>
> The plaintiffs are black concert promoters who contend that they have been frozen out of the market for promoting events with white bands by the discriminatory and anti-competitive practices of the defendants. [205 F.R.D. at 423].
>
> ***
>
> The plaintiffs' document demands are sweeping. For example, they demand production of all documents concerning any communication between any defendants relating to the selection of concert promoters and bids to promote concerts. *** Similarly, the plaintiffs have requested '[a]ll documents concerning the selection of concert promoters, and the solicitation, and bidding processes relating to concert promotions.' *** They have also demanded '[a]ll documents concerning market shares, market share values, market conditions, or geographic boundaries in which any ... concert promoter operates.' These are but three examples of the thirty-five requests made in the plaintiffs' first document demand.
>
> ***
>
> Each of the moving defendants contends that it should be relieved of the obligation of producing e-mail responsive to the plaintiffs' requests because the burden and expense involved would far outweigh any possible benefit in terms of discovery of additional information. If production is nevertheless required, the defendants ask that the plaintiffs bear the cost. ***. [205 F.R.D. at 424].

2. Was the information sought discoverable?

> The plaintiffs have successfully demonstrated that the discovery they seek is generally relevant. Although the defendants vigorously contest the plaintiffs' interpretation of the documents that have already been produced *** those documents are plainly pertinent to the plaintiffs' claims. To the extent that the defendants' e-mails contain similar information, they are equally discoverable. ***.
>
> Nor are the defendants' claims that the e-mail is unlikely to yield relevant information persuasive. General representations *** that *** employees do little business by e-mail are undocumented and are contradicted by data proffered by these same defendants. ***.
>
> Furthermore, the supposition that important e-mails have been printed in hard copy form is likewise unsupported. In general, nearly one-third of all electronically stored data is never printed out. ***. Here, the defendants have not alleged that they had any corporate policy defining which e-mail messages should be reduced to hard copy because they are 'important.' Finally, to the extent that any employee of the defendants was engaged in discriminatory or anti-competitive practices, it is less likely that communications about such activities would be memorialized in an easily accessible form such as a filed paper document.
>
> The defendants' concern about privacy is also unavailing. To the extent that the corporate defendants' own privacy interests are at issue, they are adequately protected by the confidentiality order in this case. To the degree the defendants seek to assert the privacy concerns of their employees, those interests are severely limited. Although personal communications of employees may be [sic] appear in hard copy as well as in electronic documents ***, the defendants made no effort to exclude personal messages from the search of paper records conducted by plaintiffs' counsel. Moreover, an employee who uses his or her employer's computer for personal communications assumes some risk that they will be accessed by the employer or by others.
>
> Thus, there is no justification for a blanket order precluding discovery of the defendants' e-mails on the ground that such discovery is unlikely to provide relevant information or will 41 invade the privacy of non-parties. [205 F.R.D. at 428 (citations omitted)].

3. Judge Francis' analysis of cost-bearing:

---

processing documents, contemporaneous with that event, using the word 'contemporaneous' as a rough guide." Applying that principle, he rejected further searches of all but one backup tape for one specific date. 212 F.R.D. at 35-37.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

The more difficult issue is the extent to which each party should pay the costs of production. 'Under [the discovery] rules, the presumption is that the responding party must bear the expense of complying with discovery requests [.]' ***. Nevertheless, a court may protect the responding party from 'undue burden or expense' by shifting some or all of the costs of production to the requesting party. ***. Here, the expense of locating and extracting responsive e-mails is substantial, even if the more modest estimates of the plaintiffs are credited. Therefore, it is appropriate to determine which, if any, of these costs, are 'undue,' thus justifying allocation of those expenses to the plaintiffs.

***

One line of argument, adopted by the plaintiffs, holds that the responding party should bear the costs of producing electronic data since 'if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk.' ***. But even if this principle is unassailable in the context of paper records, it does not translate well into the realm of electronic data. The underlying assumption is that the party retaining information does so because that information is useful to it, as demonstrated by the fact that it is willing to bear the costs of retention. That party may therefore be expected to locate specific data, whether for its own needs or in response to a discovery request. With electronic media, however, the syllogism breaks down because the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it. And, even if data is retained for limited purposes, it is not necessarily amenable to discovery. ***. Thus, it is not enough to say that because a party retained electronic information, it should necessarily bear the cost of producing it.

The contrary argument is that the requesting party should bear the burden since, when the costs of discovery are internalized, that party can perform a cost-benefit analysis and decide whether the effort is justified. ***. Yet, this 'market' approach has two shortcomings. First, it flies in the face of the well-established legal principle, cited above, that the responding party will pay the expenses of production. Second, it places a price on justice that will not always be acceptable: it would result in the abandonment of meritorious claims by litigants too poor to pay for necessary discovery.

Because of the shortcomings of either bright-line rule, courts have adopted a balancing approach taking into consideration such factors as: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party. Each of these factors is relevant in determining whether discovery costs should be shifted in this case. [205 F.R.D. at 428-29 (citations omitted)].

C. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) (District Judge Shira A. Scheindlin).

1. Background of case and discovery dispute:

> This case provides a textbook example of the difficulty of balancing the competing needs of broad discovery and manageable costs. Laura Zubulake is suing *** for gender discrimination and illegal retaliation. Zubulake's case is certainly not frivolous and if she prevails, her damages may be substantial. She contends that key evidence is located in various e-mails exchanged among UBS employees that now exist only on backup tapes and perhaps other archived media. According to UBS, restoring those e-mails would cost approximately $175,000.00, exclusive of attorney time in reviewing the e-mails. Zubulake now moves for an order compelling UBS to produce those e-mails at its expense.
>
> ***
>
> At issue here is request number twenty-eight, for 'all documents concerning any communication by or between UBS employees concerning Plaintiff.' The term document in Zubulake's request 'includ[es], without limitation, electronic or computerized data compilations.' 'On July 8, 2002, UBS responded by producing approximately 350 pages of documents, including approximately 100 pages of e-mails. UBS also objected to a substantial portion of Zubulake's requests.
>
> ***

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

***. UBS, however, produced no additional e-mails and insisted that its initial production (the 100 pages of e-mails) was complete. As UBS's opposition to the instant motion makes clear–although it remains unsaid–UBS never searched for responsive e-mails on any of its backup tapes. To the contrary, UBS informed Zubulake that the cost of producing e-mails on back-up tapes would be prohibitive (estimated at the time at approximately $300,000.00).

Zubulake, *** objected to UBS's nonproduction. In fact, Zubulake knew that there were additional responsive e-mails that UBS had failed to produce because she herself had produced approximately 450 pages of e-mail correspondence. Clearly, numerous responsive e-mails had been created and deleted at UBS, and Zubulake wanted them. [217 F.R.D. at 311-13 (footnotes omitted)].

2. Was the information sought discoverable?

*** Zubulake is entitled to discovery of the requested e-mails so long as they are relevant to her claims, which they clearly are. As noted, e-mail constituted a substantial means of communication among UBS employees. To that end, UBS has already produced approximately 100 pages of e-mails, the contents of which are unquestionably relevant.

Nonetheless, UBS argues that Zubulake is not entitled to any further discovery because it already produced all responsive documents, to wit, the 100 pages of e-mails. This argument is unpersuasive for two reasons. First, because of the way that UBS backs up its e-mail files, it clearly could not have searched all of its e-mails without restoring the ninety-four backup tapes. (which UBS admits that it has not done). UBS therefore cannot represent that it has produced all responsive e-mails. Second, Zubulake herself has produced over 450 pages of relevant emails, including e-mails that would have been responsive to her discovery requests but were never produced by UBS. These two facts strongly suggest that there are e-mails that Zubulake has not received that reside on UBS's backup media. [217 F.R.D. at317 (footnotes omitted)].

3. "Should Cost-Shifting Be Considered?"[22]

Because it apparently recognizes that Zubulake is entitled to the requested discovery, UBS expends most of its efforts urging the court to shift the cost of production to 'protect [it] ...from undue burden or expense.' Faced with similar applications, courts generally in some sort of cost-shifting analysis, whether
the refined eight-factor Rowe test or a cruder application of Rule 34's proportionality test, or something in between.

The first question, however, is whether cost-shifting must be considered in every case involving the discovery of electronic data, which–in today's world– includes virtually all cases. In light of the accepted principle *** that electronic evidence is no less discoverable than paper evidence, the answer is, 'No.' The Supreme Court has instructed that 'the presumption is that the responding party must bear the expense of complying with discovery requests. ...' Any principled approach to electronic evidence must respect this presumption.

Courts must remember that cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As large companies increasingly move to entirely paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases. This will both undermine the 'strong public policy favor[ing] resolving disputes on their merits,' and may ultimately deter the filing of potentially meritorious claims.

Thus, cost-shifting should be considered only when electronic discovery imposes an'undue burden or expense' on the responding party. The burden or expense of discovery is, in turn, 'undue' when it 'outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.' Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than

[22]As is evident from this quotation, Judge Scheindlin drew a fundamental distinction 21between "accessible" and "inaccessible" electronic data. That distinction is considered in Principles 8 and 9 and the comments thereto of The Sedona Principles.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying. In fact, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that available in a usable format and reasonably indexed. Examples of inaccessible paper documents could include (a) documents in storage in a difficult to reach place; (b) documents converted to microfiche and not easily readable; or ©) documents kept haphazardly, with no indexing system, in quantities that make page-by-page searches impracticable. But in the world of electronic data, thanks to search engines, any data that is retained in a machine readable format is typically accessible. [217 F.R.D. at17-18 (footnotes omitted)].

4. Judge Scheindlin's criticism of Rowe:

In the year since Rowe was decided, its eight factor test has unquestionably become the gold standard for courts resolving electronic discovery disputes. But there is little doubt that Rowe factors will generally favor cost-shifting. Indeed, of the handful of reported opinions that apply Rowe or some modification thereof, all of them have ordered the cost of discovery to be shifted to the requesting party.

In order to maintain the presumption that the responding party pays, the cost-shifting analysis must be neutral; close calls should be resolved in favor of the presumption. The Rowe factors, as applied, undercut that presumption for three reasons. First, the Rowe testis incomplete. Second, courts have given equal weight to all of the factors, when certain factors should predominate. Third, courts applying the Rowe test have not always developed a full factual record [217 F.R.D. at 320 (footnotes omitted)].

***

Certain factors specifically identified in the Rules are omitted from Rowe's eight factors. In particular, Rule 26 requires consideration of 'the amount in controversy, the parties resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.' Yet Rowe makes no mention of either the amount in controversy or the importance of the issues at stake in the litigation. These factors should be added. Doing so would balance the Rowe factor that typically weighs most heavily in favor of cost-shifting, 'the total cost associated with production.' The cost of production is almost always an objectively large number in cases where litigating cost-shifting is worthwhile. But the cost of production when compared to 'the amount in controversy' may tell a different story. A response to a discovery request costing $100,000 sounds (and is)costly, but in a case potentially worth millions of dollars, the cost of responding may not be unduly burdensome.

Rowe also contemplates 'the resources available to each party.' But here too - although this consideration may be implicit in the Rowe test - the absolute wealth of the parties is not the relevant factor. More important than comparing the relative ability of a party to pay for discovery, the focus should be on the total cost of production as compared to the resources available to each party. Thus, discovery that would be too expensive for one defendant to bear would be a drop in the bucket for another.

Last, 'the importance of the issues at stake in the litigation' is a critical consideration, even if it is one that will rarely be invoked. For example, if a case has the potential for broad public impact, then public policy weighs heavily in favor of permitting extensive discovery. Cases of this ilk might include toxic tort class actions, environmental actions, so-called'impact' or social reform litigation, cases involving criminal conduct, or cases implicating important legal or constitutional questions.

* * *

Two of the Rowe factors should be eliminated.

First, the Rowe test includes 'the specificity of the discovery request.' Specificity is surely the touchstone of any good discovery request, requiring a party to frame a request broadly enough to obtain relevant evidence, yet narrowly enough to control costs. But relevance and cost are already two of the Rowe factors (the second and sixth). Because the first and second factors are duplicative, they can be combined. Thus, the first factor should be: the extent to which the request is specifically tailored to discover relevant information.

Second, the fourth factor, 'the purposes for which the responding party maintains there quested data' is typically unimportant. Whether the data is kept for a business purpose or for disaster recovery does not affect its accessibility, which is the practical basis for 47 calculating the cost of production. Although a business purpose will often

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

> coincide with accessibility–data that is inaccessible is unlikely to be used or needed in the ordinary course of business–the concepts are not coterminous. In particular, a good deal of accessible data may be retained, though not in the ordinary course of business. For example, data that should rightly have been erased pursuant to a document retention/destruction policy may be inadvertently retained. If so, the fact that it should have been erased in no way shields that data from discovery. As long as the data is accessible, it must be produced.
>
> Of course, there will be certain limited instances where the very purpose of maintaining the data will be to produce it to the opposing party. That would be the case, for example where the SEC requested 'communications sent by [a] broker or dealer (including inter-office memoranda and communications) relating to his business as such.' Such communications must be maintained ***. But in such cases, cost-shifting would not be applicable in the first place; the relevant statute or rule would dictate the extent of discovery and the associated costs. Cost-shifting would also be inappropriate for another reason–namely, that the regulation itself requires that the data be kept 'in an accessible place.' [217 F.R.D. at 321-22 (footnotes omitted)].

5. Judge Scheindlin's analysis of cost-bearing:

> Set forth below is a new seven-factor test based on the modifications to Rowe discussed in the preceding sections.
>
> 1. The extent to which the request is specifically tailored to discover relevant information;
>
> 2. The availability of such information from other sources;
>
> 3. The total cost of production, compared to the amount in controversy;
>
> 4. The total cost of production, compared to the resources available to each party;
>
> 5. The relative ability of each party to control costs and its incentive to do so;
>
> 6. The importance of the issues at stake in the litigation; and
>
> 7. The relative benefits to the parties of obtaining the information.
>
> * * *
>
> Whenever a court applies a multi-factor test, there is a temptation to treat the factors as a check-list, resolving the issue in favor of whichever column has the most checks. But 'we do not just add up the factors.' When evaluating cost-shifting, the central question mut be, does the request impose an 'undue burden or expense' on the responding party? Put another way, 'how important is the sought-after evidence in comparison to the cost of production?' The seven-factor test articulated above provide some guidance in answering this question, but the test cannot be mechanically applied at the risk of losing sight of its purpose.
>
> Weighting the factors in descending order of importance may solve the problem and avoid a mechanistic application of the test. The first two factors–comprising the marginal utility test–are the most important. ***.
>
> The second group of factors addresses cost issues: 'How expensive will this production be?' and 'Who can handle that expense?' These factors include: (3) the total cost of production compared to the amount in controversy, (4) the total cost of production compared to the resources available to each party and (5) the relative ability of each party to control costs and its incentive to do so. The third 'group'–(6) the importance of the litigation itself–stands alone, and as noted earlier will only rarely come into play. But where it does, this factor has the potential to predominate over the others. Collectively, the first three groups correspond to the three explicit considerations of Rule 26(b)(2)(iii). Finally, the last factor–(7) the relative benefits of production as between the requesting and producing parties–is the least important because it is fair to presume that the response to a discovery request generally benefits the requesting party. But in the unusual case where production will also provide a tangible or strategic benefit to the responding party, that fact may weigh against shifting costs. [217 F.R.D. at 322-24 (footnotes omitted) [23]].

[23] What is quoted here is from "Zubulake I." In "Zubulake II," reported at 2003 U.S. Dist. LEXIS 7940 (S.D.N.Y. May 13), Judge Scheindlin addressed the plaintiff's request to release a sealed transcript. In "Zubulake III," reported at 216 F.R.D. 280 (S.D.N.Y 2003), Judge Scheindlin, again applying her seven-factor test articulated in Zubulake I, assessed 25% of the cost of restoring 77 backup tapes to the plaintiff. 216 F.R.D. at 284-89.

In "Zubulake IV," reported at 2003 U.S. Dist. LEXIS 18771 (S.D.N.Y. Oct. 22), Judge

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

D. Cost-bearing in broader perspective: Thompson v. United States Dept. Of Housing and Urban Dvlpt., 219 F.R.D. 93 (D. Md. 2003) (Magistrate Judge Paul W. Grimm):

> Because of the possible burden and expense associated with broad discovery of electronic records, courts have acknowledged the need to employ the Rule 26(b)(2) cost-benefit balancing factors to determine just how much discovery of electronic records is appropriate in any given case, and which party should bear the cost associated with the production – the requesting party or the producing party. In this regard, it is clear that, ordinarily, the presumption is that the producing party should bear the cost of responding to properly initiated discovery requests. ***.
>
> However, given the minimal threshold requirements of Rule 26(b)(1) for the discoverability of information (a requesting party is entitled to seek discovery of non-privileged information 'relevant' to the claims and defenses raised in the pleadings), and the potentially enormous task of searching for all relevant and unprivileged electronic records, courts have attempted to fashion reasonable limits that will serve the legitimate needs of the requesting party for information, without unfair burden or expense to the producing party. The precise formulas used have varied.
>
> * * *
>
> In addition to the tests fashioned by these courts, [McPeek I and Zubulake I], it also can be argued with some force that the Rule 26(b)(2) balancing factors are all that is needed to allow a court to reach a fair result when considering the scope of discovery of electronic records. Rule 26(b)(2) requires a court, sua sponte, or upon receipt of a Rule 26©) motion, to evaluate the costs and benefits associated with a potentially burdensome discovery request.
>
> ***

Scheindlin addressed the plaintiff's request for sanctions (including an adverse inference instruction) arising out of the defendant's failure to preserve some backup tapes and its deletion of isolated e-mails. In ruling on the request, Judge Scheindlin considered the obligation of a party to preserve digital information.

Finally (?), there is "Zubulake V," 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. July 20), Judge Scheindlin imposed sanctions on the defendant for deleting relevant e-mail.

Regardless of which test is used, the most important ingredient for the analytical process to produce a fair result is a particularization of the facts to support any challenge to discovery of electronic records. Conclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail. ***.

The rationale for this requirement is obvious Under Rules 26(b)(2) and 26©), a court is provided abundant resources to tailor discovery requests to avoid unfair burden or expense and yet assure fair disclosure of important information. The options available are limited only by the court's own imagination and the quality and quantity of the factual information provided by the parties to be used by the court in evaluating the Rule 26(b)(2) factors. The court can, for example, shift the cost, in whole or part, of burdensome and expensive Rule 34 discovery to the requesting party, it can limit the number of hours required by the producing party to search for electronic records; or it can restrict the sources that must be checked. It can delay production of electronic records in response to a Rule 34 request until after the deposition of information and technology personnel of the producing party, who can testify in detail as to the systems in place, as well as to the storage and retention of electronic records, enabling more focused and less costly discovery. A court also can require the parties to identify experts to assist in structuring a search for existing and deleted electronic data and retain such an expert on behalf of the court. But it can be none of these things in a factual vacuum, and *ipse dixit* assertions by counsel that requested discovery of electronic records is overbroad, burdensome or prohibitively expensive provide no help at all to the court.

In this case, the Local Defendants were cautioned by the court that any objection to producing the electronic records sought by the Plaintiffs would have to be particularized. ***. Despite this warning, Local Defendants failed to provide affidavits, deposition excerpts or similarly detailed information in opposition to the Plaintiffs' motions to obtain discovery of electronic records and subsequent motion for sanctions. ***. Such a failure to provide this information prevented the court from having available the information needed to analyze the Rule 26(b)(2) cost-benefit factors, and, predictably, resulted in rulings that the Plaintiffs' motions were meritorious. [219 F.R.D. at 98-99

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

(citations omitted)[24]].

E. A Postscript on "Factors."

Rowe and Zubulake introduced multi-factor tests to aid in shifting costs. Will new tests appear? As one commentator has stated: "There are no new factors. Only new formulations." In this regard, see Wiginton v. CB Richard Ellis, Inc., 2004 U.S. Dist. LEXIS 15722, *13 (N.D. Ill. Aug. 10), which modified Zubulake "by adding a factor that considers the importance of the requested discovery in resolving the issues of the litigation."

[24]Consistent with Judge Grimm's recognition of the options available under Rule 23 26(b)(2), The Sedona Principles state in Comment 13.b: "Shifting the costs of extraordinary efforts to preserve or produce information should not be used as an alternative to sustaining a responding party's objection to undertaking such efforts in the first place. Instead, such efforts should only be required where the requesting party demonstrates substantial need or justification."

ABA Standard 29(b)(iii) sets forth a number of factors that a court might consider "[i]n resolving a motion seeking to compel or protect against the production of electronic information or related software."

VII. AVOIDING PROBLEMS: SOME SUGGESTIONS

A. What the Manual suggests judges and attorneys can do:

> The judge should encourage the parties to discuss the scope of proposed computer-based discovery early in the case, particularly any discovery of data beyond that available to the responding parties in the ordinary course of business. The requesting parties should identify he information they require as narrowly and precisely as possible, and the responding parties should be forthcoming and explicit in identifying what data are available from what sources, to allow formulation of a realistic computer-based discovery plan. Rule 26(b)(2)(iii) allows the court to limit or modify the extent of otherwise allowable discovery if the burdens outweigh the likely benefit–the rule should be used to discourage costly, speculative, duplicative, or unduly burdensome discovery of computer data and systems. Additionally, some computerized data may have been compiled in anticipation of or for use in the litigation and may therefore be entitled to protection as trial preparation materials.
>
> * * *
>
> Evolving procedures use document-management technologies to minimize cost and exposure and, with time, parties and technology will likely continue to become more and more sophisticated. The judge should encourage the parties to discuss the issues of production forms early in litigation, preferably prior to any production, to avoid the waste and duplication of producing the same data in different formats. The relatively inexpensive production of computer-readable images may suffice for the vast majority of requested data. Dynamic data may need to be produced in native format, or in a modified format in which the integrity of the data can be maintained while the data can be manipulated for analysis. If raw data are produced, appropriate applications, file structures, manuals, and other tools necessary for the proper translation and use of the data must be provided. Files (such as Email) for which metadata is essential to the understanding of the primary data should be identified and produced in an appropriate format. There may even be rare instances in which paper printouts (hard copy) are appropriate. No one form of production will be appropriate for all types of data in all cases.
>
> Consider how to minimize and allocate the costs of production. Narrowing the overall scope of electronic discovery is the most

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

effective method of reducing costs. Early agreement between the parties regarding the forms of production will help eliminate waste and duplication. More expensive forms of production, such as production of word processing files with all associated metadata or production of data in a specified nonstandard format, should be conditioned upon a showing of need or sharing of expenses. [Manual, §11.446 (footnote omitted)].

B. What the Manual says can be done to save time and expense:

Phased or sequenced discovery of computerized data. Sections 11.41 and 11.422 have discussed phasing discovery by issue. Computerized data, however, are often not accessible by date, author, addressee, or subject matter without costly review and indexing. Therefore, it may be appropriate for the court to phase or sequence discovery of computerized data by accessibility. At the outset, allowing discovery of relevant, nonprivileged data available to the respondent in the routine course of business is appropriate and should be treated as a conventional document request. I f the requesting party requests more computerized data, consider additional sources in ascending order of cost and burden to the responding party, e.g., metadata or system data, archived data, backup data, and legacy data. The judge should encourage the parties to agree to phased discovery of computerized data as part of the discovery plan. But with or without a prior agreement, the judge may engage in benefit-and-burden analysis under Rule 26(b)(2)(iii) at each stage and enter an appropriate order under Rule 26©), which may include cost sharing between the parties or cost shifting to the requesting party * * *.

Computerized data produced in agreed-on-formats. Information subject to discovery increasingly exists in digital or computer-readable form. The judge should encourage counsel to produce requested data in formats and on media that reduce transport and conversion costs, maximize the ability of all parties to organize and analyze the data during pretrial preparation, and assure usability at trial. Wholesale conversion of computerized data to paper form for production, only to be reconverted into computerized data by the receiving party, is costly and wasteful. Particularly in multiparty cases, data production on CD-ROM or by Internet-based data transfer can increase efficiency. Section 11.444 discusses 'virtual' document depositories.

Sampling of computer data. Parties may have vast collections of computerized data, such as stored E-mail messages or backup files containing routine business information kept for disaster recovery purposes. Unlike collections of paper documents, these data are not normally organized for retrieval by date, author, addressee, or subject matter, and may be very costly and time-consuming to investigate thoroughly. Under such circumstances, judges have ordered that random samples of data storage media be restored and analyzed to determine if further discovery is warranted under the benefit versus burden considerations of Rule 26(b)(2)(iii). [Manual, §11.423 (footnotes omitted)].

C. What a district court should not do:

In this case, Ford [the defendant] and Russel [the plaintiff] dispute whether Ford properly responded to Russell's earlier requests for production. Although Russell asserts that Ford has not been forthright in providing documents, Ford contends that it has produced all relevant information. The district court was in the best position to determine whether Ford had improperly dealt with the earlier discovery requests. But the district court made no findings–express or implied–that Ford had failed to comply properly with discovery requests.

The district court also did not discuss its view of Ford's objections and provided no substantive explanation for the court's ruling. Ford objected to the search on the grounds that (1) Russell had established no discovery abuses by Ford, (2) Ford had already searched the database and produced all relevant, non-privileged materials, and (3) the discovery rules did not allow the court to grant Russell free access to the databases regardless of relevance, privilege, or confidentiality. When a party objects to a motion for discovery, a court should rule on the objections and ordinarily give at least some statement of its reasons. ***.

Furthermore, in its order, the district court granted Russell unlimited, direct access to Ford's databases. The district court established no protocols for the search. The court did not even designate search terms to restrict the search. Without constraints, the order grants Russell access to information that would not–and should not–otherwise be discoverable without Ford first having had an opportunity to object.

While some kind of direct access might be permissible in certain cases, this case has not been shown to be one of those cases. Russell is unentitled to this kind of discovery without–at the outset–a factual

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

finding of some non-compliance with discovery rules by Ford. By granting the sweeping order in this case, especially without such a finding, the district court clearly abused its discretion." [In re: Ford Motor Co., supra, 345 F. 3d at 1317].

D. In Metropolitan Opera Ass'n v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003), egregious misconduct in discovery by the defendant union local led to the entry of judgment as to liability against it as well as other sanctions.[25] Here are some suggestions about what the defendant attorneys could have done to avoid the sanctions:

> The Metropolitan Opera decision does set out what the union should have done, at a minimum, to properly discharge its discovery obligations. Essentially, the court avers that the union had a duty to 'establish a coherent and effective system to faithfully and effectively respond to discovery requests.' According to the court's discussion, elements of that plan should have included:
>
> . a reasonable procedure to distribute discovery requests to all employees and agents of the defendant potentially possessing responsive information, and to account for the collection and subsequent production of the information to plaintiffs;
>
> . a method for explaining to their client what types of information would be relevant and responsive to discovery requests;
>
> . an inquiry into the client's document retention or filing systems, and implementation of a systematic procedure for document production or for retention of documents, including electronic documents; and
>
> . proper supervision of all elements of discovery that were to be carried out by non-legal personnel." V. Llewellyn, "The Court's Prescription," Vol. 3, No. 3, Digital Discovery & e-Evidence 4 (March, 2003)[26]].

E. Use of digital information at trial.[27]

1. What the Manual says:

> In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The

[25]For another example of an award of sanctions against a party for failure to produce digital information, see Residential Funding v. DeGeorge Financial Corp., 306 F.3d 99 (2d Cir. 2002), In Residential Funding, there were two distinct "events" by the sanctioned party: failure to
maintain e-mail in an accessible format and "purposeful sluggishness" in complying with an order to produce the e-mail. Although the latter led to a sanction, the court of appeals stated in dicta that ordinary negligence as a result of which a party breached its obligation to produce e-mail was sanctionable. Residential Funding was followed in MasterCard Internat'l, Inc. v. Moulton, 2004 U.S. Dist. LEXIS 11376 (S.D.N.Y. 2004). In MasterCard, the defendants were sanctioned for "at least gross negligence" in failing to preserve e-mail.

In Theofel v. Farey-Jones, 341 F.3d 978 (9 Cir. 2003), the court held that, by serving th pursuant to Rule 45 a "massively overbroad" and "patently unlawful" subpoena on an internet service provider, which responded to the subpoena by posting e-mail on its own site, a party in a civil action and his attorney could be sued for violation of federal electronic privacy and computer fraud statutes.

Readers interested in Theofel might also be interested in decisions which consider the civil liability of employers which search or seize employee laptops or e-mail. For such readers, see Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) and Muick v. Glenayre Electronics, 280 F.3d 741 (7 Cir. 2002).

[26]Metropolitan Opera and means to avoid its harsh "lesson" are discussed in two articles by Virginia Llewellyn that both begin on page 1 of this issue of Digital Discovery and e-Evidence. See also the comments of the district judge who decided Metropolitan Opera reported in "Conference Report: Jurists Offer Perspective, Tips on E-discovery," Vol 3, No. 10, Digital Discovery & e-Evidence 3 (Oct. 2003).

[27]This section is included to remind attorneys that admissibility issues should be considered during discovery. See Manual, §11.445. For example, if a nonparty produces digital information in response to a subpoena, what will the requesting party need to ensure that the information will be admissible?

ABA Standard 29(b)(iv) encourages attorneys to stipulate "to the authenticity and identifying characteristics (date, author, etc.) of electronic information that is not self-authenticating on its face."

For a detailed discussion of admissibility of computer-enhanced and computer-generated evidence, see State v. Swinton, 268 Conn. 781 (Sup. Ct. 2004).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.

The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings so that challenges to the evidence are not made for the first time at trial. When the data are voluminous, verification and correction of all items may not be feasible. In such cases, verification may be made of a sample of the data. Instead of correcting the errors detected in the sample–which might lead to the erroneous representation that the compilation is free from error–evidence may be offered (or stipulations made), by way of extrapolation from the sample, of the effect of the observed errors on the entire compilation. Alternatively, it may be feasible to use statistical methods to determine the probability and range of error. [Manual. §11.446 (footnote omitted)].

2. Something to consider: admissibility of a facsimile transmission:

The [District] Court was correct that ordinarily a fax's sender would authenticate the document by testifying to such foundational facts as that the fax machine automatically date–stamps transmissions, that it was in proper working order, that she did not tamper with it, etc. ***. In this case Khorozian [the defendant] exercised her Fifth Amendment right against self-incrimination and thus did not take the stand. However, Kono [a witness] could–and did– authenticate the fax under Federal Rule of Evidence 901(a) by testifying that she received the fax on the date indicated on the header. Authentication does not conclusively establish the genuineness of an item; it is a foundation that a jury may reject.

Moreover, neither the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 901(a), a statement is something uttered by 'a person,' so nothing 'said' by a machine . . . is hearsay.' ***. The fax contents were not hearsay because Khorozian sought to introduce the fax for the fact that it contained the name Teixiera (and was sent on May 15), not for its truth. The fax is relevant, regardless of its truth, to rebut the Government's contention that she and Queirolo fabricated the document after May 25 as part of a scheme to defraud the bank. [United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) (citations omitted)[28]].

[28]Admissibility of electronic evidence over authenticity and hearsay objections is addressed in, for example, United States v. Tank, 200 F.3d 627, 630-31 (9 Cir. 2000), United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11 Cir. 2000) and Kearley v. State, 843 So. 2d 66, 70 (Miss. Ct. App. 2002), cert. denied, 2003 Miss. LEXIS 76 (Miss. Sup. Ct. Feb. 12, 2003). Admissibility of electronic evidence is also discussed in Chapter 8 of Arkfeld's Electronic Discovery and Evidence.

For a broad discussion of computer-generated evidence, see K. Magyar, "Computer Generated Demonstrative Evidence," For the Defense 35 (Jan. 2004).

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

VIII. CONCLUSION[29]

A. Learn about the relevant technology. "[C]ounsel must be cognizant of not only electronic discovery but also the details so that they can communicate effectively with clients, vendors, other counsel, and the courts." J. Redgrave & E. Bachmann, "Ripples on the Shores of Zubulake," The Federal Lawyer 31 (Nov./Dec. 2003).

B. Learn about the client's information systems. Work with clients to avoid spoliation.[30]

C. Make early-and specific-requests for discovery of digital information. "Discovery requests should make as clear as possible what electronic documents and data are being asked for, while response and objections should disclose the scope and limits of what is being produced." The Sedona Principles, Principle 4.

D. Use data sampling: "In a growing e-evidence trend, courts are looking to data sampling protocols-searching a small number of hard drives, servers, backup tapes, etc.- to see if relevant evidence exists * * *." W. Furnish & M. Lange, "Lessons Learned: Rowe, Murphy Oil, Zubulake and Beyond," Vol. 3, No. 12, Digital Discovery & e-Evidence 3 (Dec. 2003). "Statistical sampling is a common technique used to determine a pattern of conduct." Farmers Ins. Co. v. Peterson, 81 P.3d 659, 661 (Okla. Sup. Ct . 2003).[31]

E. The case law on discovery disputes is fact-specific. Make the most complete record

F. The pervasiveness of electronic information leads to issues for lawyers to consider far beyond those related to discovery and admissibility. For example, may an attorney dispense with paper files in favor of computerized records? See Maine Board of Bar Overseers Professional Ethics Commission, Op. No. 183 (Jan. 28, 2004). What should an attorney do to protect the confidentiality of e-mail with a client? See American Bar Association Formal Op. No. 99-413 (Mar. 10, 1999).

[29]These conclusions are drawn in part from the articles cited.

[30]Regrettably, "there is a lot out there on spoliation." In addition to the decisions cited in this outline, see Rambus, Inc. v. Infineon Technologies AG, 220 F.R.D. 264, 280-88 (E.D. Va. 2004) (addressing spoliation in context of crime/fraud exception to attorney-client privilege).

[31]See with regard to backup tapes, A. Prosad & W. Hubbard, "Sampling of Backup Tapes," For the Defense 37 (June 2004).

THE SEDONA CONFERENCE® WORKING GROUP SERIES

wgs℠

BEST PRACTICES FOR THE SELECTION OF ELECTRONIC DISCOVERY VENDORS:

Navigating the Vendor Proposal Process

A Project of The Sedona Conference®
Working Group on Best Practices for Electronic Document Retention & Production (WG1)
RFP+ Group

JULY 2005 VERSION

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

NAVIGATING THE VENDOR PROPOSAL PROCESS

Executive Editor: Richard G. Braman, Esq.

Authors: Matthew I. Cohen, Esq., Skadden Arps
Conor R. Crowley, Esq., Labaton Sucharow
Sherry B. Harris, Hunton & Williams
Anne E. Kershaw, Esq., A. Kershaw, P.C.
Mark V. Reichenbach, Milberg Weiss

With Input from the RFP+ Vendor Panel (See Appendix F)*

Republication or Redistribution is not permitted except upon the express prior permission of The Second Conference®. Requests for reprints or further information should be directed to the Executive Director of The Sedona Conference at tsc@sedona.net or 1-866-860-6600.

*This document is for educational purposes only and is not a substitute for legal advice. The opinions expressed herein are consensus views of the Editor and Authors, and do not necessarily represent the views of any of the individual participants or authors or any of the organizations to which they belong or clients they represent.

Copyright© 2005
The Sedona Conference®

Visit www.thesedonaconference.org

Table of Contents

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Preface

Overview

Welcome to the next publication in The Sedona Conference® Working Group Series (WGS[SM]), Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process (July, 2005 Version). This effort is an outgrowth of our Working Group on Electronic Document Retention and Production (WG1), and represents the work of its RFP+ Group: 5 "users" of electronic discovery vendor services (2 from defense firms, 2 from plaintiff firms, and 1 consultant/attorney) with input from time to time provided by the RFP+ Vendor Panel, a group of over 30 electronic discovery vendors who signed up as members to support this effort in response to an open invitation and whose membership fees have financially supported the efforts of the Group (See Appendix F for a listing of the RFP+ Vendor Panel as of April 1, 2005; see www.thesedonaconference.org for a current listing of the RFP+ Vendor Panel).

The goal of the RFP+ Group and this paper is to outline an approach to the selection of an electronic discovery vendor that allows the "user" to compare apples to apples, to the extent feasible, and which makes it easier for all parties to the process to better understand the nature, cost and impact of what is being discussed. In the belief that an informed market will lead to reduced transaction costs, more predictable outcomes, and better business relationships, the RFP+ Group was formally launched on July 1, 2004, and this paper is its first work product, along with its companion, The Sedona Glossary.

The Sedona Conference® is primarily known for its efforts as a law and policy think-tank and premium conference provider in the areas of antitrust, complex litigation and intellectual property rights, and our Working Groups are focused on these areas. Though the RFP+ project may seem more nuts and bolts than our others, it is one that we believe can be of benefit to all participants in the process, and that may contribute to one of the overall goals of our Working Group on Electronic Document Retention and Production — the prevention of the tail wagging the dog when it comes to discovery of electronic information in complex litigation. We hope our efforts have the intended effect. Please send all feedback to us at tsc@sedona.net.

wgs™

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

IMPORTANT CAVEAT RE: USAGE OF THESE GUIDELINES

This paper, a guide through the RFP process in the selection of an electronic discovery vendor, must be placed in context to be used properly. There are three levels at which context is relevant: (1) information management; (2) business relationships with information management and electronic discovery vendors; and (3) the creation of a specific RFI and RFP for the selection of a vendor for a single piece (or related pieces) of litigation. Finally, as with all such matters, ultimately good judgment must be the final arbiter.

(1) Information Management

Business today operates in an information-based economy, and the identification, selection, review, storage and retrieval of information critical to any particular enterprise is now getting Board-level attention (or, at least, should be) simply to ensure that the business does not lose, or lose control of, any of its valuable information assets. The less attention an organization pays to effectively managing its information assets, the bigger the headache of electronic discovery in any particular litigation.

(2) Business Relationships With Vendors

There are obvious transaction costs to either selecting or changing vendors. There are some who advocate going through the RFP (if not both the RFI and RFP) process in every litigation. There are others who espouse the benefits of long-term vendor or vendor-team relationships. As we emphasize, the selection choice is one based on the exercise of sound business judgment; this paper should prove a useful starting point regardless of the business model chosen for the vendor relationship, and is not intended to be read as endorsing either approach.[1]

[1] The current literature on supply chain management and the approach to quality through continuous improvement, as exemplified by TQM, CMM, Six Sigma or other standardized process improvement methodology, for example, suggests selecting very few supplier partners and working with them to improve process. *See* Zero Base Pricing (1990) and Out of the Crisis (1982). As noted in the text, above, this paper advocates neither approach in general - it is a business decision.

wgs™

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

(3) Creation of Specific RFI or RFP

This paper is meant to ensure that all pertinent factors are considered in the creation of any specific RFI or RFP. The sample, tailored RFI (Appendix C-2) and RFP (Appendix C-3) based on a hypothetical case pattern (Appendix C-1) are meant to show how the long-list of considerations can be tailored to a specific case, as not all considerations are necessarily pertinent to each case, or vary in degree of importance depending on the litigation (see Decision Matrix, Appendix E). Hence, the sample RFI and RFP appendices are not meant to simply be copied and used, nor are the long lists of questions simply to be converted into a broad-form RFI and RFP. Similarly, the inclusion of a decision matrix is not meant to imply that the choice is mechanical. As mentioned throughout, going through all the considerations mentioned in this paper, including the Decision Matrix, are the foundation for an informed business judgment, not a substitute for it.

With that by way of prelude, I hope you find the following helpful in the event you find yourself in situations involving the need to select an electronic discovery, or information search and retrieval, vendor. As with all of our efforts, feedback and input from any interested party is encouraged.

Special thanks go to our "user group" for all their hard work on this project: Matt Cohen (Skadden Arps); Conor Crowley (Much Shelist); Sherry Harris (Hunton & Williams); Anne Kershaw (A. Kershaw, PC//Attorneys & Consultants); and Mark Reichenbach (Milberg Weiss).[2]

Richard G. Braman
Executive Director
June, 2005
Sedona, AZ

[2] The WG1 RFP+ "User" Group also wishes to acknowledge the contributing efforts of Shelley Podolny, A. Kershaw, PC//Attorneys & Consultants.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

I. Introduction

The purpose of this paper is to provide guidance to law firm and law department attorneys and litigation support professionals who must face the increasingly daunting challenge of finding the appropriate electronic discovery vendor. The proliferation of these vendors is not surprising in light of an increased demand for such a broad range of services—from collection, processing, review and production of electronic documents to strategic consulting in the creation of a discovery plan or even high-stakes forensics. Electronic discovery, like most aspects of litigation, is not susceptible to a cookie-cutter approach.

Determining the scope of the electronic discovery project must precede the vendor search, although we trust that the vendor evaluation process described in this paper will assist users in framing not only the process for selecting vendors, but also the process for defining the parameters of the electronic discovery process itself. The evaluation process starts with a request for information — RFI — which is designed to identify vendors with the capabilities for the prospective project, a request for proposal — RFP — which is designed to elicit proposals tailored to a specific project, and finally a decision matrix which is designed to help weigh and compare proposals and vendor capabilities. Samples of a tailored RFI and RFP are attached as appendices. It is critical to note, however, that these attachments are only samples and that any RFI or RFP to be submitted to vendors ***must*** be tailored to the specifics of the case if it is to be useful in selecting a vendor. Indeed, the greater the degree of detail as to the case and its requirements, the easier the process will be.

As Comment 6.d. of ***The Sedona Principles for Electronic Document Production*** notes, "[c]onsiderations in evaluating vendor software and services include the defensibility of the process in the litigation context, the cost and experience of the vendor." Each of these issues must be evaluated thoroughly, and later weighed against each other in selecting a vendor that is appropriate for the individual project. The process outlined herein is scalable. It is designed to assist solo practitioners in relatively small cases as well as practitioners or litigation support professionals at large law firms selecting vendors to assist with the preservation, harvesting, processing and production of terabytes of data. The nature of the case will necessarily drive the scope of the electronic discovery to be conducted, which may well dictate the selection of the vendor, or perhaps a consultant specializing in vendor research and processes. Large projects or

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

in-house counsel seeking across-the-board solutions may be well served by input from an experienced consultant, whose knowledge can streamline and expedite the process, providing the extra arms and legs needed to get the project done.

Electronic discovery vendors, like law firms and corporations, run the gamut in terms of size and capabilities—from self-employed individuals who specialize in one particular area, such as computer forensics, to subsidiaries of publicly traded corporations that handle every aspect of the electronic discovery process.

Also included in this paper is a discussion concerning the processing of traditional paper-based documents in the evaluation process because it is inevitable that the discovery of paper-based documents will continue to be an important part of the discovery process for some time, and because it is important that paper and electronic documents be treated in an integrated manner. Recognizing that paper documents will be around for a while, many vendors are incorporating features to support the review and production of paper-based documents into their electronic document review tools.

The challenge of choosing among competing vendors in the electronic discovery arena is exacerbated by the lack of standards and uniform processes across the industry. In fact, many vendors consider their processes and methodologies to be proprietary and jealously guard them. The lack of transparency in these proprietary processes can make the "defense of process" prong of our analysis more difficult than it would otherwise be. However, because the party (whether plaintiff or defendant) will ultimately be responsible for the production of relevant information, it is critical that the process employed in the collection, processing and production of e-data be understood and defensible.

II. Square One: Knowing What Before Who

The number of vendors in the electronic discovery business has ballooned in recent years, and there are now hundreds of companies offering electronic discovery services in one form or another. Many have come to the world of electronic discovery by way of expanding existing services, such as software vendors, litigation support providers, document management experts, or forensic specialists. As a result, these potential suppliers have different strengths (and

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

weaknesses) relevant to the project at hand. Electronic discovery issues can span the spectrum from anticipated production of two million documents to recovering data from a recycled laptop to needing a vendor that can provide consulting services for a broad discovery plan, or an expert to testify that back-up tapes from 1985 are too old to read.

These are a few among the many electronic discovery issues, but an initial search for vendors, either for a specific case or as part of an ongoing litigation support effort, should not necessarily lead to the same short list every time. From among all of those who may be able to help with electronic discovery and evidentiary needs, the goal is to find the best fit —a vendor suited to both the organization and the particular project. The process of paring down the universe of possible vendors and comparing their services can be daunting, especially if there is no systematic way to request, compare and evaluate the information necessary to select the finalists. Enter the *Request for Proposal (RFP)* and its precursor, a *Request for Information (RFI).*[3]

III. Finding Out What to Find Out

The most important thing to know about an RFI or RFP is that the requesting party [4] bears a large part of the information burden. By nature, electronic information requires some kind of technology to be processed, complicating the life of the person who just wants to know what a document *says*. New technologies in electronic discovery can make life challenging for the person or group who may not understand the technology requirements for a particular project or know what solutions might be available to solve a problem. Nonetheless, it is squarely on the shoulders of the requesting party to take on the due diligence of defining the scope of a project, collecting and prioritizing requirements, and understanding and communicating the IT landscape to a potential supplier so that there will ultimately be the best possible match of problem and solution. This "pre-RFP" process, while demanding, is well worth the effort. Done properly, and where appropriate, it brings together business, legal and IT assets, helps establish objectives and clarify requirements (including budget and timeline), defines the parameters for success, and

[3] A sample RFP and RFI tailored to a hypothetical fact pattern are attached as Appendices C-1 through C-3.

[4] The one seeking a vendor.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

suggests the direction a vendor search should take. Plus, it serves to enlighten the participants, who may be direct stakeholders in the end result.[5]

Because the requesting party will ultimately need to evaluate the responses to the RFP, this up-front work, which ideally has fully prescribed the scope of the project, will inform and expedite the evaluation process. A well-structured RFP provides a framework by which vendors can work from the same set of rules and requirements to craft their proposals, enabling a comparison of apples to apples, thus making it easier to understand the similarities and differences among proposed solutions. The Companion Sedona Glossary (see www.thesedonaconference.org/publications), to which the RFP+ Vendor Panel Members have agreed, is meant to assist in the effectiveness of communication and to improve the ability to conduct an apples-to-apples comparison.

IV. Where to Look: Getting to the Short List with an RFI

Once a project or need has been identified, there are several ways to become generally educated and to begin collecting information about potential vendors who may be able to assist with a product or service. One such way is to request technical literature, case studies and mission statements from vendors who advertise in trade publications. Attending seminars and conferences, product demonstrations and trade shows or surfing the Internet can be very helpful, as can speaking with procurement and IT departments within the business or with other industry insiders. There are also independent consultants who offer services in this area. These methods go a long way towards refining the list of possible suppliers as well as helping to create a more productive RFI.

Once familiar with the range of needs and the basic vendor landscape, the next step is the RFI. An RFI, which is similar in form to an RFP, gives potential suppliers an opportunity to provide information about their own products and services (including suggestions to help refine requirements and helpful insight with respect to the specific request, such as in the description of the project or feasibility of the task.) Perhaps there is no available technology that can

[5] This process may also parallel what one would follow were one to tackle information management separate from any litigation need.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

accomplish, in a cost-effective way, the product or service as requested. Perhaps there are new technologies that will suggest re-evaluation of original requirements. Unlike an RFP, which implies a project green light, an RFI is primarily a fact-finding document. At this point in the process, the doors should be thrown open for any information that may be useful in narrowing the list of vendors and providing information that will assist in a clear definition of the project requirements for the RFP. It often helps if a dialogue is initiated with potential vendors about the nature and scope of the project so that they can provide "active" feedback. (This should be undertaken only after an appropriate confidentiality agreement is in effect, and attention is paid to conflicts considerations. See § V.C., *infra.*)

The next section of this document sets forth the considerations that should help with the development of a meaningful RFI.

V. What to Look For

A. First Things First: Vendor Background

As with any business entity being considered for a project, a responsibility exists to investigate the reputation and integrity of the firm in question and ensure that they offer the kinds of services required. (More on this later.) Presumably, those selected to respond to an RFI and/or RFP have been vetted for the basics prior to their inclusion in the list of possible responders. (See § IV above.) Seek and evaluate basic vendor background information about the company, the personnel, and the product or service that they are offering.

About the Company

Any potential vendor should be stable and known to provide a reasonable quality of service. These are not, on the whole, subjective qualities; it should not be difficult to determine a company's reputation. Nonetheless, it pays to ask for details and evidence. When was the company founded and by whom? Have they been around long enough for your needs? Do they have a track record providing the product or service required? How big are they, both in dollar

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

volume and personnel? Does size matter?[6] A small-dollar vendor with the right expertise and/or product and a good track record may be better than a large one with more dispersed business resources bringing in dollars. Also know that many electronic discovery vendors which were scanning and coding operations yesterday claim to be experts in electronic discovery today; as with the selection of any expert, one must get behind the representations. Ask for client references, and use them (NDA's may prohibit disclosure of some references). Take a look at prior testimony and court opinions involving the vendor where available. Remember, it is possible the vendor may need to provide testimony regarding the transparency of the process. As with law firms, remember also that retention involves retaining a specific person or team as well, not just the "company". (See "About the Personnel" below).

Find out about obligations, representations and warranties to ensure that the vendor is qualified to do what they say they do, aren't doing the same job for an adversary, can guarantee confidentiality and the appropriate safeguards for information, and are reputable in pricing and bidding practices.

The physical location(s) of the vendor may or may not be an issue, depending upon the type of service they provide, but safety and security are, especially for electronic data involved in litigation where chain of custody issues are a concern. Can the data be handled without altering metadata? Does the physical plant of the vendor provide the appropriate disaster recovery ability? Is there a fully-enabled back-up site? If the vendor is providing a website, is it sufficiently secure, safe from viruses and hackers? Asking the vendor to describe in detail existing security capabilities in the RFP will allow assessment of which vendors most closely conform to the requirements. These are issues that each vendor should be asked to address in an RFP before being considered for a project.

[6] There is no intention to imply that start-ups not be considered, just that when dealing with a company that is not a start-up, the length of time the company has been in business is a valid consideration, and if dealing with a start-up, it should be knowingly. Similarly, if the vendor is privately held, certain types of information may be considered proprietary and not made available.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

About the Personnel

General background information about a company is one thing, but a background check should include, more specifically, information about the people who work there and those who may work on the project at hand. What is the experience level of the personnel? Do they employ and use lawyers? Have personnel been appropriately screened for security? In some cases, a criminal record and background check for all vendor employees may be necessary. Are they located in the United States or overseas? Do they have the collective expertise to handle and are they available for the project at hand? Sometimes a vendor's success results in a work overload that may impact delivery of the project. Will the vendor need to hire new, possibly inexperienced or temporary staff to handle the work? Will they need to sub-contract any part of the work? It is important to understand the current capacity and workload of the vendor, as well as personnel turnover. To the extent possible, satisfied and content personnel should be working on any project.

If your case is going to require testimony on the part of the electronic discovery vendor, it is best to determine if the vendor has had that type of experience. What has been the outcome? Are there copies of the testimony or expert affidavits that can be shared?

It is also important to know the project management approach (process) of a vendor. Although this may vary depending upon the type of product or service, project tracking and client communication are always an important part of the mix on both sides. A dedicated project manager, or at the very least, a single liaison or point of contact should be available to manage and troubleshoot, so that conflicting messages do not exacerbate existing problems and lead to deadline, or worse, quality problems.

About the Product or Service

Notwithstanding the quality of the company and personnel, the vendor must also have the goods to provide and support the product or service they sell. Again, client references can shed valuable light on vendor product/service performance. In addition, ask for the names and experience levels of the personnel who may be assigned to the project at the appropriate time (may not be known until job has been scoped and scheduled). Assuming the vendor's product or

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

service can live up to their claims, how good are they at providing the appropriate level of quality assurance? What is their method of providing information to their client? What technical support is available, at what times, and by what methods? Do software or systems need to be upgraded on a regular basis? Do the technologies they use have unanticipated dependencies that must be otherwise supplied, such as network, operating systems, capacity, or compatibility issues?

Up-front work in preparation of the RFI should detail as many technical concerns as possible to give the vendor the opportunity to anticipate potential glitches. Remember that the RFI is a two-way street—the request is just as important as the response. The more explicit and detailed the description of the project, the better the chance the vendor has to recognize and realistically address potential limitations.[7] Mapping out the expected processes and work flow, and subsequently tracking changes is recommended, particularly in the event testimony is needed down line (it's always good to be able to demonstrate how hard you worked to do it right . . .). Most vendors also welcome the establishment of a communications protocol, with scheduled progress reports, together with a protocol for reporting and resolving unexpected changes, delays, or other problems.

In addition to the basic information described above, electronic discovery projects pose additional areas of concern. It is important to request information to ensure understanding of the following about the potential vendor:

- *Maintenance of Document Integrity*: An important evidentiary consideration. The vendor should describe what is done to ensure that a document has not been changed during processing, and further, that the "processed" document can later be compared to the original item received by the vendor. Again, a detailed description of the process can help track chain of custody and ensure preservation of content. The vendor should confirm as part of that process that a complete, exact copy of the data is securely stored, in case something does go wrong.

[7] Tables in Appendix A summarize the information to consider requesting from each vendor, tailored and weighted according to the project at hand. See Sample RFI (Appendix C-2), and the sample Decision Matrix (Appendix E).

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

- *Amenability to Escrow*: For any large, long term project, it is important to escrow any software code, together with instruction manuals and other documentation, to guard against problems in the event the vendor becomes financially unstable or is purchased by another entity with whom there may be a conflict of interest.

- *Expert Testimony Experience*: In electronic discovery cases, the vendor may need to be a participant in the litigation. It is advisable to ensure that the vendor has a spokesperson with appropriate expertise and who is comfortable on the witness stand to attest to the integrity and transparency of all processes and quality control. It may also be desirable to shield this potential testifier from attorney-client privileged or work-product protected information throughout the process.

- *Sub-Contracting*: It is very important that the vendor disclose all sub-contracting relationships that may be involved in getting the work done, and that a process be established for disclosure and approval of any sub-contracting, with all sub-contractors named as additional insureds in any required insurance policy. In addition, the vendor should be prepared to certify that all sub-contractors are free of conflicts.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

VENDOR BACKGROUND

A List of Considerations Regarding Potential Vendors

VENDOR BACKGROUND

ABOUT THE COMPANY		
Area of Concern		***What to Ask About***
Company Stability	*Where the vendor has been in business for more than one year, they should have proven experience providing the required services.*	▪ **Company Age.** Information regarding the establishment of the company, as well as any mergers or consolidations. ▪ **Financials.** Taxpayer identification and financial statements for the last two years, as well as bank references. Also consider requesting information regarding any pending lawsuits against the company. These items may not necessarily be made available at the initial stages of the process and/or from privately held companies depending on the parties and the situation. Bank references and client references are also helpful if financials are not available. ▪ **Company History and Performance Information.** A description of the vendor's background and expertise in the areas covered by the RFI, including years of experience, past cases and performance.
Company Quality	*The vendor should be able to provide information that will show a proven track record of successful projects and satisfied customers.*	▪ **Client References.** Names of clients for whom the vendor has performed services similar to those required. (When requesting references, ask for a general description of the scope of the project and the value achieved by the company, as well as timelines of deliveries.) ▪ **Past Performance Information.** Follow-up to ensure that clients were satisfied with the outcome of the project, project management, deadlines, fee arrangements, quality control and perceived integrity.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

VENDOR BACKGROUND

ABOUT THE COMPANY		
Area of Concern		***What to Ask About***
Company Obligations, Representations and Warranties	*The vendor should have sound business practices for their own and their clients' protection, and be willing to adhere to liability and confidentially standards.*	▪ **Proof in writing of the existence of:** - Insurance and licenses - Any potential privilege and/or conflicts issues - Confidentiality guarantees - Pricing methods - Non-collusive bidding assurances
Physical Plants	*The vendor should have secure and safe premises for conducting business and safeguarding any information and/or electronic data that may be provided by their clients.*	▪ **Physical plant/office locations.** Address and contact information for all plant/office locations, domestic and international for the vendor's company, as well as any affiliated businesses or organizations ▪ **Safety** Information pertaining to building or site disaster safeguards (fire, flood, etc.), especially if the vendor will be hosting data ▪ **Security** Information pertaining to building and data access, employee screening, security methods (ID cards, etc.), hacker/virus protection.
ABOUT THE PERSONNEL		
Area of Concern		***What to Ask About***
Quality of Personnel	*The vendor should employ an appropriately educated and dedicated staff.*	▪ **Rate of employee turnover** Information regarding length of time on the job for those involved in the potential project ▪ **Client References**. As with information regarding company quality, ascertain the level of satisfaction with personnel from other vendor clients, including ease of communication, turnaround times, quality of work, etc.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

VENDOR BACKGROUND

ABOUT THE PERSONNEL		
Area of Concern		***What to Ask About***
Experience	*Staff should have experience commensurate with their responsibility.*	▪ **Past Performance** Success that employees have had at completing the kind of tasks required for the particular product or service required. ▪ **Testimony** Prior experience in giving testimony related to product or service
Staffing Capacity	*The vendor should advise in advance if any subcontracting or temporary staff will be utilized on the project.*	▪ **Employee Data.** Information regarding the location and number of employees, staffing and composition anticipated for the project, and their technical expertise and years of experience.
Project Management	*The vendor should have experienced management to oversee, troubleshoot and communicate information about the job.*	▪ **Project Oversight** Who will manage the project, product or service, and by what method and how frequently will the information be tracked and reported?
ABOUT THE PRODUCT/SERVICE		
Area of Concern		***What to Ask About***
Quality of Work	*The vendor should have standard practices to validate and measure the quality of products, services, processes and procedures.*	▪ **Quality Assurance Procedures** Request documentation of steps taken to validate and verify the products/services the vendor provides. ▪ **Client references** As with information regarding company and employee quality, ascertain the level of satisfaction with the products/services from other vendor clients, including ease of use, stability, problem-solving, technical support, documentation, and the like. ▪ **Reporting Methods** Ascertain the methods the vendor uses to provide information to clients during the lifecycle of a project.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

VENDOR BACKGROUND

ABOUT THE PRODUCT/SERVICE		
Area of Concern		***What to Ask About***
Process and Infrastructure	*The vendor should have demonstrable safety measures in effect, as well as the appropriate infrastructure to meet demands of the project.*	▪ **Maintenance and Support** Information regarding maintenance and support of the product /service, such as type, quality and availability of technical support, procedural updates, product maintenance, upgrades, etc. ▪ **Disaster Recovery** Information regarding disaster recovery plans and facilities during the lifecycle of the project. (If implementation has not yet occurred, is the entire project lost in the event of a fire?) ▪ **Security** Request a description of procedures for screening employees and maintaining security on the premises, such as requiring badges for entry.

B. Is it Safe? Vendor Security

Engaging a vendor to process data or engage in any kind of service related to electronic discovery requires the same attention to security risk that would apply to the company seeking the service. There is every reason to want and expect the potential vendor to have security safeguards in place to protect all involved client's assets, both in terms of physical safety and confidentiality. In addition, the vendor must be willing to guarantee agreed-upon courses of action should their company face financial hardship, gain a new conflicting client, be acquired by another company, or have their programming guru seek an island respite. Security issues should be considered for the company, the data, and the project itself.

Company Security

Site security for the vendor and any third party entity they might employ is crucial. A site visit to "kick the tires" is not a bad idea (at lest at the RFP stage), and may provide a glimpse into the culture of the organization as well. The company should have obvious security measures in place such as access restriction to network hardware, telecommunications security, as well as disaster recovery plans, back-up servers, and appropriate insurance.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Personnel security is just as important. What kind of security checks do they use to ensure the reliability of their own employees? Background checks? Conflict checks? Are the employees bonded? What procedures are in place when an employee leaves the company? Can they work for your client's adversary?

Data Security

Hardware and software security have practically generated their own industry, and with good reason. Electronic information is recognized as a valuable business asset today as never before, and endangered data can be life threatening to a business or the outcome of litigation. While it may be a reasonable assumption that vendors have the appropriate safeguards in place, the questions must still be asked. What are their back-up and disaster recovery procedures? Are their software systems sufficiently protected from intruders, hackers, and viruses? Are users screened and validated? How does data get from place to place, and is it encrypted before it goes anywhere? Do they keep their protections up-to-date? Deficiencies in this area are not worth the risk.

Project Security

If the vendor passes muster on company and data security measures, there is still the project to consider. What happens when the project is over (and what determines the end-date)? What happens to electronic and hardcopy data, work-product, etc.? What happens if the vendor has not met their obligation—is there an articulated method to handle disputes? One thing to keep in mind is that the dynamic electronic landscape is driving business mergers and acquisitions, not to mention failures. What happens if the vendor is acquired or files for bankruptcy? Will your client's data be involved in the mess? If homework is done regarding company stability, it is possible to head such a problem off at the pass, but ensure that safeguards are in place in case of such business surprises.

Also specify what should be done with electronic and hard copy data at the conclusion of the relationship, such as returning all original paper and media or shredding all copies, and certifying compliance with these procedures at the conclusion of the project.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

C. Conflicts

The consideration of an electronic discovery vendor – or any other litigation support vendor for that matter – in connection with either pending or threatened litigation or an administrative proceeding, should always start with a conflicts check as the first step. While there may be situations in which a vendor is retained to perform ministerial or quasi-ministerial type services (equivalent to photocopying) there are others in which the vendor will be privy to confidential information about the client's information management systems and policies as well as their litigation strategy. It is therefore imperative to ensure that there are no conflicts or potential conflicts at the outset. It is also imperative that a conflicts check be performed by any entity that will be acting as a sub-contractor to the vendor, and that any potential conflict be addressed.

In situations where an RFP will be issued, considerations regarding potential conflicts should always precede the issuance of the RFP. Responding to an RFP is a time-consuming and expensive process for vendors, and in appropriate cases no conflicts check is required to ensure that there are no conflicts which would preclude the vendor's retention to provide the services described in the RFP. In order to facilitate this process, we recommend that a non-disclosure agreement be executed prior to disclosing to prospective vendors the name of the client and the nature of the case or proceeding for which vendor retention is sought. A sample non-disclosure agreement is contained in Appendix B.

What constitutes a conflict? Lawyers are constrained from taking on the representation of a party who is adverse to their other clients, and electronic discovery vendors, as well as all litigation support vendors, should follow the same conflicts rules that lawyers follow. While it is understood that adhering to the conflict rules followed by lawyers may result in vendors having to turn down certain engagements, this may be a cost of doing business that is necessary in order to protect parties during litigation and proceedings. Moreover, because parties may waive a conflict, vendors may be able to undertake engagements in situations where a party grants them a conflicts waiver. Clients, lawyers and vendors should engage in an open and frank discussion concerning conflicts, and, where appropriate, parties should consider the waiver of conflicts and allow vendors that are providing, or that have provided services to also provide services to adverse parties in situations where there will be no prejudice suffered as a result of having waived the conflict.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

The fact that no two electronic discovery projects are the same complicates the conflict analysis, and makes it that much more difficult to draw bright lines. Every potential conflict must be examined in light of the circumstances of the case at issue. There may be situations where past, existing or prospective clients are not concerned about a potential conflict because the nature of the services rendered or to be rendered was or is such that there is no concern about the potential disclosure of information that could prejudice its position.

It is recommend that any services agreement to be ultimately executed by the parties contain a clause memorializing the parties' agreement concerning conflicts. This is especially important in light of the fact that vendors are not bound to the rules of ethics that preclude lawyers from representing parties who are adverse to their other clients. The following sample provision strikes a good balance between protecting clients and maintaining a vendor's ability to undertake engagements. It is recommended that a provision offering the protections afforded by this sample language be included in every services agreement.

Sample Conflicts Provision for Engagement Agreement

Vendor represents that it has conducted a conflict check prior to undertaking this engagement and that it has informed Client of every engagement in which it is currently involved [or has been involved over the course of the preceding __ years] where the party to whom the Vendor is providing, or to whom it did provide services, is adverse to Client. A third-party shall be deemed to be "adverse" to Client if the third-party has any interest or involvement in any lawsuit or proceeding in which Client (or any subsidiary or affiliate) is a named party.

Vendor agrees that it will perform conflicts checks prior to undertaking services for new clients and that it will:

1. Not provide services to any third-party that is adverse to Client in a matter in which Vendor has provided, or is providing services to Client.

2. Not provide services to any third-party that it knows is adverse to Client on a matter in which it is not providing services to Client, without first obtaining written consent from Client. Client agrees that it will not unreasonably withhold consent for Vendor to provide services to third-parties under this provision provided that granting such consent will not adversely impact Client in any pending or future litigation or proceeding; and

3. Promptly inform Client if it learns that any third-party to whom it is providing services is adverse to Client.

Vendor agrees that it will follow the conflicts policy outlined above after the termination of the Engagement, pursuant to paragraph __, for a period of __ years.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

VENDOR SECURITY

COMPANY SECURITY		
Area of Concern		***What to Ask About***
Physical Site Security	*The vendor should demonstrate provision of appropriate physical and data security procedures.*	The vendor's physical site should be as secure as the client's. Ask about: ▪ Building safety and security (e.g., access, back-up, disaster recovery) ▪ Telecom (types and locations) ▪ Third Party Outsourcing
Employees	*The vendor should be accountable for the quality and reliability of all employees or subcontractors under their auspices.*	Who works for the vendor, and how are they screened? Ask for information about: ▪ Employee exit process ▪ Turnover ▪ Conflicts ▪ Background ▪ Drug Testing ▪ Bonding
DATA SECURITY		
Hardware Security	*The vendor should be able and willing to commit to prescribed procedures in the event of disruption or termination of the project.*	Description of what happens if the vendor cannot finish the job or has an unforeseen disruption of business. Ask about: ▪ Mirror Site ▪ Server lock-downs ▪ Access Restrictions ▪ Insurance

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

DATA SECURITY		
Area of Concern		***What to Ask About***
Software Security	*The vendor should demonstrate provision of appropriate physical and data security procedures.*	Information related to: ▪ Building safety and security ▪ Telecom ▪ Third Party Outsourcing ▪ Ability to guarantee data integrity ▪ Mirror Site ▪ Secure Delivery of Data
PROJECT SECURITY		
Rights on Termination	*The vendor should be able and willing to commit to prescribed procedures in the event of disruption or termination of the project.*	Description of what happens if the vendor cannot finish the job or has an unforeseen disruption of business. Clarify the vendor's position on: ▪ Rights to data ▪ Contract disputes ▪ Business failure/acquisition
Conflicts	*The vendor should investigate and fully disclose any potential conflicts with parties related to the client's business or litigation.*	Information related to: ▪ Procedures for checking for conflicts ▪ Agreements not to work with opposing parties ▪ Protocol if vendor acquired by another company

VI. What's for Sale: Electronic Discovery Services

Section V, above, mainly addresses concerns that could be considered due diligence when contracting with any outside entity. Now the crux of the matter: assuming that the problem has been defined, the requirements collected, and the scope understood, what is the nature of the task and what kind of vendor is best suited for the job?

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

For purposes of this paper, the electronic discovery tasks that may be at issue can be described as generally falling into these five categories:

1) Consulting/Professional Services

2) Data Collection/Processing

3) Data Recovery/Forensics

4) Hosting/Review/Production/Delivery

5) Other Litigation Support-Related Services

The services that electronic discovery vendors offer become more robust every day as greater demands and innovation lead to new technologies. Generally speaking, there are three principal types of electronic discovery vendors available to address the tasks above, each of which requires certain expertise, hardware, software, and/or processing abilities. In light of increasing industry consolidation one vendor may provide one or more of these three categories of services, in combination or otherwise:

1) *Vendors that process data*, whose activities are primarily volume-driven
Examples: Data collection, hosting, storage, review, litigation support services

2) *Vendors that that provide software solutions* and are thus driven by their intellectual property
Examples: Case management tool providers, document management and/or review, search/categorization/retrieval tools

3) *Vendors that consult*, with expertise in one or more specific areas
Examples: Forensics, Data Recovery, Discovery Strategy, Risk Management

Vendor firms may provide solutions for any aspect of data collection, processing, hosting and production and although they may provide a combination of services (which is happening more and more), they often play to one strength. This is an important factor to keep in mind when evaluating potential vendor offerings.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

The following table describes the most common electronic discovery services currently offered:

Service Category	Type of Services Provided	Things to Consider
Consulting / Professional Services	▪ Testimony ▪ Analysis o Assessment of IT Infrastructure o Assessment of preservation issues o Recommendations for discovery plan	▪ Forensics 30(b)(6) ▪ *Daubert* challenge ▪ Past experience/outcome
Data Collection /Processing	▪ Data/File Management ▪ Data Harvesting ▪ Data Filtering ▪ Email Processing ▪ Review services or software ▪ Redaction services	▪ File types processed, especially for email ▪ Preserving metadata ▪ Types of tools used ▪ Keyword/phrase taxonomy ▪ Search methods (context, concept, fuzzy, etc.) ▪ Custody ▪ Foreign language capability ▪ Document relationships ▪ De-dupe capabilities ▪ Email string processing ▪ RFC822 standards

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Service Category	Type of Services Provided	Things to Consider
Data Recovery/Forensics	▪ Legacy Data Restoration ▪ Backup systems/enterprise backup ▪ Reverse engineering ▪ Corrupted/deleted/hidden/ encrypted /temp data ▪ Damaged media ▪ Password protected files ▪ Mirror hard drives	▪ Experience ▪ Attest to methodology, procedure, fact regarding treatment and location of electronic information ▪ Avoiding alteration of source data ▪ May be called to testify
Hosting/Production/ Review/Delivery	▪ Data/ website hosting ▪ Review/Support ▪ Production	▪ Web capability ▪ Accessibility, FTP Site ▪ Export capabilities ▪ Capacity limitations ▪ CD/DVD or other storage media ▪ Data verification, MD5 or other hash coding ▪ Native format documents ▪ Image processing ▪ Training ▪ Online review capability ▪ Production media types (CD/Web, etc.) ▪ Make available capability ▪ Production number application tracking ▪ Reporting capabilities ▪ Custody ▪ Foreign capabilities

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

Service Category	Type of Services Provided	Things to Consider
Other Litigation Support-Related Services	▪ Scanning/Copying/OCR ▪ Coding (objective/subjective) ▪ Conceptual organization	▪ Facility ▪ Methodology ▪ Capacity ▪ Format ▪ Integration capability ▪ Export capability ▪ Quality assurance procedures ▪ Auto-coding vs. human coding ▪ On-shore vs. off-shore ▪ Accuracy statistics ▪ Coder expertise ▪ Quality assurance procedures

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

VII. Making the Cut: How to Select Vendors to be Included in the RFP

Review of the vendor responses to an RFI or other investigation should lead to identification of a smaller group of vendors from which a request for project proposals through the RFP process will be made. The number of vendors selected for the RFP process may vary greatly from project to project, but generally speaking, those selected to respond to an RFP should all be viable contenders. Keep in mind that this is a time-consuming process for the vendor, and it is unethical and unfair to request a proposal from a company that is not truly in the running, not to mention the undue consumption of time in reviewing responses that are not really needed. The use of a decision matrix or other scoring tool to evaluate vendor responses is useful in arriving at a final list for submission of the RFP.

VIII. Crafting the RFP

An RFP is not a form for a vendor to "fill in the blanks." Not all projects are the same and the RFP must be tailored to specific needs if meaningful responses are expected and if a vendor is to be specific in responding to needs. Perhaps the biggest area of concern is assuming that a vendor's knowledge of the project needs may be complete – such assumptions have been proven wrong in the past, and it helps tremendously to engage potential vendors in a dialogue to make they are aware of all considerations. There are, of course, certain sections that are amenable to boilerplate language, such as confidentiality, rights of the parties and representations and warranties, and a sample "tailored" RFP containing those sections is included in Appendix C. Such information requests generally remain consistent from project to project, but as with everything, should still be reviewed each time to make sure they are appropriate to the matter at hand.

The RFP sections that must be customized for a project include the following:

A. Project Overview (Scope of Work): As discussed, a thorough description of the project may be the most important element of a RFP, and this description, together with the requirements list, should be discussed with all project team members to insure as complete a description as is reasonably practicable. Indeed, this is where the problem is defined, specifying the number and type of information sources, the systems on which they reside, timelines, scope of relevancy, and any applicable court orders. Also specify the services required and the expected format for review and production. (A list of vendor services is set forth in Appendix A). This is an appropriate time to develop internal checklists regarding electronic discovery needs, etc.

B. Management: Describe the roles of client, counsel, and staff in the management of the work contemplated. Also spell out the expected lines of communication, measurements of success, and procedures for status reporting.

C. Requirements Description: In this section, describe for the vendor, to the extent known or reasonably anticipated, the technical requirements, specific services needed, the time constraints, the volume, the required output, and the required service and quality levels. If review software is involved, also inquire regarding any training requirements. It is important to specify the goals and objectives of the project, as well as priorities. Ask for "what" is needed, and allow the vendor to describe "how" they will meet those needs.

D. Definitions: *The Sedona Glossary*, published as an integral companion piece to this document, defines terms frequently used in connection with electronic discovery matters. Including in the RFP all definitions that may apply to avoid misunderstandings down line is recommended. RFP+ Vendor Panel members have agreed to work within the framework of this *Glossary*.

E. Vendor Process and Infrastructure: Here the vendor is asked to describe, in detail, assumptions, processes and infrastructure for getting the project done. Seek their internal reporting structure, and their process for "change control," i.e., how surprises are handled. Remember, litigation often involves "surprises" as the norm.

F. Quality Assurance: Following up on the RFI question and responses regarding quality assurance, this inquiry seeks to determine if the vendor will institute any additional quality assurance procedures in light of the nature of the project.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

G. Processing Methods: Questions here are driven, of course, by the nature of the services requested. In the sample "tailored" RFP (Appendix C-3) a list of suggested questions is supplied for the various services offered in connection with a specific fact pattern. Note that any intention on the part of any vendor to sub-contract should be fully disclosed and understood.

H. Vendor Recommendations: The electronic discovery arena is very dynamic, with technological capabilities changing daily. Asking for the vendor's recommendations will give the vendor an opportunity to educate as to new service offerings that may provide a better solution for the project, or guide away from outdated assumptions that may be embedded in services requests. As mentioned in "C" above, ask for "what" is needed, and allow the vendor to explain "how" they may meet those needs.

I. Pricing Alternatives: Specify the pricing model(s) preferred, so that meaningful comparisons of the vendor pricing responses can be made. For example, if a project is scanning and objective coding, possibly specify a 'per page' or 'per document' price from the vendors. If seeking an on-line (ASP) document hosting and review service for a very large population, consider requesting pricing 'per gigabyte' (GB). Appendix D lists various pricing models for various services. Be sure to ask the vendors to list all possible charges, so there are no surprises. If the vendor is using some form of "conversion" to respond in the pricing model requested, the "conversion" should be transparent, and understood.

J. Vendor Qualifications and References: Be sure to check trade references, carefully read the vendor's web site, and then follow-up with questions as to various representations made therein. It is also important to speak with references provided by the vendor. While some of the vendor's clients may have insisted on confidentiality, be certain to speak with those familiar with the vendor's ability to perform just as one would any service provider.

K. Follow-up Processes: Set forth a procedure for handling questions that arise during the RFP process, allowing each RFP participant to weigh in.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

L. Post-RFP Briefings: It is a good practice to explain to those vendors that did not get the job, the reason for the selection made. This preserves good-will for the next project, and helps improve the process overall by educating the competition.

IX. Making the Selection: Evaluating RFP Responses — the Decision Matrix

As with analyzing responses to a tailored RFI, the beginning point for analyzing and comparing vendor RFP responses is through the use of a scoring sheet or decision matrix (Appendix E). To complete this process, each item in the RFP (hardware security, software security, etc.) is assigned a level of importance (to the project) and then each vendor response is given a 'grade' or number assessing the sufficiency of the response. The vendors are ranked by multiplying the importance level and the response grade, and then adding the results. (See Appendix E). Of course, a decision matrix cannot, and should not, replace the exercise of common sense and good judgment but will hopefully inform the exercise of that judgment, usually made in conjunction with the client.

X. Trends

A. Certification Programs: Along with the development of the electronic discovery market, various electronic discovery "certification" programs are springing up. There is no process yet in place, however, for "certifying" the certification programs, and purchasers should be wary of relying on such programs for comprehensive knowledge. In addition, many of these certification programs are generally limited to a specific company or technology set. These are new and rapidly developing areas of the law and technology, with knowledge thresholds changing daily. Accordingly, whether or not the vendors being evaluated have such a program should have no bearing on selection. While independent certification courses offering true objective measures of certification will become available in the future (The Sedona Conference® RFP+ Group, itself, may begin a move in that direction), at this point it is important to make independent assessments of vendors and the technologies and services offered.

B. Artificial Intelligence: Technology is developing that will allow for electronic relevancy assessments and subject matter, or issue coding. These technologies have the potential to dramatically change the way electronic discovery is handled in litigation, and could save litigants millions of dollars in document review costs. Hand-in-hand with electronic relevancy

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

assessment and issue coding, it is anticipated that advanced searching and retrieval technologies may allow for targeted collections and productions, thus reducing the volume of information involved in the discovery process.

C. Online Repositories: Already in use in large, complex cases, on-line repositories have great potential for smaller cases insofar as they allow for all litigants to work off the same database of information from any computer. Down the line, this would allow for uniform, paperless identification of deposition and trial exhibits, with links to transcripts, all of which could also be available to the court on-line. For large productions, on-line repositories allow for electronic "make-available" productions, in which all potentially responsive documents are produced under an agreement protecting against privilege and confidentiality waiver. The receiving party then selects or tags the documents in which they are interested, and which documents the producing party then reviews for privilege and confidentiality. In essence, this type of procedure cuts down on cost and time expenditures considerably by applying the privilege and confidentiality review to only those documents that the receiving party actually wants. There is, of course, substantial debate about the wisdom and efficacy of such "clawback" agreements, and this document should not be read as an endorsement of the procedure.

D. Mixed Media: While we currently think of "Mixed Media" as various types of non-searchable data now residing in the in-box of an email system, it is interesting to note that Microsoft recently released their XP Multimedia Operating System for home entertainment. Though not a ground-breaking announcement, this quiet release to the home entertainment market and others similar to this could have a very real effect on the future concept of where one should look for relevant data stores.

This release coupled with the currently available hardware (computers, TVs, phones, etc), the increased penetration of digital TV, digital phones and broadband cable Internet access into individual's homes may produce the following scenario. Executives sitting on their couch, checking their email on a 42" flat panel screen connected to a cable box that is really a computer. This executive will be reviewing faxes that have come to his inbox (business and personal), looking at video email sent to his inbox and

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

responding to all with ease. These communications and any attachments could possibly contain relevant information yet may or may not be fully searchable.

While there are 50 million or more homes in America that have the basic three or four necessary components (i.e. telephone, computer, cable box/TV, playstation/Xbox), someday there will be only one component and that one component will handle the job of all of these and provide additional features in the works or yet to be dreamed up. The software, game, cable and consumer electronic industries are all actively working on such a device, all with a slant toward their particular industry. It will handle email, voice mail, faxes, documents, videos purchased, Websites visited, online purchases made, video recorded from TV, music listened to, games played, home movies and photo albums, to name only what is currently known. To paraphrase Oracle's CEO, "Privacy? What privacy?" Definitely an issue to be addressed.

E. Enterprise Records Management: It has become increasing clear that, for large electronic data producers, the most effective way to handle preservation, collection and production of electronic media begins with management of that media as it is created and stored. Accordingly, "Knowledge Management," "Records Management," and '"Retention Policies" are likely to become the linchpins of defensible preservation and collections protocols, with the execution and criteria for those protocols built into software designed for the enterprise's overall records and/or knowledge management. As this trend develops, it will become necessary to add elements to your RFI and RFP questions that will identify whether or not the vendor's services will integrate with the enterprise's records management system.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Appendices

A. Summary Charts

Electronic Discovery RFP+ Overview
Introduction
Vendor Background
Security
Electronic Discovery Vendor Services
Conflicts
Trends

B. Sample Non-Disclosure Agreement

C. Sample Tailored RFI and RFP (with fact pattern)

D. Pricing Models

E. Decision Matrix

F. RFP+ Vendor Panel List

G. RFP+ User Group

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

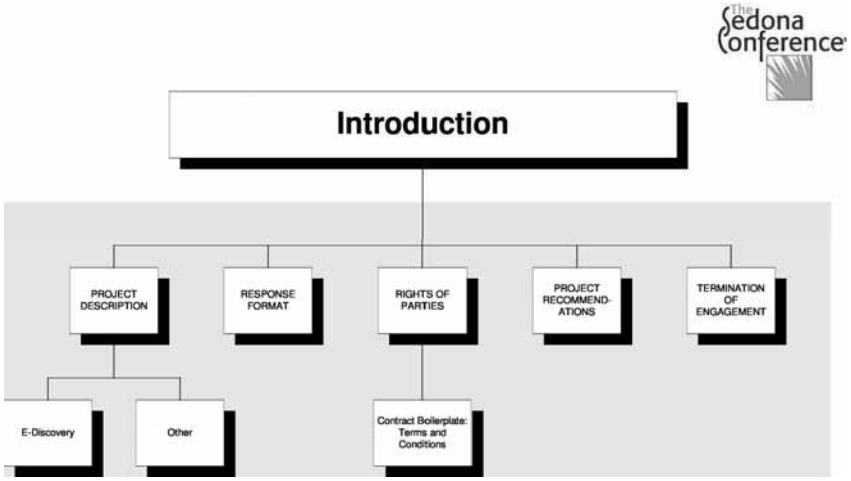
Appendix A

RFP+ Group

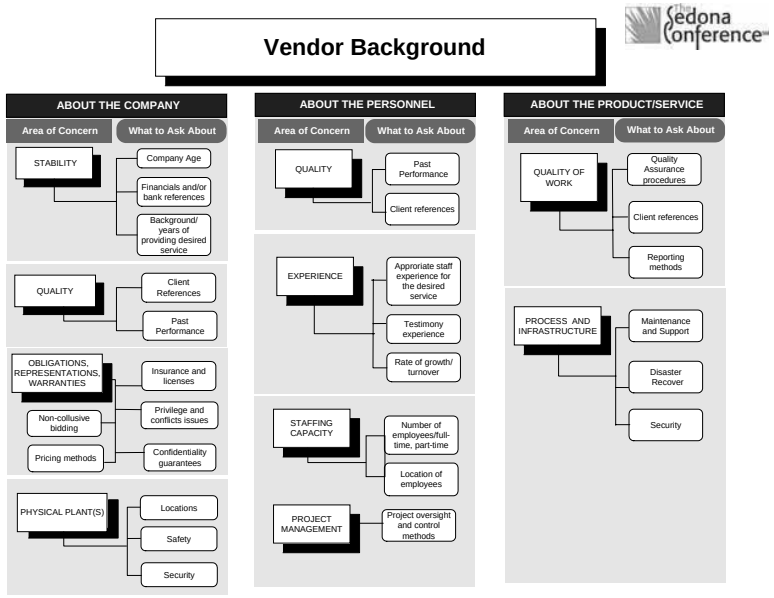
Selection of an Electronic Discovery Vendor
Summary Charts

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

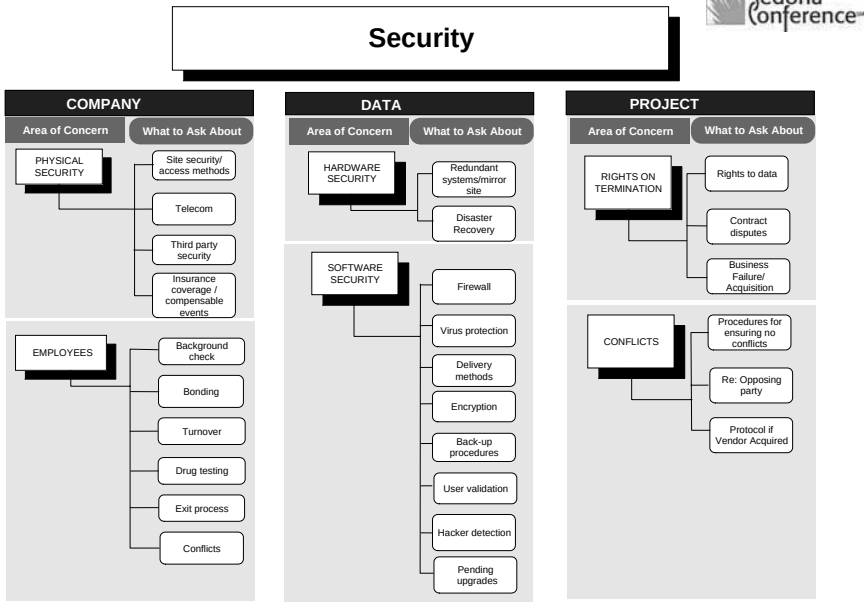


wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

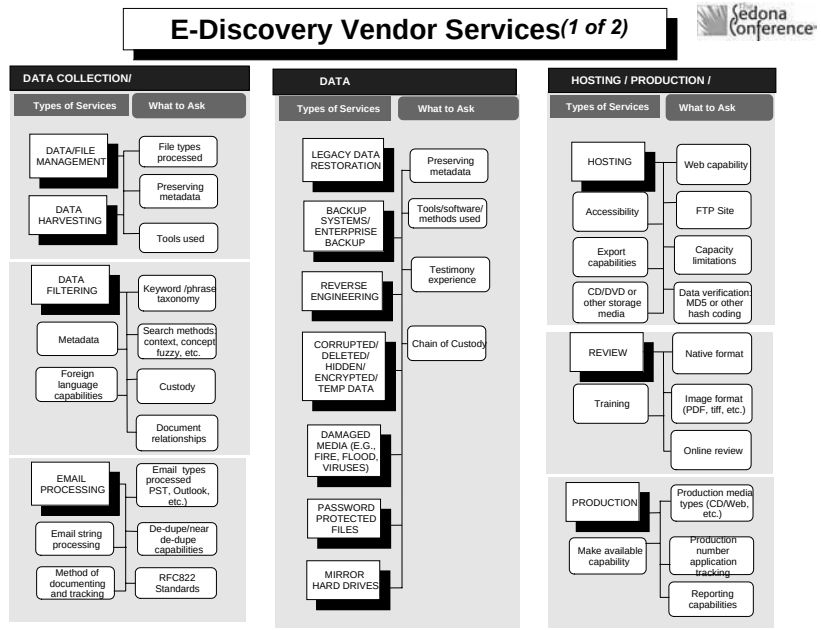


wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).



Copyright© 2005, The Sedona Conference®. All Rights Reserved.

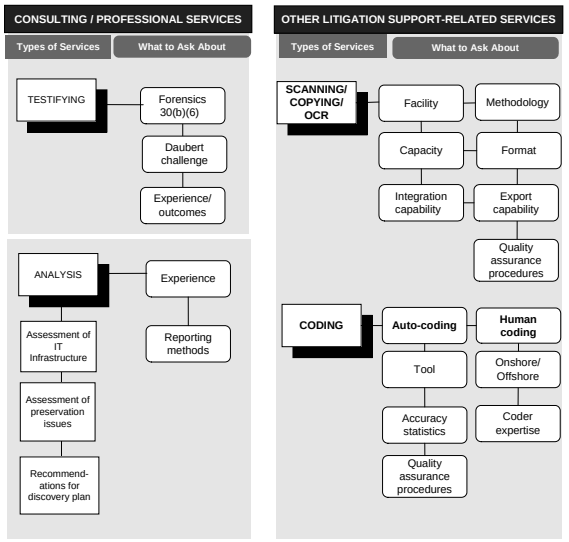


*See Glossary (Appendix ?) for definition of terms and concepts on this page.

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

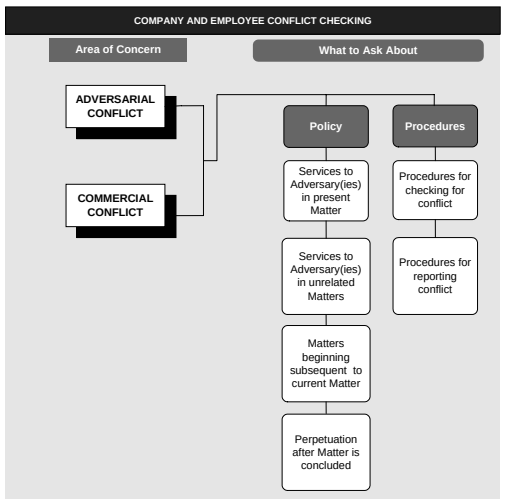
E-Discovery Vendor Services *(2 of 2)*



*See Glossary (Appendix ?) for definition of terms and concepts on this page.

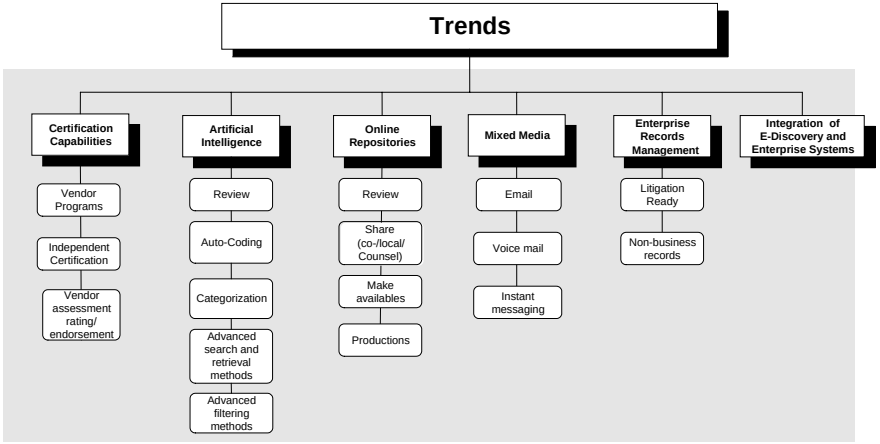
wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Conflicts



wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).



Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Appendix B

Sample Non-Disclosure Agreement

MUTUAL NONDISCLOSURE AGREEMENT

THIS MUTUAL NONDISCLOSURE AGREEMENT is made and entered into this ___ day of _____, 200_, between XYZ, Inc., a _____ Corporation, and ABC, Inc., a _____ Corporation.

1. Purpose. The parties wish to explore a business relationship of mutual interest and in connection with this opportunity, each party may disclose to the other certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

2. "Confidential Information" means any information relating to the business plans, financing, capital structure, proprietary processes, or technologies owned by, licensed to, developed by and/or discussed by either party and any other information the parties should reasonably assume is confidential or proprietary to the disclosing party. Confidential Information shall not, however, include any information which (i) was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party; (iii) is already in the possession of the receiving party at the time of disclosure by the disclosing party as shown by the receiving party's files and records immediately prior to the time of disclosure; (iv) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession; or (v) is required by law to be disclosed by the receiving party, provided that the receiving party (i) gives the disclosing party prompt written notice of such requirement prior to such disclosure, (ii) provides a letter from counsel confirming that the Confidential Information is, in fact, required to be disclosed, and (iii) provides assistance in obtaining an order protecting the information from public disclosure.

3. Non-use and Non-disclosure. Each party agrees not to use any Confidential Information of the other party for any purpose except to evaluate and engage in discussions concerning the business relationship between the parties. Each party agrees not to disclose any Confidential Information of the other party to third parties or to such party's employees, except to those employees of the receiving party

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

who are required to have the information in order to engage in the business relationship between the parties.

4. Maintenance of Confidentiality. Each party agrees that it shall take reasonable measures to protect the secrecy of and avoid disclosure and unauthorized use of the Confidential Information of the other party. Without limiting the foregoing, each party shall take at least those measures that it takes to protect its own confidential information.

6. Return of Materials. All documents and other tangible objects containing or representing Confidential Information which have been disclosed by either party to the other party, and all copies thereof which are in the possession of the other party, shall be and remain the property of the disclosing party and shall be promptly returned to the disclosing party upon the disclosing party's written request.

7. No License. Nothing in this Agreement is intended to grant any rights to either party under any patent, mask work right or copyright of the other party, nor shall this Agreement grant any party any rights in or to the Confidential Information of the other party except as expressly set forth herein.

8. Term. The obligations of each receiving party hereunder shall survive until such time as all Confidential Information of the other party disclosed hereunder becomes publicly known and made generally available through no action or inaction of the receiving party.

9. Remedies. Each party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

10. Miscellaneous. This Agreement shall bind and inure to the benefit of the parties hereto and their successors and assigns. This Agreement shall be governed by the laws of the State of _____, without reference to conflict of laws principles. This document contains the entire agreement between the parties with respect to the subject matter hereof, and neither party shall have any obligation, express or implied by law, with respect to trade secret or proprietary information of the other party except as set forth herein. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision. This Agreement may not be amended, nor any obligation waived, except by a writing signed by both parties hereto.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

XYZ, Inc.	ABC, Inc.
_____	_____
By Name / Title	Name
_____	_____
Signature	Signature
_____	_____
Date	Date

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Appendix C-1: Hypothetical for Sample RFI & RFP

Hypothetical Fact Pattern
For "Sample" Tailored RFI (C-2) and RFP (C-3)

Introduction

The legal and technical situations pertinent to each of our clients vary widely, and there is no 'one size fits all' form of RFI or RFP. There is a certain thought process, however, that walks through the considerations necessary for compiling a case specific understanding of the requirements to be described in these documents. To frame this thought process, we set forth below a very simple hypothetical fact pattern to walk through the various considerations. We have opted to approach this from the producing party's viewpoint, yet with sufficient information that should show how to "tailor" an RFI or RFP for your particular situation.

The Case

As attorney for the defendant, you have just received a Summons and Complaint in a new matter wherein their main competitor, "Make Believe Management, LLP", is suing your client, "Cold Reality Inc.". Make Believe Management is claiming that Cold Reality is infringing its patent on a new video game show involving fictional lawsuits called "Sue Me." The allegedly infringing show marketed by Cold Reality is called "Court Fun." Aside from docketing the pleading in your office calendar and calling your client about this unfortunate turn of events, what do you do next? What should your immediate considerations be, specifically from the standpoint of determining what potential electronic information may exist and be relevant, and how to approach the issues?

Case Assumptions / Understanding What Your Client Has

The first thing you need to do is gain a thorough understanding of all of your client's potential sources of relevant data and make sure that appropriate preservation orders are issued and followed up with appropriate contacts with pertinent individuals. This will require you to meet with whoever is responsible for Cold Reality's Information Technology ("IT") infrastructure. The goal is to obtain a comprehensive list of all applications, databases, and web

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

tools used by Cold Reality, an accurate map of their network (listing all networked computers), a list of all hardware issued to employees, a list of back-ups and legacy data, a copy of the Cold Reality's Policies and Procedures regarding internet and computer use, and copies of any organizational charts. Your investigation reveals that Cold Reality has the following:

1. A staff of fifteen (15) full-time employees and three (3) traveling sales persons.
2. Each full-time person has a desktop computer connected to Cold Reality's network.
3. Each sales person has a company provided desk-top computer at their residence and a company provided laptop computer to use while they are on-the-road.
4. Sales staff can remotely access the firm network via a Citrix server.
5. Cold Reality has a large sales and marketing database within which it tracks customers and sales efforts;
6. Cold Reality has a database of pending and current patents, and research regarding similar patent filings made by others;
7. Cold Reality's network consists of three (3) server computers. One (1) for email, which runs Microsoft Exchange; one (1) for document storage; and one (1) Citrix server for the sales staff remote access.
8. Cold Reality has a 30-day document retention policy which has been strictly adhered to.
9. Cold Reality backs-up its information systems every night of the work week, using 4 tapes, so that on any given day it has 20 back-up tapes. These tapes are rotated weekly.

Preservation Notices [See The Sedona Guidelines, Best Practices for Managing Information in the Digital World, Principle No. 6]

Once you have identified all of the data, files and other information sources that must be preserved, notices must be issued to the employees of Cold Reality that are responsible for or otherwise possess the data or files, or are responsible for the content of an information source such as a database or web site. If you suspect that relevant information that has been deleted from the company's computers may exist on back-up tapes, you must consider whether you need to preserve the current back-up tapes by taking them out of the back-up rotation. The Preservation Notices should generally describe the nature of the lawsuit, the relevant time

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

periods (if known), and the subject matters of the documents, emails, files or other data that must be preserved. For example, in the case of Make Believe's lawsuit against Cold Reality, the Preservation Notice will instruct employees to save all documents concerning the development and marketing of the Sue Me game show and all documents concerning the Court Fun game show. In addition, the Preservation Notices should ask employees to immediately identify others in the company with knowledge of the issues raised by the lawsuit. The notices should be sent via email and hardcopy, with return receipts and follow-up telephone calls to confirm their receipt and understanding of the Notice.

Regarding employees who have left the company, but who may have generated relevant information during their tenure, steps should be taken immediately to locate the hardware used by those employees, and if their machine and hard drive were wiped and recycled, the dates of those events should be documented.

It is also important to review previous Preservation Notices issued by the company to determine of any covered subject matters similar to the subject matters covered by the current lawsuit. If any do, you will need to collect relevant documents from the document collections made in connection with those prior suits.

It is important to keep detailed records of when and to whom the preservation notices are issued. Given that Cold Reality is a fairly small organization, it probably makes sense to issue the preservation notices to all 18 employees.

Developing a Collection Protocol

Estimate the Size of Cold Reality's Data Set

How you collect the information for production is a function of: (1) the size of the case; (2) the amount of data expected; and (3) discussion with counsel for Make Believe as to how they want the information produced. Basically, the bigger the case, the bigger the data set, making expenditures on mining, searching and review technologies appropriate and welcome. Smaller cases with smaller data sets may require some combination of less sophisticated or expensive technologies. In either case, the analysis begins with estimating the size of the data sets, both electronic and hard copy, involved. Again, since Cold Reality has only eighteen (18)

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

employees to collect from, it makes sense to meet with each of them to review their electronic and hard copy data sources. These meetings should be conducted by two (2) individuals and should include a form interview sheet that will record the fact of the meeting, the questions asked, and the answers given. It is important to establish written collection procedures for each of the individuals and the types of information identified in the organization. The amount of data pertaining to these individuals can generally be gleaned directly from the server and employees hard drive. Once you have an understanding of the size of the data sets, you can begin the process of determining what technologies will best assist you in expediting the collection, review and production.

In the case of Cold Reality, because it is a small company, our interviews indicate that virtually everyone in the company was involved in the Sue Me product. In addition, it is clear that both the marketing and patent databases have relevant information. Because we are concerned that some employees may have deleted emails after receiving the Preservation Notices, we have decided to remove all the current back-up tapes from rotation and replace them with 20 new tapes. Also, during one of the interviews an employee located some legacy tapes in a closet that he had saved "just in case." These tapes contain data from the Company's old email system which ran Lotus Notes, as well as its legacy sales database.

1. Making a Plan

The final result of the ideal plan is a single fielded, relational database containing .pdf or .tiff images of all information collected, reviewed and produced; together with basic metadata and text for electronic documents, bibliographic coding, OCR text for hard copies, subjective coding, privilege assessments, confidentiality assessments, production history, and - ultimately - tracking as to exhibit use at depositions, trial and evidentiary rulings. In many cases it is also preferable to maintain the document database within your case management program, so that, for example, the pleadings and transcripts can be linked to the documents; and the documents can be used to develop timelines, chronologies, and demonstrative exhibits.

2. Identifying Needed Electronic Media Processing

A list of the various services provided by electronic discovery vendors is set forth in the accompanying white paper, titled "Best Practices for the Selection of Electronic Discovery

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Vendors: Navigating the Vendor Proposal Process." **See** Chapter VI, What's for Sale: Electronic Discovery Services. Use this list to develop a description or list of the services you need. You will use this list to ask various vendors receiving your RFI which of the services they provide. After you have narrowed the field of vendors to choose from with the RFI process, the same list will be used in the RFP to inquire as to vendors processes and pricing for each service needed.

In the case of *Make Believe vs. Cold Reality*, it appears that a complete set of vendor services will be necessary, including but not limited to:

- Harvesting files and data from servers, including email;

- Restoring current back-up tapes and harvesting the restored data;

- Restoring legacy back-up tapes and harvesting the restored data;

- Harvesting files from C drives and thumb drives;

- Harvesting relevant data from databases;

- Collecting, scanning and OCRing;

- De-duplicating all of the above;

- Processing all the electronic information collected so that metadata and text are fielded, and can be placed in an application for review, designation and redaction;

- Review - relevancy, privilege, etc. - creation of appropriate logs;

- Conversion for production (and/or prep for production in native format);

- Creation of production load files for production or for use in an in-house review tool.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Appendix C-2: Sample Tailored RFI

SAMPLE REQUEST FOR INFORMATION (RFI)

– MAKE BELIEVE VS. COLD REALITY -

Confidential

[Date]

Any Electronic Evidence Vendor
One Discovery Street
Hard Drive, Illinois 12345

Re: Request for Information ("RFI"): Electronic Data Preservation and Collection Services

Dear XXX

The undersigned firm represents Cold Reality Inc with respect to the litigation brought by Make Believe Management, LLP, *Make Believe v Cold Reality*, a fairly small matter in the Northern District of California in San Francisco. Your firm has been identified as a potential provider of litigation support, electronic evidence and data hosting services for defense counsel in this litigation. We would appreciate your execution and return of the enclosed Non-Disclosure Agreement ("NDA") prior to submitting your responses to this RFI. Please fax the executed NDA to _____ at _____, sending the original to us via first class mail.

Your response to this RFI will be used to identify whether you are a candidate suitable for issuance of a Request for Proposal containing specific inquiries as to how you propose to satisfy the preservation, collection and production needs of this case. Accordingly, we appreciate detailed responses to this RFI and we welcome your suggestions and offerings of information that we have failed to ask about, but may nonetheless be helpful to our case. Please feel free to provide additional information on other services you feel would be benefit or value to the firm or our client.

This litigation revolves around patent infringement issues with respect to the game shows "Sue Me" and "Court Fun," produced by the parties and currently viewable on national television networks. The firm is looking for a full service provider capable of providing litigation preservation, collection and production services for both electronic data and hardcopy, paper documents. In addition, the data and documents collected will need to be processed for hosting on an externally hosted site, securely accessible by our attorneys and client's in-house counsel.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

SAMPLE REQUEST FOR INFORMATION (RFI)

– MAKE BELIEVE VS. COLD REALITY -

While we cannot guarantee that this case will not be resolved by motion practice or settlement, no dispositive motions are pending and neither party has indicated an intention to resolve this dispute outside of court. Accordingly, this RFI is issued with our full intent to retain an appropriate service provider.

Your complete response to this Request for Information, which should be delivered to us in printed paper form and an electronically searchable PDF file, must be submitted within 7 days of receipt of this RFI.

Please direct your responses to the undersigned with copies to John Dough and John Cash, at this firm as well as Bud E Guy, Esq., in-house counsel at Cold Reality, Inc. 1313 Mockingbird Lane, Centerville, USA. Please do not hesitate to contact me at _____, or by email at _____.com, if you have any questions, suggestions, or concerns.

Very truly yours,

Mr. John Lit Supp
Director of Litigation Support

Little, Firm, That, Could, LLP
One Defense Way
Struggle, Ohio.

cc: J. Dough

J. Cash

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

SAMPLE REQUEST FOR INFORMATION (RFI)

– MAKE BELIEVE VS. COLD REALITY -

REQUEST FOR INFORMATION

Please provide us with information regarding your capabilities to provide the necessary support for the following:

- Length of engagement: medium-term litigation (potentially 1-3 years).
- Number of documents: At least 100,000, although potentially more than 1,000,000, including documents in native format.
- Harvest of data from approximately 18 hard drives, 3 servers and potentially other sources.
- Type of documents: Documents will be collected and produced in both paper and electronic format. Those documents not in "native format" will need to be scanned, bibliographically coded, and "OCR" processed, with an identified degree of OCR accuracy.
- Please describe your reporting and quality assurance procedures.
- What are your standard representations, warranties and service level guarantees?
- Document Review and Production Database: Please identify your capabilities in the following areas:
    - Ability to organize and segregate documents in a variety of manners (including by producing party)
    - Ability to host all documents in a single uniform image format with the corresponding native format file linked with images
    - Handling of all metadata captured and saved in situations where native files have been converted to images, including captured and searchable text.
    - Backup procedures and redundant layers of protection of the data
    - Security: Facility, Server, Database and user security are all of great importance. Please describe your security protections, procedures and audit procedures for same, as applied to both network and physical security
    - The provision of ASCII load files for in-house review tools.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

SAMPLE REQUEST FOR INFORMATION (RFI)

– MAKE BELIEVE VS. COLD REALITY -

- Electronic File Processing: Please describe your capabilities in the following areas:
    - The processing and chain of custody protocols and other measures used to avoid spoliation charges;
    - Your de-duplication methodologies and process and testing of same;
    - Identify artificial intelligence algorithms or other tools, if any, used to parse, categorize, segregate, or tag data, together with process for using and testing same;
- Document Review: Please advise as to your systems and processes for administering document review capabilities and support to the following specifications:
    - Access to a document review database by 10 or more attorneys and/or paralegals (potentially in different parts of the country) at a given time through standard web browsers, from any internet-connected computer, with or without tokens for security. Documents should be available for review for 24 hours per day, with exception for normal database maintenance.
    - Single web-based review tool for all databases. Please specify any required client software downloads or agents.
    - Training: Please describe your processes, extent, and frequency of training.
    - Technical support: Set forth the extent and method used for providing technical support for issues relating to accessibility, functionality and content management.
    - Printing: Please describe your print capabilities for batch printing provided at your facility, the facility of a vendor of our choice, or to a local printer at the user's office.

VENDOR BACKGROUND

Please supply a narrative description of your history, together with your contact information, proof of financials viability, and data regarding your corporate structure, number of employees, and other pertinent information regarding your business.

SECURITY

We would like to understand the measures undertaken by you to ensure the security and integrity of your networks and physical building.

wgs™

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

SAMPLE REQUEST FOR INFORMATION (RFI)

– MAKE BELIEVE VS. COLD REALITY -

SUB CONTRACTORS

Please set forth any areas of work that you prefer to sub-contract, together with the reasons for sub-contracting this work.

CONFIDENTIALITY

This matter, the participants and any information disclosed during this RFI process or (for the vendor selected) during the actual engagement is deemed confidential. In addition to the non-disclosure agreement submitted by you prior to responding to this RFI, you may be required to sign a confidentiality order imposed by the Court.

CONFLICTS

Prior to retention, vendor shall be required to run a conflict check of its existing clients and its engagements to ascertain that conflicts do not exist with this case. This would include other engagements for actions our adversaries may be involved in.

wgs™

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Appendix C-3: Sample Tailored RFP

Bid Number:xxxxxxxx

LITTLE FIRM THAT COULD, LLP
ONE DEFENSE WAY
STRUGGLE, OHIO 12345

REQUEST FOR PROPOSAL **[DATE]**

Vendor Contact Vendor Name Vendor Address

You are invited to submit a proposal to provide services for electronic discovery services for Little Firm That Could, LLP

INSTRUCTIONS TO VENDOR

The following is a Request for Proposal (RFP) that conforms to the model RFP developed by The Sedona Conference's "RFP+ Working Group". Your company was selected to receive this RFP due in part to your willingness to adhere to the parameters the working group set forth (with input by your company and other professionals in the field) and your firm's professional capabilities. Please know that by responding to this RFP+, you are aiding in the fair and accurate interpretation of services and their pricing. By doing so, you are helping the consumer of these services reach their decision in a more timely and informed manner.

Responses to the proposal must be received by _____.

Base your proposals on the terms and conditions herein.

If you do not plan on bidding, please notify _____ as soon as possible.

Please review the RFP General Information, Contract Terms and Conditions. Please acknowledge your agreement to and understanding of these terms and conditions by signing on page 5 where indicated. Please return this part of the RFP with your proposal.

Information contained in this document is considered proprietary and confidential to Little Firm That Could, LLP, and you are subject to the terms and conditions of the non-disclosure agreement previously executed by you. Pursuant to the non-disclosure agreement, unauthorized disclosure of information contained herein may result in rejection of your proposal and legal action.

Sincerely,

_____
Requestor Name and Title
[Requestor contact information]

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

GENERAL INFORMATION, CONTRACT TERMS AND CONDITIONS

I. Definitions

The definitions set forth in the [Sedona Glossary] apply to the RFP and all related documentation, including your response to this RFP.

In addition, the following words shall have the following definition throughout this RFP:

Agreement and *contract* mean the final executed business arrangement between Little Firm That Could, LLP and the applicable Vendor, together with the constituent services, products, terms, conditions and costs of that relationship.

Vendor, *bidder*, *you* and *your firm* refer to the entities that will be submitting response(s) to this RFP.

RFP and *specifications* refer to each and every requirement stated in this document and all attachments hereto and any additional instructions that are developed and incorporated subsequent to the distribution of this document.

Proposal, *response* and *bid* refer to the complete product, service and price proposal submitted by the bidder as a result of this RFP.

II. Rights of Little Firm That Could, LLP

Little Firm That Could, LLP reserves and may exercise, at any time, any of the following rights and options with respect to this RFP:

* To reject any and all bids without incurring any cost, to seek additional bids, to enter into negotiations with and subsequently contract with more than one bidder, and/or to award a contract on the basis of criteria other than price.

* To evaluate separately the individual component(s) of each bid, such as any proposed subsystem, product or services, and to contract with such vendors for any individual component(s).

* To cancel or withdraw this RFP with or without substitution, to alter the terms or conditions of this RFP and/or to alter, within reason, the proposed implementation schedule.

* To conduct investigations into the qualifications of any bidder prior to time of award.

III. Incorporation

Your response to this RFP will constitute an offer to develop a contract based on the terms stated in this RFP, and in your Proposal. Little Firm That Could, LLP may, at its option, incorporate any or all parts of this RFP, and your Proposal into the contract.

IV. Proposal Validity

All terms and quotations of each bid, including but not limited to Vendor's price quotations, shall be valid for a period of not less than 60 days following the date of submission.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

V. Confidentiality and Use of Little Firm That Could, LLP Name

The specifications and information verbally gathered contain confidential and proprietary information and are provided to you and your firm solely for the purpose of enabling you to prepare a proposal. It is not to be used for any other purpose or disclosed to any third party or to any of your employees, agents or representatives other than those who have a need to know such information in preparing the proposal. You agree not to disclose to any third party the existence of the RFP.

In connection with this RFP, bidders shall not use the name of Little Firm That Could, LLP or any of its subsidiaries or affiliates in any publication or public relations document without the written consent of Little Firm That Could, LLP prior to such publication or announcement. Little Firm That Could, LLP reserves the right to review and approve all press-related copy and may withhold consent for release of such copy, with or without cause.

VI. Completeness of Response

By virtue of submitting a signed bid, a bidder warrants that the requirements of this RFP have been read and understood and represents that the delivery and implementation of the products and services specified in this RFP shall in no way obligate LITTLE FIRM THAT COULD, LLC to pay any additional costs to the Vendor for services or products other than those presented in the bid.

VII. Contract

This RFP represents a definition of specific requirements. It is not an offer to contract. Only the execution of a written contract will obligate Little Firm That Could, LLP in accordance with the terms and conditions contained in such contract.

VIII. Bid Costs

This RFP does not obligate Little Firm That Could, LLP to pay any costs that you incur in the preparation of your Proposal. All costs associated with the preparation of a Proposal in response to this RFP will be borne solely by the vendor. Your Proposal shall become the property of Little Firm That Could, LLP.

IX. Terms and Conditions

It is expressly understood that the successful bidder and its representatives shall carry all necessary licenses, permits and insurance and successful bidder shall hold harmless and indemnify Little Firm That Could, LLP for any claims related to a service agreement with Little Firm That Could, LLP.

X. Non-Collusive Bidding

By submitting this bid, the Bidder certifies that:

(a) the prices in this bid have been arrived at independently without collusion, consultation, communication or agreement for the purpose of restricting competition as to any matter relating to such prices with any other bidder, any competitor, or any Little Firm That Could, LLP employee or representative;

(b) the prices quoted in this bid have not been, and will not be, knowingly disclosed, directly or indirectly, by Bidder to any other bidders, competitors or Little Firm That Could, LLP employee prior to the final date of submission of such bid;

(c) no attempt has been made and none will be made by the Bidder to induce any other person, partnership or corporation to submit a bid (complimentary or otherwise) for the purpose of restricting competition.

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

XI. BID PROPOSAL DUE DATE

Proposals will be received at the address specified until the close of business on _____.

XII. PROPOSALS

All Proposals will become the property of LITTLE FIRM THAT COULD, LLP and will not be returned. Questions regarding the RFP should be in writing and directed to _____. These questions will be responded to as quickly as possible. Copies of questions and the answers may be provided to all Vendors without identifying the source of the question.

Please submit 4 copies of the proposal to:

_____
Requestor Title
LITTLE FIRM THAT COULD, LLP
ONE DEFENSE WAY
STRUGGLE, OHIO 12345

Phone:
Fax:
Email:

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

SCOPE OF WORK

Preamble

The undersigned firm represents Cold Reality, Inc with respect to the litigation brought by Make Believe Management, LLP, *Make Believe v Cold Reality*, a fairly small matter in Federal Court, 9th Circuit, San Francisco, California. Your firm has been selected to receive this RFP based on your responses to a previously issued Request for Information (RFI)I as to providers of litigation support, electronic evidence and data hosting services for defense counsel in this litigation.

This litigation concerns patent infringement issues with respect to the game shows "Sue Me" and "Court Fun" produced by the parties and currently viewable on national television networks. The firm is looking for a full service provider who will be capable of providing paper and electronic data preservation, collection and production services. In addition, the data will need to be collected, processed and made available on an externally hosted site, securely accessible by our attorneys and in-house counsel for Cold Reality, Inc.

As set forth in the RFI, this project requires the following general capabilities, expertise and commitments. You confirmed in your response to our RFI that your firm has the expertise and capabilities to meet all of these requirement, and Little Firm That Could, LLP has relied on the representations in your RFI responses in submitting to you this RFI. All of your responses to our RFI are incorporated herein by reference.

General Requirements:

- Length of engagement: medium-term litigation (potentially 1-3 years).
- Number of documents: At least 100,000. although potentially more than 1,000,000, including documents in native format.
- Harvest of data from approximately 18 hard drives, 3 servers and potentially other sources.
- Type of documents: Documents will be produced in both paper and electronic format. Those documents not in "native format" will need to be scanned, bibliographically coded, and "OCR" processed
- Database: The provider is responsible for administering the databases to the following specifications:
  - Ability to organize and segregate documents in a variety of manners (including by producing party)
  - Documents should be hosted in a single uniform image format with the corresponding native format file linked. Other images should be in Group IV Tiff format, 300 dpi. OCR specs to be discussed.
  - All Metadata captured and saved in situations where native files have been converted to images.
  - Back-up: Proper backup procedures and redundant layers of protection of the data must be evidenced.
  - Security: Facility, Server, Database and user security are all of great importance and the selected vendor will be required to demonstrate capability and auditing procedures.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

  - Provider may also be required to provide ASCII load file for in-house review tools, as well.
- Electronic File Processing
  - Court tested and established professional processing and chain of custody protocols must be demonstrated to avoid spoliation charges.
  - De-duplication methodology and process must be demonstrated.
  - Artificial intelligence algorithms, if any used to parse data to review folders, must be tested and approved prior to engagement.
- Review of documents: The provider is responsible for administering the document review capabilities to the following specifications:
  - Access by 10 or more attorneys and/or paralegals (potentially in different parts of the country) at a given time through standard web browsers, from any internet-connected computer, with or without tokens for security. Documents should be available for review for 24 hours per day, with exception for normal database maintenance.
  - Single web-based review tool for all databases. We prefer that the review be available without client software download or agent.
  - Training: End user training for those accessing the databases should be initially done in person several times, with subsequent training sessions via online methods.
  - Technical support: All users accessing the databases will need to have live and easy access to tech support for issues relating to accessibility, functionality and content management. Access to a project manager will be required during expanded business hours.
  - Printing: Users should have the ability to print either individually or in bulk to a printer at your facility, the facility of a vendor of our choice, or to a local printer at the user's office.
  - Security: There must be configurable levels of security to allow partitioned access to all users and user groups maintainable by an administrator based at one of the client law firms.

Specific Requirements

The requirements set forth below represent only those requirements currently known by Little Firm That Could, LLP and is in no way an exhaustive list. Little Firm That Could, LLP fully expects that the vendors responding to this RFP will recognize and specify any additional requirements necessary to satisfy the company's needs in connection with properly preserving, collecting and producing paper and electronic data, as well as requirements for establishing, maintaining and using an Electronic Document Database. The basic requirements are:

I. Housing and maintenance of the Electronic Document Database in a secure environment for an indefinite period of time, with appropriate back-up and system recovery processes and support procedures. Please describe your recommended approach and the technical architecture for:

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

A. Storing and maintaining this repository of documents and the associated meta data, including the type of hardware utilized (optical or magnetic)

B. Will all data will be stored on line or does your solution differentiate between online and near line storage. If there is a differentiation please describe how this data will be made available when needed.

C. Will the data repository and associated applications be hosted on equipment dedicated to Little Firm That Could, LLP? If not please describe what components of this architecture are shared.

II. Please provide a high level technical architecture of your proposed solution including application and data servers, security components, firewall/routers, and access points to and from the network.

A. Facilities: Please describe how your proposed solution will satisfy each of the following requirements:

1. Backup power supplies for hosting facility
2. Hosting facility redundant power supply
3. Dual power feeds to each cabinet in the hosting facility from two different power systems
4. HVAC environmental control including air conditioning and humidity control
5. Carbon dioxide and fire suppression and detection systems
6. Geographical location to be within the United States
7. Physical security of the facility
8. Other relevant attributes of your facility that should be taken into consideration.

B. Ongoing support and professional services: Please describe how your proposed solution will satisfy each of the following requirements:

1. Hours of help desk support for client based services and operational needs. Unlimited 24x7x365 helpdesk support is requested for operational needs. If client support is not 24x7x365 please describe the process and costs associated with obtaining additional support outside of normal service hours;
2. Change & Configuration Management – documented procedures to support change management. This must include a cataloged inventory of change records monitored and managed by the vendor Project Manager, overseeing the day-to-day and the strategic direction of the environment;
3. Server problem diagnosis and resolution --- System troubleshooting, diagnosis, problem resolution, reboots/restarts, rebuilds;
4. Problem Management – documented problem management procedures including escalation path. Please identify the anticipated point of escalation;

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

a) Hardware maintenance and component upgrades – replacement of failed components, scalability-on-demand;

b) Dedicated Vendor Project Manager - For transition and part of support team after "go live";

c) Dedicated Technical Support Team;

d) Process for reporting and responding to system outages, including time to respond and time for repair;

e) Identify standard rate for any T&E professional services that may be required for future upgrades or other services that might be outside of the scope of this RFP.

C. Backup and Restore Services: Please describe how your proposed solution will satisfy each of the following requirements:

1. Daily backups of system, content and databases;
2. Tape storage;
3. Tape retention;
4. Recovery procedures and costs for restoration/recovery;
5. Disaster Recovery plan, including estimated recovery time.

D. Monitoring Services: Please describe how your proposed solution will satisfy each of the following requirements:

1. Real-time monitoring of the network, operating system, firewalls, web servers, database servers, network routers and switches;
2. Proactive Server Fault Management / Monitoring – This must include regular testing to ensure infrastructure and applications are operating properly, documented results provided to Little Firm That Could, LLP;
3. Predictive Server Fault Management / Monitoring;
4. Basic Server Monitoring to include:
   a) CPU
   b) Disk Space
   c) Memory
   d) Ping
   e) Operating System Services
5. Database Monitors

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

6. HTTP Port Monitor
7. SSL Port Monitor
8. URL Monitor
9. Content match monitor
10. Internet utilization monitor
11. End-user performance monitoring (e.g., Keynote)

E. Security Services: Please describe how your proposed solution will satisfy each of the following requirements:

1. Network Intrusion Detection System;
2. Host Intrusion Detection System (optional);
3. Incident Management (how are incidents handled, reported to customer and escalated?);
4. Security Patch Deployment;
5. Dedicated Redundant Firewalls;
6. Virus scanning (optional);
7. Vulnerability scanning (optional).

F. Performance Services: Please describe how your proposed solution will satisfy each of the following requirements:

1. Local load balancing (improved performance and high availability);
2. Stress testing production environment.

G. Service Level Agreements: Please describe how your proposed solution will satisfy each of the following requirements:

1. Provide the service level (i.e., 99.9%) you will agree to for access to the environment and any exclusions Little Firm That Could, LLP would be expected to agree to for this calculation
2. Please describe the reporting that will be provided to Little Firm That Could, LLP
    a) Operational, utilization, and availability
    b) Capacity and performance
3. Please describe the process that will be used for supporting changes to the environment or support for special projects.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

III. Please define for Little Firm That Could, LLP how the metadata and the email and its contents will be stored within the repository. Please explain why you believe that your approach, native, PDF, TIF, database, etc. is the best approach based on Little Firm That Could, LLP requirements, given the other alternatives that may be proposed.

A. For the purpose of providing this metadata to the Vendor along with the email with its contents, please define the approach you prefer Little Firm That Could, LLP utilize to transfer this data to you for inclusion into the repository.

B. Analyze the impact on your proposal of whether or not Little Firm That Could, LLP transfers to the Vendor imaged documents (tiff or pdf) or documents in their native format.

C. Please describe the process that you recommend Little Firm That Could, LLP employ to securely transfer the collected documents to you, along with the process for validating the receipt of the data and its successful inclusion into the repository. Upon your notification of receipt Little Firm That Could, LLP plans to delete the associated media from our environment.

IV. Software and training (for all users, including administrators, attorneys, and support personnel) for the secure web-based review of documents in the Electronic Document Database by company personnel and its outside counsel, with the following features: Please provide detailed descriptions and visuals as appropriate to help Little Firm That Could, LLP understand the functional capabilities available with your offering.

A. Centralized management of document review;

B. Ability to designate documents, (individually and in batches, without opening each individual document), with customized designation categories;

C. Redaction capabilities;

D. Tracking capabilities; Text and field (metadata) searching capabilities; Please describe if the metadata can be used to selected a subset of documents and/or based on searching capabilities if metadata can then be leveraged to further refine the search.

E. Ability for reviewers to batch print selected documents locally;

V. Please provide an overview of the production services offered, the quality control processes that will be utilized and the costs associated with such services; on a case by case basis, provide printing, CDs with specified metadata and/or text, or web-based viewing limited to specified documents, text and/or metadata;

VI. On going support to Little Firm That Could, LLP regarding data transfer from Little Firm That Could, LLP's IS department to Vendor, attorney review support, and system administration support.

VII. Ongoing legal education and consultation to Little Firm That Could, LLP attorneys as to legal developments in the area of electronic discovery.

VIII. It is requested that the software capabilities described above be provided to Little Firm That Could, LLP and its client through a secured web site. It is expected that approximately 30 individuals will have access to this repository. These individuals will be located in a variety of different locations each employing different desktop and security requirements within their environment.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

A. Please describe the process that will be used to provide access to the environment.

B. Please describe the security of the web site and any security components that are used for 2nd level of authentication.

C. Please describe the ability to provide authorization to individuals based on different levels of access that may be needed or restrictions to data based on either the Meta data or the users role in the review process.

D. Please describe any restrictions based on software, operating systems, network connections, etc., that will be required for operation of the web site.

E. Please define if any software or other components need to be loaded onto the client workstation for access to the web site;

F. What if any firewall ports need to be opened for access to this environment.

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Navigating the Vendor Proposal Process *July 2005 Version*

Appendix D: Pricing Models

Pricing Models

When evaluating proposals from multiple vendors, one of the hardest areas to compare is the pricing for the proposed project. Because there are no standards governing the processing of electronic data, most vendors follow their own proprietary workflow, and base their pricing on that workflow. Even when looking at the pricing for discrete portions of an electronic discovery project, such as conversion to TIFF, it is often difficult to compare multiple vendor proposals because some vendors bundle the pricing for this step with other processing steps.

The number of options for processing electronic data for review and production also make it difficult to compare proposals from multiple vendors. While the vast majority of all electronic data was traditionally converted to TIFF for review and production (either on paper or in load files), more and more vendors are changing their processes to allow the review to take place in "native" format. Because of the predominance of TIFFing, the vast majority of electronic discovery projects were priced on a per page basis, and while the cost of TIFFing is not the only cost associated with processing e-data for review under the traditional model, it represents a significant portion of the overall cost of the process. However, as more and more e-data is reviewed in native format, the pricing of electronic discovery projects has moved towards volume or gigabyte" based pricing, which is not the only cost associated with processing e-data for review under this model, but also represents a significant portion of the overall cost of the project.

A few observations are in order before delving into the nuts and bolts of pricing. The cost to process e-data for review and production (whether to TIFF, PDF, Native or some other format) is by far the most expensive and time consuming component of the electronic discovery process. Therefore, any steps that can reduce the amount of data to be processed, whether by harvesting only potentially responsive data – as opposed to copying entire hard drives – or by eliminating non-relevant data by culling out system files, using date filters or keyword searches,

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

will almost certainly reduce both the time it takes to process the data for review as well as the overall cost of the project. Using objective criteria to remove non-responsive data from the review set using filtering technology (whether keyword or concept based) will always be more efficient, and cost effective, than using human reviewers to eliminate this data.

New processes, such as "concept" search engines, a fairly new technology to the electronic discovery world, bring with them their own set of pricing models, which tend to look somewhat like the pricing models for native review. However, because the process itself is different than traditional native processing, comparing proposals for these services with TIFF or Native processing proposals may have to be done at a higher level than the granular line item comparison that we propose in this White Paper. In fact, it may be that the only way to compare a proposal involving these new technologies with proposals for TIFF or Native processing is to look at the total cost of the project, and in some instances, because these new processes involve different review strategies, the comparison may have to include the projected review costs. [Indeed, as noted by David Burt in connection with supply chain management, the "all-in" cost, or total cost, is the key metric to consider.]

In order to fully understand the pricing of electronic discovery services, it is imperative to understand the process itself. To that end, the following is a representation of the electronic discovery process – starting with collection of electronic data and concluding with the production of electronic data, either electronically, or on paper. We have broken down the process into 6 broad steps, each of which is itself composed of multiple steps. Obviously, not every step described below will be necessary in every project. As you would expect, vendors have different pricing models for each of the steps, or in some cases, for each of the sub-steps described below.

Harvesting

(forensic recovery or active data acquisition, restoration of back-up tapes)

Processing
(elimination of system files, de-duplication, culling by date ranges, keyword searching)

Conversion
(extraction of metadata, conversion to TIFF\PDF, processing for native review)

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Creation of Review Database
(loading, user fees, hosting)

Production
(endorsement – bates numbering, confidentiality logo, etc. – printing of production sets or creation of load files if documents are to be produced electronically)

Creation of Production Database
(loading, user fees, hosting)

Another important, and often significant, component of the total cost of the electronic discovery process are project management fees. Some vendors incorporate these costs into their overall price model, others charge a percentage of the total project cost, while others charge by the hour for project management, strategic partnerships are sometimes entered into, with totally unique pricing models.

Outside of the context of strategic partnerships or long-term relationships, most vendors use one of two general pricing models, albeit generally with their own twist. We will briefly examine these models, point out some of the issues associated with each of them, and then describe our proposed methodology to compare proposals from vendors using different models – although our hope is that vendors will respond to an RFP (such as the attached sample) with pricing based upon the pricing model sought in the RFP – or at least breaking down their pricing in such a way that it can be compared with other proposals based upon the pricing format sought in the RFP.

The most common pricing model in use today is based on a per page fee, under which the vendor charges based upon the number of pages of TIFF or PDF images generated from the e-data in question. Given that until fairly recently, almost 100 % of e-data processed for review and production was converted to TIFF or PDF, many vendors, law firms and clients are fairly comfortable with this model, primarily because, like photocopying, it provides objective criteria – the client pays for the numbers of TIFF or PDF pages that are generated from the data set. However, one of the principal disadvantages of this model is that it is difficult to accurately estimate the number of TIFF or PDF pages that will be generated from a data set prior to processing, thus making it difficult to estimate the cost to process the data set. While some vendors include the cost of keyword searching, culling (based upon file types and\or date ranges)

wgs™
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

and de-duplication in their per-page TIFF or PDF charge, others charge separately for each of the steps.

A second common pricing model used by vendors is based upon the amount of data processed. Under this volume based pricing model, typically referred to as megabyte or gigabyte pricing, the vendor charges a set fee based upon the volume of data to be processed. Some vendors that use this model charge only for the data actually processed, after keyword searching, culling and de-duplication, but charge separately for each of these steps, while other vendors charge based upon the size of the raw data set, before keyword searching, culling and de-duplication but bundle the cost of these steps into their processing charge. While this pricing model at least appears to make it easier to estimate the cost of processing e-data – if the cost per Gigabyte is X and the data set consists of 100 Gigabytes of data, one can quickly calculate the cost to process the data set – it may be unlikely that all 100 gigabytes of data will have to be processed. As with the per page pricing model, the raw data set will most likely be reduced by keyword searching, culling and de-duplication, which will result in less than 100 gigabytes of data being processed.

Pricing models are as dynamic as the technology and processes used by vendors to process e-data. Therefore, it is imperative that the requesting party be able to break down the pricing contained in multiple proposals, regardless of the process used by the vendor. The requesting party should specify a pricing scenario in the request for proposals and vendors who use different pricing scenarios should provide a way for the requesting party to compare the pricing in their proposal to proposals in the requested format. For example, if the request calls for proposals based on a volume based pricing model, vendors who use a page based pricing model should include estimates of the number of pages of per gigabyte, so that the requesting party can compare the proposal to proposals based on volume based models.

Not surprisingly, pricing is an area of much innovation in this area. Fixed price models, incentive price models, and strategic long-term relationships represent alternatives to the basic approaches to pricing described above that are some of the innovations being tested today by major organizations.

wgs

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Appendix E: Decision Matrix

Sample Decision Matrix*

REQUEST FOR PROPOSAL: DECISION MATRIX **Sample Only-Weighting is key**

Score: 1-5
Weight: 1-3

	Weight	VENDOR SCORES			RESULTS			
		Vendor A	Vendor B	Vendor C		*Vendor A*	Vendor B	Vendor C
ABOUT THE COMPANY								
Stability	2							
Quality	2	3	3	5	About the Company	22	18	28
Obligations, Representations, Warranties	2	4	3	5	Personnel	36	36	42
Physical Plants	2	4	3	3	About the Product/Service	18	20	12
PERSONNEL					Company Security	18	20	12
Quality	3	3	3	3	Data Security	30	24	21
Experience	3	3	3	3	Project Security	23	20	25
Staffing Capacity	3	3	3	3				
Project Management	3	3	3	5	TOTAL	143	138	138
ABOUT THE PRODUCT/SERVICE								
Quality of Work	2	4	5	3				
Process and Infrastructure	2	4	5	3				
COMPANY SECURITY								
Physical Site Security	2	4	5	3				
Employees	2	4	5	3				
DATA SECURITY								
Hardware Security	3	5	4	4				
Software Security	3	5	4	3				
PROJECT SECURITY								
Rights on Termination	3	5	4	5				
Conflicts	2	4	4	5				

NOTE: Numerical entries for Score which are outside the range of 1-5, and numerical entries for Weight which are outside the range of 1-3, will be highlighted in RED.

***As mentioned in the text, only a beginning point.**

wgs

Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Appendix F: RFP+ Vendor Panel

RFP+ Vendor Panel List
(as of April 1, 2005)*

ACT Litigation Services
Applied Discovery
Aspen Systems Corporation - iCite Division
Attenex Corporation
Capital Legal Solutions
CaseCentral
Cataphora, Inc.
Celerity Consulting Group
The Common Source, Inc.
CompuLit
CoreFacts
Cricket Technologies, LLC
Daticon
Digital Mandate
Diskcovery Information Management Pty Ltd
DolphinSearch, Inc.
Electronic Evidence Discovery, Inc.
Fios, Inc.
Forensic Consulting Solutions, LLC
FTI Consulting, Inc.
H5 Technologies, Inc.
LECG
LDM - Legal Document Management Ltd.
Lex Solutio
LextraNet
Litigation Solution, Inc.
National Data Conversion
Relevant Evidence, LLC
Renew Data
SPI Litigation Direct
Stratify, Inc.
Technology Concepts & Design, Inc.
Zantaz, Inc.

*See website (www.thesedonaconference.org) for the current listing of the RFP+ Vendor Panel.

wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

Appendix G: RFP+ "User" Group

RFP+ User Group

Richard G. Braman, Esq.
Executive Director
The Sedona Conference

Matthew L. Cohen, Esq.
Skadden, Arps, Slate, Meagher & Flom LLP

Conor R. Crowley, Esq.
Labaton, Sucharow & Rudoff LLP

Sherry B. Harris
Hunton & Williams LLP

Anne E. Kershaw, Esq.
A. Kershaw, PC//Attorneys & Consultants

Mark V. Reichenbach
Milberg Weiss Bershad & Schulman LLP

wgs
Copyright© 2005, The Sedona Conference®. All Rights Reserved.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

What Every Lawyer Should know about the Impact of the Amended Federal Rules of Civil Procedure Regarding "Electronically Stored Information"

1. Be Aggressive. A computer organizes data in ways that make little sense to human beings. For instance, the computer operating system distributes data stored on the hard drive more or less randomly as free space becomes available, and then keeps track of what data resides where through an indexing system and by monitoring data in each file header. The machine does not automatically track files according to their content or context or meaning as a human being would naturally do. As a result, when large amounts of electronically stored information are collected or produced, it appears disorganized to us, and it can be very hard to discern what that information might mean within the context of a legal proceeding, investigation, or claim. In addition, electronically stored information is also highly duplicative; the same files can reside in multiple locations due to client-server conventions and back-up protocols. So while the data may be carefully stored and routinely backed-up, such attention to preservation does not mean it is easy for a legal team to discern relevant information from the irrelevant, or privileged information from non-privileged during the discovery phase of a legal matter. In fact, electronic data collected from hard drives on workstations or servers, or from digital tapes and other back-up media, is typically referred to as “unstructured data” precisely because it is not organized in a way that gives human beings much insight into what it really contains without reading all of it – an unenviable, perhaps even impossible task. Yet despite these difficulties, under the new Amended Federal Rules of Civil Procedure regarding “Electronically Stored Information” (ESI) it is very risky for a producing party to disregard such disorganized electronic information on the basis that it is too burdensome or messy to deal with, or that it is so disorganized as to be meaningless. Software tools now exist which can help us make sense of large sets of unstructured data, and the amended rules tacitly acknowledge this. Unstructured cannot be ignored any longer just because it is electronic; by rule it must be considered at the outset of a matter. Good lawyers can use this to their advantage by identifying where potentially relevant electronic information resides, and by asking for it, and by analyzing it using the modern e-discovery tools now available. Under the amended rules it pays to be aggressive when it comes to electronic discovery no matter which side of a matter you represent.

2. Review “Native Files.” Electronically stored information contains "metadata" which is not visible when those files are printed. This “metadata” is sometimes colloquially (and misleadingly) referred to as “data about data” and it can comprise information that may be crucial to the understanding of a case. For instance, metadata can reveal when documents were first created, who created them, and on what machine. It may also contain information about who may have contributed to revisions of documents, where they were stored, how and to whom they were distributed, who viewed them, and who did not, as well as other potentially useful information. In fact, dozens of pieces of hidden information may be available for review about each relevant file in a litigation matter if only the metadata were preserved during discovery. Yet whenever information is changed from one format to another prior to production, that metadata is also changed or even destroyed. So lawyers who have the technical savvy to ask for “native files” in their discovery requests, and can review that data in its native form, have the upper hand in gaining authority over the true nature of the evidence. “Native files” are bit-by-bit copies of electronically stored information and thus include all metadata. Data that has been transformed into other formats, such as paper, images, or PDFs will not have the potentially relevant metadata still associated with it.

3. Avoid Spoliation. In large part because of electronically stored information comprises "metadata," it is subject to inadvertent spoliation. The mere act of booting up a computer, viewing a file, or running a background system maintenance program can alter or destroy existing metadata associated with important files. Therefore, the preservation of data takes on an entirely new and more pervasive meaning when the object of discovery is native files rather than paper copies. It is especially important in such circumstances to take special care when preserving a client’s electronically stored information that is likely to be relevant to a matter. Likewise, it is important to be aggressive in requesting electronic information that is particularly vulnerable to spoliation and to enlist the courts’ help and explicit instruction in making sure electronic data is not spoiled before production.

4. Look for Data in Unlikely Locations. It is also important to consider the many places electronically stored information may reside, and to ask for it when crafting discovery requests. For instance, back up tapes and server hard drives and local workstation hard drives can be expected to contain information that may be relevant to a matter, but other locations as just as likely to be repositories of information. These might include external hard drives, or so-called thumb-drives or pen-drives which attach to workstations through standard USB ports. Also consider whether data has been written to CDs, DVDs, or floppy disks. iPods and other portable music devices may contains data of all kinds, as do Jaz and Zip drives, PCMCIA cards, Bernouli Drives, so-called “Memory sticks,” and “Smart Cards,” and so on. Be creative and thorough in your discovery requests.

5. Always Request/Review E-Mail. E-mail and Instant Messages (or IMs) are relatively recent forms of communications which do not have a paper-based equivalent. In other words, e-mail and IMs must be analyzed differently from other forms of communications such as paper documents, word processing files, and voice mail. E-mail and IM communications are short messages and are highly dependant on context for their meaning. That context may be entailed in the entire discussion from which the individual e-mail derives, or from the relationship between and among the people who are participating in the discussion. In any case, it is important to consider the meaning of individual e-mails from within their context, otherwise the e-mail, perhaps because it contain unattributed pronouns, slang, fragments, emoticons, and the like, may not have much if any meaning at all. Because of its informal, even casual nature, people often say in e-mail what they would never otherwise say in conversation or in formal communications. That makes e-mail a very fruitful area of discovery, but it also suggests that tone and context are as important in evaluating e-mail as word choice or format. E-mail should never be ignored in discovery.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Automated Document Review
CLE Course Handout

Techniques for Automated Document Review in Litigation

The Holy Grail of automated document review in litigation is to identify within a large collection of electronically stored information (ESI) ALL the information relevant to a legal matter that is not privileged or otherwise legally protected, and ONLY the information that is relevant. Using the traditional terms of automated litigation support, this goal is one of both *recall* and *precision*. Yet these are increasingly difficult tasks to accomplish accurately in a world where communications of all types and forms are captured and stored electronically as a consequence of standard business practices – especially those entailed by document retention requirements or by routine data back-ups. Not only are the resulting information collections so overwhelmingly voluminous as to offer no option to a machine-assisted review, but they are painfully redundant and chaotic, suggesting no ready organizing principle to guide the review. Legal practitioners are caught between these two uncomfortable realities.

One thing is clear, however. To the extent the automated systems are accurate, and can identify both relevant and irrelevant materials precisely, the review proceeds more quickly. This is not a trivial outcome, because a shortened review cycle can have significant strategic and economic benefits for legal professionals and for their clients.

Removing Duplicate Data

So what are the strategies available to legal professionals when separating the wheat from the chaff in automated document review? Especially when they are facing the challenge of reviewing data collections that frequently amount to hundreds of gigabytes or more? An obvious place to start is by analyzing the entire data collection at the outset for the purpose of identifying duplicate files.

Given that e-mail messages, for instance, are often sent to multiple recipients simultaneously, and are also frequently backed-up in multiple places, it is quite common to find that large sets of electronically stored

Automated Document Review
CLE Course Handout

information comprise many copies of the very same files. Yet, obviously, it makes no sense to review multiple copies of the same files for relevancy. One copy will do well enough. By eliminating file duplicates from the collection, the litigation team can often reduce the collection size quite significantly at the outset, while also preserving a good deal of equanimity among the reviewers.

De-duping, as it is called, is easily and accurately accomplished by comparing the *hash value* assigned to each and every file created or managed by a computer operating system. A *hash* is a digital signature, representing a string of data (i.e., any file) that identifies its contents. *Hashing* is the transformation of a string of data into a fixed-length value or key (often 128 bits) that represents the original string or file. Each hash value is unique. It is also useful, because it enables the operating system to find the file it needs much faster, by searching not for the entire file, but only for the unique hash identifier. And as a consequence of this universally employed file retrieval strategy, we can also be assured that if the hash values of two strings are identical in any collection of data, the two files represented by the data strings must also be identical. Identical files thus identified can then be safely culled down to a single copy preserved in the collection that is to be reviewed, a result that saves much time and human effort later on.

Segregating System Files

Since the data collection is most likely a complete bit-by-bit image of a hard drive or a restored Digital Linear Tape (DLT) back-up tape, a logical second step in reducing the quantity of data in the collection being reviewed is to segregate all the system files in the collection. System files are not business records. Rather, they comprise all the data required to run the machine on which they were originally loaded or created. These files would include the operating system files themselves, along with all related tables and internal utilities, peripheral drivers, software applications, communications, security, and network modules, as well as all other executable files of any kind, and also such associated items as document templates, clip art, sample pictures or sample audio files, help directories, error messages, and so on.

System files can also be readily and accurately identified by simply comparing their unique hash value against a hash table that lists known

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

system files. There could be very little reason, in the context of litigation, to want to review system files; they can almost always be set safely aside in the interests of further (and significantly) reducing the size of the collection that must be more closely analyzed by the review team for relevance or privilege.

Identifying Relevant Materials

To this point, the methods outlined for reducing the data set are straightforward and objective; not much doubt should remain that the data thus far segregated are irrelevant to the litigation or to furthering any understanding of the implied business practices under scrutiny. The next logical step, however, is to begin looking for files that are irrelevant to the litigation based on their content or on their contextual meaning, rather then their function. This is also a first step towards the subjective, a concept that begins to separate the reviewers from their machines.

In practice, however, many such files judged irrelevant by their content or contextual meaning would still include many items about which there would be little or no debate regarding that relevancy. For instance, they would surely include unsolicited e-mails – commonly referred to as "Spam" – as well as clearly personal information that is unrelated to the conduct of business: personal e-mail conversations and their attachments, for instance, or eBay receipts and related correspondence, family photos, jokes and cartoons, pushed news articles, solicited advertisements, saved HTML pages, and so on. And they would also include conversations that linguists and anthropologists call "phatic communion," intended not to convey information, but to establish or maintain relationships between and among people for purposes of purely social activities or to convey a sense of community, e.g., "Hi, how are you doing today?" or "How'd you like that game last night?" or "Welcome back!" and the like.

But that is not all that could likely be identified as irrelevant at this point in the process. What about the files created in the legitimate course of doing business which have nothing to do with the legal matter at hand or the investigation of interest? And how is that judgment to be made? In many instances it will require more than a cursory look at the data.

Automated Document Review
CLE Course Handout

So we have now reached a level of analysis that requires some subjection. Any automated solution to this level of analysis begins to require tools that can take deeper and more nuanced approaches to determining the content, and, ultimately, the true contextual meaning, of the remaining collected files. So what is the first next step?

Keyword Searching

The simplest approach to start with is keyword searching. It is common practice in automated document review to make an index of every word in the collection with pointers from the index to every instance of that word in the database. In that way reviewers can inquire about words that might be important to the facts in the case, or to the legal issues, or to persons involved, and thus identify both the documents that contain that word and those that do not. Typically, these keywords can also be concatenated with Boolean operators (*e.g., and, or, not*) to ascertain where two or more words of interest may appear together or in close proximity – or perhaps to ascertain the opposite.

Keyword searching can thus be helpful, particularly in the context of litigation where subpoenas and document requests sometimes even refer to specific keywords of interest. But it can also be very imprecise and misleading. For one thing, people do not employ language consistently. For another, even individuals use language differently depending on the form of their communication and the circumstances. In a formal report, an aeronautical engineer might refer consistently to ***aircraft*** but in her e-mail she refers to ***plane*** or ***copter*** or ***the beast*** when meaning the same thing. One way of addressing this is to throw a thesaurus or various kinds of dictionaries (*e.g. collegiate, regional, colloquial, technical*) at the problem and by incorporating them into the keyword searching software with cross-referencing strategies.

But even that can only goes so far. In this age of e-mail and IM much of our written communications consist of abbreviations, misspellings, and other shortcuts. And what of pronouns in such communications? They seldom have clear antecedents. Context is crucial in these kinds of communications. An individual e-mail may be so obscure by itself as to have no discernable meaning whatsoever when taken out of the context of the conversation that prompted it.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

And then there is the seeming illogic of Boolean operators themselves. What do we mean when we insert the word ***or*** between two search terms? Is it exclusive, as in the choice on a menu between ***hash browns*** or ***french fries***? Or is it inclusive, meaning that when searching for ***aircraft*** or ***copter*** you get a positive result when BOTH words appear in a file? Would the waiter think us confused if, when in response to the question of which potatoes we wanted, we answered: *Both*?

So for a host of reasons, keyword searching is both imprecise and incomplete. As a search strategy for large or complex discovery tasks, it is a mere baby step. Clearly there has to be something better.

Linguistic Clustering

One search strategy that represents a clear logical step beyond keyword searching is the analysis and subsequent clustering of files that have similar topics in them, even when the words used to represent those topics are not identical. This is done through various grammatical, semantic, and even punctuation algorithms designed by combination to detect topics rather than just individual keywords. When files are determined to be about the same or similar topics, they are clustered together, and usually displayed on the computer monitor by the search engine in some kind of graphical relationship that facilitates reviewing similar documents together. That way, in reviewing a small number of files that appear in a single cluster, reviewers can make a judgment about whether the whole set is relevant to the matter under investigation. This represents a significant efficiency, and an important step beyond simple keyword searching.

The limitations of clustering, however, are still significant in data collections comprising large amounts of informal communications because those files frequently do not contain the number of words sufficient for the algorithms to identify any topics at all. Moreover, when the clustering tools do identify topics and cluster individual files together, the files cannot then also be clustered with other files comprising other topics when the document in question actually does address more than one distinct topic, as is common in formal communications. In other words, traditional clustering strategies employed in document review are exclusive, and files cannot be a part of more than one cluster. Moreover, that determination is based entirely on a

Automated Document Review
CLE Course Handout

statistical analysis of the files by topic with no regard as to whether those similarities are either salient or whether they are trivial. The topics that form the basis for the clusters are arbitrary. And in the largest collections, the clusters themselves can be so large as to offer little benefit during review. So while clustering is another logical step toward more precise searching strategies, it leaves too much to chance to be relied upon alone if better strategies are available.

Vector Space Modeling

And better strategies are available. For one, there are more comprehensive ways to map the complex relationships between and among files in a large collection than simply creating arbitrary clusters. Vector Space Modeling (VSM) is a concept that first came into favor in the early 1970s and it has provided some additional guidance in automated document review even to this day. It is based on building vectors that describe the relationships between each search query and each file in the collection. Each vector, by its magnitude and direction then maps to other files that are closest to it in relation to the same *feature* as emphasized by the search query. Each file thus becomes a compilation of *features* that place it in a multi-dimensional construct. That construct can be realized in a graphical display depicting all the relationships as vector lines between and among separate files. This graphical display can then provide some guidance to the reviewers on which files are related to one another within the parameters of a search inquiry with the result that the review is further focused and efficient.

Vector Space Modeling is especially useful in large collections that might overwhelm clustering models by the sheer number and size of the clusters. A vector can be construed to have any length, and thus scales easily to match any sized collection. The result is much better recall properties than either keyword searching or clustering. But its strength as a searching strategy is also its weakness. By connecting all the files in a collection according to their features into a single multi-dimensional construct, the precision of the search is compromised. Where is the reviewer supposed to start when the files are organized by their similarity rather than by their context or their meaning?

Many business documents, for instance, are similar in form but have no logical relationship to one another in practice. In fact, in business

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

enterprises, many documents *are* forms, and will always appear similar, yet when filled out with particulars, might pertain to entirely unrelated circumstances. Most of those circumstances are probably irrelevant to the litigation at hand. We need to have a way of determining not just how documents are similar, but how they are related to a specific subject of interest if we expect to raise the degree of precision in automated document review.

Latent Semantic Indexing

One way of enhancing the precision of vector analysis is by adding a semantic component that expands the modeling to include concepts rather than just keywords or topic clusters. The theory is that unstructured files comprise *latent* concepts that are not readily recognized and remain hidden until a more precise lexicon is developed out of the whole collection.

This theory of Latent Semantic Indexing (LSI) has been put in practice in several different ways, but in general multiple concepts are extracted from the data collections through a statistical semantic analysis of each file. These concepts then form a dictionary (lexicon) for the collection that can be weighted for both frequency of occurrence and relevance. At that point each file in the collection is compared to the concepts list, and it is assigned a *fingerprint* (or value) that uniquely defines the file according to those criteria. Searches can then be conducted by requesting files that are statistically similar, i.e. that have similar fingerprints, under the presumption they will be not just similar but conceptually related as well. The precision of any specific search is thus greatly enhanced.

And concept searching has the added benefit of simplifying searching for the reviewers. For instance, queries do not have to be strictly formatted as is required with term searches that include Boolean operators, but can be written in more natural language. In addition, the queries can be more comprehensive and generalized, extending even to reviewers offering up entire documents as exemplars of the kinds of subject matter being sought. And more generally, of course, concept searches can be conducted by non-technical reviewers, those who might otherwise struggle with more technical searches involving technical language.

Automated Document Review
CLE Course Handout

So, in review, by looking back at the continuum of search strategies so far, we can see they have morphed from keyword searches to topical searches to file feature searches to searching by concept. All of these approaches can be helpful, and each is better by virtue of building on the benefits of the previous. Nevertheless, each of these strategies derives from the same starting point; each is based on some higher and evolving form of indexing – creating lists of individual words and then noting their interconnections or frequencies or semantic relationships. In other words, by such schemes the reviewers have to know what they are looking for before they can find it.

But what if they don't know? What if there is something in the data that is exculpatory, but the reviewers are not looking for it? What if there is something actionable in the data, but it is unrelated to the current litigation? Certainly it would be extremely valuable to identify this kind of data, before any data are produced. But how are reviewers to find these important pieces of information if they cannot inquire about them? In other words, how can the reviewers know what they don't know?

Neural Networking

The answer lies in the old adage: "The more I know, the more I realize I don't know." A search strategy that learns as it works would be able to build new inquiries from any knowledge gained from the results of previous inquiries. In theory, it wouldn't necessary matter whether it were the computing system or the reviewer that was doing the learning, so long as the knowledge gained during the review were incorporated into back into the algorithms of the analysis. In that way the process would address the problem of "not knowing what we don't know" by constantly tweaking the search criteria in concert with the developing understanding the reviewers or the system have of the entire data collection. Such a strategy allows previously unconsidered and unrecognized patterns to emerge from the collection.

Artificial Neural Networking (ANN) systems operate in exactly this way. They incorporate an information processing paradigm that is inspired by the way biological systems process information. Learning in biological systems involves small and continuous adjustments to the synaptic connections that exist between the neurons of the brain. Neural networks mimic that

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

biological process by implementing large numbers of highly interconnected processing elements that work in parallel to solve specific problems.

The key element of this paradigm is the structure of the information processing system. Neural networks are designed to learn by example and are particularly good at solving problems dependant on experience, such as pattern recognition or data classification. The networks must first be trained, however, to associate certain outputs with given input patterns. The power of neural networks then is revealed when it finds a pattern that has no output associated with a given input. In such instances, the network gives the output that corresponds to a taught input pattern that is least different from the given pattern. And so it "learns" something about the data.

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computing techniques. A trained neural network can be thought of as building expertise in the category of information it has been given to analyze. This expertise can then be used to inquire into new domains of interest and even to answer highly theoretical questions.

Since neural networks rely on training, they require the reviewers, in the context of document review, to do some upfront work before any search tool based on this paradigm will deliver meaningful results. But that also means that neural network algorithms can be adopted to learn or recognize reviewer preferences or points of view even as those preferences or points of view change over time. This can be very powerful in automated document review both because reviewers typically have different areas of expertise, and because legal issues and litigation strategies are subject to constant evolution as the matter progresses.

Ontologies

So how can the preferences or interests of the reviewers be made to inform the search strategies in the same way that what is learned about the data collection is brought to bear on the same strategies through neural networking? Can natural language be reduced to mathematical terms so that machines can understand it and then apply it back to a collection of

Automated Document Review
CLE Course Handout

data comprising natural language statements in a large collection of unstructured files? Can all of this be put together into a state of the art searching mechanism for automated document review?

Scotty, the engineer on the Starship Enterprise, used to talk to his on-board computer with the assurance that the computer would speak back to him coherently, in his own language, and with the correct answer to his question. Wouldn't it be nice if reviewers could simply ask the automated system to present all the relevant data with the assurance that the results have a high likelihood of being correct and complete? Accomplishing this means coupling the subtlety and flexibility of natural language with the blinding processing speeds and enormous memory capacities of a computer.

Today this goal is most nearly accomplished by an automated review strategy that incorporates ontologies into all of the other strategies we have previously discussed.

An ontology consists of a (frequently large and complex) arrangement of discrete and hierarchical words, phrases and search terms that are related to an area of inquiry. Ontologies are thus three-dimensional approaches to organizing and understanding the data collection, and are much more powerful and versatile than any two-dimensional index- or concept-based strategy. The legal team can establish the level of precision they want from an ontology (based on criteria of their own choosing that would, nevertheless, include at least *time, cost*, and *risk*) which can be iteratively refined until the team decides that it is precise enough for their needs. Much of the power and effectiveness of using ontological approaches to automated review comes from the experience and expertise of the people developing the ontology and from the learned patterns of data relationships uncovered by the neural networking algorithms.

Any realistic ontology is going to be quite large and complex. This is especially true in the context of litigation where the issues of interest can be quite abstract. For instance, when reviewing data for ***Anti-Trust Language***, the ontology may in turn be built out of other sub-concepts, such as ***Competition Language*** and ***Market Share Language***. Only after drilling down into deeper levels of the analysis do reviewers actually reach the terms that make up the over-arching concept, where the right words reside within the right context to suggest they will need to be closely

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

considered as directly relevant to the issue of "Is this an anti-trust violation?"

An ontology such as this anti-trust example will likely contain a huge number of terms. These terms include synonyms, abbreviations, slang and technical terms specific to a particular organization or situation. An ontology may also be tailored to reflect idiosyncrasies such as spelling mistakes in the data and unusual terminology or phrases or, in the case data collections from multi-national corporations, the inclusion of more than one language. Ideally, an ontology should act as an extension of the legal team's evolving understanding of the matter. To get to this point, sample data is typically examined, and legal and subject matter experts may be interviewed. The ontology is repeatedly tested against the data set and then adjusted (or *tuned*) until the files it identifies as responsive meet the general standards of desired accuracy.

Once the effort has been put into developing a good ontology, the legal team can leverage the benefit from its use by realizing not just more focused review, but by having revealed related patterns of communications on subjects of interest. They can also use the ontology for investigating the data, and formulating very powerful search queries that would be impractically large and complex to build or conduct using only the search strategies we have discussed previously. Once again, by building on the search strategies that have come before, gradually more effective and powerful ontology-based searching becomes possible. Moreover, as the search tools reveal a deeper understanding of the data, this knowledge can also be leveraged across matters within an organization, perhaps to assist in patterns of litigation involving the same data, the same departmental or group behaviors, or the same legal issues, but perhaps involving different plaintiffs or jurisdictions . The automated document review gets better and better recall and precision results over time precisely because the systems are established so as to never remain static. Improving results are part of the very process.

Ontologies Capture Point of View

Moreover, ontologies can be readily developed to accommodate differing or evolving points of view, as the neural networking strategies before them predict. For example, the concepts of good and bad weather can be very different, depending on the observer's point of view. This table illustrates

cataphora
Automated Document Review
CLE Course Handout

how different people might take different views of what is good weather and what is bad weather.

	TRAVELER	FARMER	SKIER
GOOD WEATHER	Sunshine	Rain	Snow
	Dry	Cool	Cold
	Warm	Still	Still
BAD WEATHER	Rain	Dry	Rain
	Snow	Hot	High winds
	Still	High winds	Warm

A traveler may hope for warm, dry weather with plenty of sunshine, and would regard rain or snow as a bad thing. However, for a farmer, the term *rain* might be a GOOD WEATHER concept. Or a skier might consider *snow* to be a GOOD WEATHER concept. In other words, the way a concept is categorized depends very much on the point of view of a given observer. Also, this viewpoint may also change over time. For instance, during the growing season the farmer may hope for rain, but during harvest, he would prefer dry weather and sunshine.

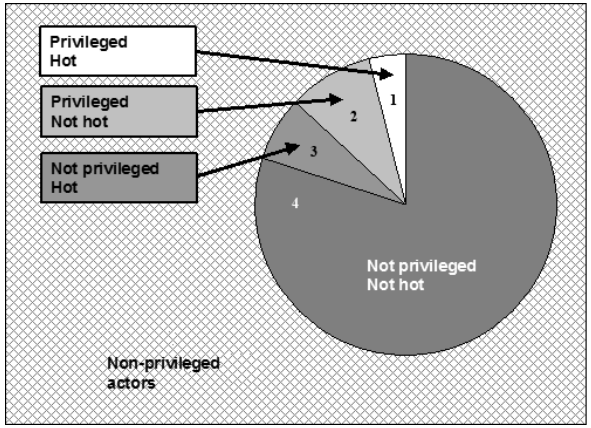
Ontologies are ideally suited to encapsulating differing viewpoints such as these into searching strategies, and they are therefore a powerful technique in automated document review. It is important to realize, however, that an ontology that applies in one situation may not be completely correct in another, even if the two matters seem to be highly related. This is where linguists and legal experts or technical experts might be brought in to play a role and to make sure that an ontology accurately reflects the specific situation in any given matter.

Multiple Ontologies Focus Review

Ontologies are also interdependent, and not exclusive like traditional clustering strategies. They become additionally powerful searching strategies when employed together. Using multiple ontologies can be a very effective searching strategy for identifying the most important documents and then prioritizing them for review. The reviewers are thus directed to the potentially most important documents at the very outset of the review process. An example of this is shown in the diagram below. The entire large rectangle represents all of the data, while the circle represents those

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

documents that reference privileged actors, identified as anyone sending or receiving privileged information.



Not all of the information sent or received by privileged actors is privileged, however. And not all of the information referenced by them is relevant even if it is not privileged. Therefore, in addition to applying an ontology identifying the privileged information, the reviewers have applied ontologies to identify relevant information, as well as information within the relevant category that is most likely to be *hot*, or of particular significance. The result is that the total set of information sent or received by the privileged actors can be subdivided into narrower segments:

1. Both privileged language and hot language
2. Privileged language but not hot language
3. Hot language but not privileged language
4. Neither privileged language nor hot language

The privileged and hot documents will get the highest priority for review, being reviewed first and perhaps being passed to more experienced

cataphora
Automated Document Review
CLE Course Handout

reviewers. The documents with neither privileged nor hot language will have the lowest priority. Typically, as in this example, the highest priority categories are much smaller than the lowest priority ones. Based on this, resources can be focused on a much smaller set of documents, saving both time and cost.

Developing an Ontology for a Given Matter

The basis of any ontology is real-world information about the area of interest. Attempting to develop a general ontology without reference to the specifics of the matter will invariably result in two kinds of problems. Either it would include terms that do not mean what the reviewers or legal team would expect, or it would entail the omission of terms that are used in the matter, but which would not be included in any general, unspecific ontology.

To address this, understanding of the terms that are relevant to a particular matter may be obtained from documents such as memos, case strategy information, primary actor list (custodian list), case theories, discovery requests, subpoenas, lists of prior produced data, and so forth. The linguists developing the ontology may also meet with and interview topic experts and lead attorneys who can provide insight into the theory of the case. Linguists then develop an ontology and test it against a sample data set. The results are examined for accuracy, and the ontology may be refined to improve results as required. This process can be repeated until the ontology performs with the desired standard of accuracy.

Detecting tone

Ontologies can even be used to detect the tone of a written communication such as an e-mail message. Messages that contain language that is angry or fearful, for example, might be of particular interest in pinpointing important potential evidence. An e-mail containing language such as: "It's hopeless. We have to let the client know we can't deliver on this contract. There are too many risks of defects" might be a tired, frustrated employee letting off steam, or a potential whistle-blower pointing out a real problem. A further example might be a message along the lines of: "If the auditors find real problems, this could be a criminal issue. You really need to look into it personally." Such "friendly advice" can remove the defense of ignorance on the part of the recipient.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Ontologies are Built on Other Search Strategies

Ontologies are particularly powerful when they are combined with other search strategies, such as those we have discussed previously. For example, clustering may be used to expand the results obtained by means of an ontology.

Clustering identifies documents that are in some way similar to each other. Some examples of possible clustering criteria include:

- Content – documents that share syntactic features;
- Meta-data – e.g. document type or date;
- Business criteria – e.g. documents created within a certain department;
- Proprietary – other criteria that have been identified as leading to effective clustering.

Clustering serves two purposes. The first is that it can work in tandem with the ontology to categorize documents that the ontology has not yet categorized. The second is that the ontology and the clustering can validate each other. Most documents within a cluster should be categorized in an identical way by the ontology. If the results of ontology categorization and clustering align well, this provides a strong indication that the results are valid. On the other hand, it might be that clustering and the ontology seem at cross purposes – with documents from a cluster falling into multiple categories. In that case, either the ontology or the clustering method need to be further refined.

Developing an ontology is also typically combined with the expansion of terms that may be of interest – a kind of variation on the theme of keyword searching. As an example of the many different terms that might be used for a single concept, here are a number of ways in which the term "board meeting" might be expressed:

- board meeting
- board meetings
- board meeting
- board mtg
- board mtgs
- boards meetings
- board's meetings

Automated Document Review
CLE Course Handout

- boards mtg
- board's mtg
- meeting of the board
- meeting of board
- mtg of board
- mtg of the board
- meetings of the board
- mtgs of the board
- meetings of the boards
- mtgs of the boards
- meeting of the boards
- mtg of the boards

Such expansion of terms can also encompass foreign languages to handle the case, for example, of a multi-national corporation whose employees communicate in French and German, as well as in English.

Once their searching strategies have reached the level of ontology, both those that are basic building blocks for any file segregation, and well as ontologies developed for special purposes, perhaps including special language components or carefully devised legal strategies, we have come close to a place when the legal team can have total authority over the data collection. At that point automated document review has reached a level of recall and precision that is quite close to that Holy Grail goal we described at the outset of this paper.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

SERVICE LEVEL AGREEMENT

This Service Level Agreement is executed as of this _____ by and between VENDOR and Customer. This Amendment amends that certain Master Hosting and Services Agreement between the parties dated as of _____ ("**Agreement**"). Capitalized terms not otherwise defined in this Amendment shall have the meanings given them in the Agreement. Except as expressly amended as set forth herein, the Agreement shall remain unchanged and in full force and effect.

1. DEFINITIONS

"Aggregate Monthly Case Administrator Fees" shall mean the aggregate monthly fees paid by Customer for Dedicated Case Administrators.

"**Available**" shall mean that the Introspect System is accessible by Customer's Named Users.

"**Availability**" shall mean that percentage of time, as measured monthly, during which the Introspect System is Available. Availability will be expressed as a percentage calculated in accordance with the following formula:

Availability % = 100% x (Scheduled Uptime Minutes – Unscheduled Outage Minutes) / (Scheduled Uptime Minutes)

"**Monthly Hosting Fees**" shall mean both the monthly Hosting Storage Fees and the monthly Named User Fees.

"**Navigation Available**" shall mean that the Introspect System is meeting the navigation time requirements set forth in Section 2.2 below.

"**Navigation Availability**" shall mean that percentage of time, as measured monthly, during which the Introspect System is Navigation Available. Availability will be expressed as a percentage calculated in accordance with the following formula:

Navigation Availability % = 100% x (Scheduled Uptime Minutes – Unscheduled Navigation Minutes) / (Scheduled Uptime Minutes)

"Regular Business Hours" shall mean 8:00 a.m. EST and 8:00 p.m. EST (7 days per week)

"Scheduled Maintenance" shall mean scheduled maintenance performed in accordance with Section 4.2 of Schedule I of the Agreement, provided that scheduled maintenance shall not occur during the hours of 8:00 a.m. EST to 12:00 a.m. EST (7 days a week) without Customer's prior written consent.

"Scheduled Uptime Minutes" shall mean the difference between (i) total minutes in the applicable month and (ii) minutes in that month in which the Hosting System is not Available due to Scheduled Maintenance.

"Service Credit Request" shall mean a written notice from Customer in which Customer notifies VENDOR of a failure of one or more of the Service Levels set forth in Sections 2.1 through 2.4 below, including (i) a reasonably detailed description regarding the nature of the failure, (ii) the date and time on which Customer first became aware of such failure and (iii) the date and time upon which the failure commenced (if and to the extent known by Customer).

"Total Monthly Fees" shall mean the total dollar amount that VENDOR bills Customer in a given month for all services associated with Customer's usage of the Introspect system that month. (Does not include Electronic Data Discovery Fees)

"Unscheduled Outage Minutes" means all those minutes in which the Introspect System is not Available, excluding (i) minutes arising from Scheduled Maintenance and (ii) minutes arising from any of the reasons specified in Section 2.1.5 below. Unscheduled Outage Minutes shall be counted from the time that Customer notifies VENDOR of an outage to the time that a VENDOR case administrator notifies Customer that the outage is resolved; provided, however, that if Customer objects within ten (10) minutes of receipt of such notification on the grounds that the system is still not Available, and VENDOR verifies the same, then the Unscheduled Outage Minutes shall be deemed to resume at the time that Customer does object.

"Unscheduled Navigation Minutes" means all those minutes in which the Introspect System is not Navigation Available, excluding (i) minutes arising from Scheduled Maintenance and (ii) minutes arising from any of the reasons specified in Section 2.1.5 below. Unscheduled Navigation Minutes shall be counted from the time that Customer notifies VENDOR of navigation problems to the time that a VENDOR case administrator notifies Customer that the navigation problem is resolved; provided, however, that if Customer objects within ten (10) minutes of receipt of such notification on the grounds that the system is still not Navigation Available, and VENDOR verifies the same, then the Unscheduled Navigation Minutes shall be deemed to resume at the time that Customer does object.

2. SERVICE LEVELS AND CREDITS

2.1 Uptime Service Level

2.1.1 Uptime Service Level. VENDOR agrees that the monthly Availability of the Introspect System shall be equal to or greater than 99.7% (the "**Uptime Service Level"**).

2.1.2 Uptime Service Level Credits. For each month in which there is a failure to meet the Uptime Service Level, Customer shall receive a Service Level Credit for such month equal to an amount determined in accordance with the following schedule:

Availability %	Service Level Credit
Greater than or equal to 99.7%	None
Less than 99.7% but greater than or equal to 97.0%	5% of Total (or Hosting) Monthly Fees for applicable month
Less than 97% but greater than or equal to 95%	7.5% of Total (or Hosting) Monthly Fees for applicable month
Less than 95%	10% of Total (or Hosting) Monthly Fees for applicable month

2.1.4 Exceptions. Notwithstanding anything herein to the contrary, minutes in which the Introspect System is not Available due to any of the following reasons shall not be considered Unscheduled Outage Minutes for purposes of the calculation of Availability:

(a) Circumstances beyond VENDOR' reasonable control, including, but not limited to, acts of war, acts of God, earthquake, flood, embargo, riot, sabotage, power outages, labor shortage or dispute, governmental act, OR failure of the Internet; provided that VENDOR gives Customer prompt notice of such cause and uses its reasonable commercial efforts to promptly correct such failure or delay in performance;

(b) Failure of hardware, software or other equipment provided by Customer and used in connection with the Services;

(c) denial of service issues outside the direct control of VENDOR;

(d) Scheduled maintenance and upgrades;

SAMPLE

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

(e) Acts or omissions by VENDOR when done at the request of Customer;

(f) Outage caused by Customer electing to not have VENDOR add additional hardware recommended by VENDOR to support increased usage of Customer's web site(s); or

(g) Customer not providing information or approval that is necessary to bring a system back online or release a system. (e.g. provide system fields in order to allow users on the system before release).

2.2 Navigation Service Level.

2.2.1 Customer navigation from document to document or page to page during review will execute in five (5) seconds or less, assuming that the file type is a TIFF and the size of the document or page is less than 200kb. VENDOR will set-up a folder under a shared area in which Fannie and VENDOR will use to validate that document to document or page to page navigation is within five (5) second timeframe ("Validation Area"). Validation needs to be made at both the VENDOR site and the CUSTOMER site. If navigation times are greater than or equal to five (5) seconds, and this continues for more than one (1) hour, all minutes, until the issue is corrected, shall be considered "Unscheduled Navigation Minutes." If VENDOR is unable to validate document to document and/or page to page navigation times in the Validation Area, but Customer continues to experience document to document and/or page to page navigation times greater than or equal to five (5) seconds in the Review Area (assuming that the file type is a TIFF and the size of the document or page is less than 200kb), one half (1/2) of the minutes counted from the first reported instance of slow navigation time until the issue is corrected to Customer's satisfaction shall be considered "Unscheduled Navigation Minutes."

2.2.2 Uptime Service Level Credits (Navigation). For each month in which there is a failure to meet the navigation Service Level set forth in Section 2.1.1 above, Customer shall receive a Service Level Credit for such month equal to an amount determined in accordance with the following schedule:

Navigation Availability %	Service Level Credit
Greater than or equal to 99.7%	None
Less than 99.7% but greater than or equal to 97.0%	5% of Monthly Hosting Fees for applicable month
Less than 97% but greater than or equal to 95%	7.5% of Monthly Hosting Fees for applicable month
Less than 95%	10% of Monthly Hosting Fees for applicable month

2.3 Response Time Service Level.

2.3.1 Response Time Service Level. So long as Customer continues to maintain at least XXX Dedicated Case Administrators, VENDOR agrees that all requests made to the dedicated telephone support line and/or to the email address during Regular Business Hours shall be responded to within twenty (20) minutes (the "**Response Time Service Level**").

As part of the "Response Time Service Level" VENDOR agrees to provide further information every 3 hours business hours on unscheduled outage minutes until outage is resolved. VENDOR also agrees to provide further information within 24 hours for all other requests.

2.3.2 Uptime Service Level Credits. For each month in which there is a failure to meet the Response Time Service Level, Customer shall receive a Service Level Credit for such month equal to an amount determined in accordance with the following schedule:

Availability %	Service Level Credit
One (1) failure in the month	2.5% of the Aggregate Monthly Case Administrator Fees for such month
Two (2) failures in the month	5% of the Aggregate Monthly Case Administrator Fees for such month
Three (3) failures in the month	7.5% of the Aggregate Monthly Case Administrator Fees for such month
Four (4) or more failures in the month	10% of the Aggregate Monthly Case Administrator Fees for such month

2.4 Deliverables Service Levels and Credit. In the event VENDOR fails to meet a mutually agreed upon deliverable date for the completion of specified Services relating to data loading, data production and/or report publication ("**Production Services**"), and provided all Customer and 3rd party dependencies are met, all assumptions are correct and delivery is within control of VENDOR (e.g. FedEx lost package), then (a) the fees associated with the delayed Production Services shall be reduced by ten-percent (10%) and (b) VENDOR shall promptly provide Customer with a new deliverable date for the completion of such Production Services.

2.5 Access Service Level and Credit. From time to time Customer will need to grant access to documents to additional agents and other external parties. Customer will define, document and provide appropriate security / access levels to VENDOR. VENDOR guarantees that the appropriate security / access levels will be implemented and monitored. In the event any Customer agents or external parties are given inappropriate access to fields or documents that are explicitly excluded in Customer's requirements documents, Customer shall receive a Service Level Credit of Two Thousand Dollars ($2,000) for the first occurrence and Five Thousand Dollars ($5,000) for each occurrence thereafter throughout the term of this Amendment.

3. REPORTING AND CONFIRMATION

In order to receive any Service Level Credits described in Sections 2.1.2, 2.2.2, 2.3.2, 2.4 and 2.5, or to exercise the termination right under Section 2.1.4, Customer must notify VENDOR by submitting a Service Credit Request within seven (7) days of each instance of non-compliance. Failure to comply with this requirement will forfeit Customer's right to receive a Service Level Credit for that instance. VENDOR will acknowledge receipt of a Service Credit Request via email no later than the next business day after such receipt and will review all requests within fourteen (14) days after such receipt. Customer will be notified via email upon resolution of the request. If a Service Credit Request is approved, VENDOR will issue the applicable Service Level Credit to Customer's account. The Service Credit will appear on Customer's invoice within two (2) billing cycles.

4. EXCLUSIVE REMEDY

The Service Level Credits specified in Sections 2.1.2, 2.2.2, 2.3.2, 2.4 and 2.5 shall be Customer's sole and exclusive remedies for a failure by VENDOR to meet the service levels specified. For the avoidance of doubt, the preceding sentence shall not limit Customer's rights of termination under the Master Services Agreement.

SAMPLE

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Patrick L. Oot
Director of Electronic Discovery and Senior Counsel
Verizon Legal

1515 N. Courthouse Road
Suite 500
Arlington, VA 22201-2909

Phone: (703) 351 - 3084
Fax: (703) 351 - 3653
patrick.l.oot@verizon.com

February 10, 2006

To Whom It May Concern:

Verizon invites your firm to submit a proposal to provide electronic discovery services. Although this combined request for information and request for proposal (RFP) is not matter-specific, Verizon intends to establish a list of two to three preferred eDiscovery vendors to provide:

- Electronic file processing;
- Online document database hosting;
- Printing;
- Scanning;
- Imaging Electronic Files;
- Electronic Bates Stamping; and
- Building Electronic Document Production Databases.

Feel free to submit bids to provide some or all of these services. Verizon seeks to adopt a preferred vendor list for use by in-house counsel, outside law firms, and all Verizon business units (including the recently acquired MCI). Vendors that provide all of these services will have a significant advantage in being selected as a preferred vendor.

Attached, you will find an Excel spreadsheet with a series of questions about your firm's capabilities, background, and pricing. Please be specific in your responses. Should a question call for a quantitative response, please provide a numerical answer; when a question calls for an affirmative or negative answer, please respond appropriately. Verizon views long narrative answers to such questions as non-responsive and will rate such responses poorly. Because Verizon is a long-time and experienced consumer of eDiscovery services, we seek short, concise, well-tailored responses, not gratuitous "catch all" answers. Please craft your responses accordingly.

Please use the attached Excel spreadsheet as a template for your responses. You may submit your responses in the empty columns in the spreadsheet to the right of each question. If you do not plan on bidding, please notify me via e-mail as soon as possible. The deadline for submitting a response to this RFP is 8:00 a.m. eastern time on February 20, 2006. Should you have any specific questions, please feel free to e-mail me. However, I will be unavailable to take unsolicited meetings or phone calls prior to February 20, 2006.

Sincerely,

Patrick L. Oot
Director of Electronic Discovery & Senior Counsel
Verizon Legal

NOTICE: Information contained in this document is considered proprietary and confidential to Verizon, unauthorized disclosure of information contained herein or collusive bidding may result in rejection of your proposal and legal action.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Verizon e-Discovery Questionnaire

Basic Processing
Briefly list methods for receiving data from client (secure FTP, media, etc.).
What is the vendor's daily file transfer capacity from each form of media listed above?
Does the vendor have any new or unique method to acquire data from client?
Describe the process and software used for native-file data extraction.
Identify database software used for processing native files.
Describe the process for extracting and preserving metadata.
Describe the process for extracting and preserving text.
Does the vendor possess the ability to image only specified documents, not the entire collection?
Identify types of loose and mail files vendor can process.
Describe in what format the post-processed data is provided (load-ready file, etc.).
Provide daily per gigabyte processing capacity for Lotus Notes, Outlook, and compressed file archives.
Provide daily per gigabyte processing capacity for loose files.
Provide the number and locations of processing servers.
Describe procedures for responding to exception files.
Can the vendor provide a list of exception files prior to resolution attempt?
Does the vendor have the ability to crack passwords?
Can the vendor provide a list of password files prior to resolution attempt?
Does the vendor eradicate viruses?
Name database structures and litigation software used for exporting.
Can the vendor import scanned image files into the database structure?
Can the vendor OCR scanned images? If so, what OCR engine(s) does the vendor use?
Are document relationships maintained when data is processed?

Deduplication
Can the vendor deduplicate files?
Can the vendor deduplicate files on client-provided custom criteria?
Can the vendor deduplicate files both within and across custodians?
Can the vendor deduplicate near duplicates?
Can the vendor create a placeholder record in the database for duplicate files?

Pre-Culling
Does the vendor have the ability to pre-cull data using keyword search terms before processing the data?

Review Software: General
Identify review software used.
Can the review database be hosted online?
Can the client host a review database internally?
Identify the minimum and recommended server requirements to host a review database internally.
Identify the minimum and recommended system requirements to use review software on a PC.

Review Software: Coding Functionality
Can the client create custom data fields and values for coding on the fly without assistance from vendor?
Can the client create custom coding forms on the fly without assistance from vendor?
Does the review tool allow for a native file review without images?
Does the review tool allow users to redact files?
Can the review tool redact the native file?
Does the review tool offer multi-screen functionality?
Does the review tool offer left or right click speed coding?
Provide file formats supported by the review software.
Can a reviewer download and open a file in its native application?
Can the client create images without vendor interaction?
Can the client bates stamp images for production in the review tool without vendor interaction?
Can a reviewer "print to file" branded images to a local drive; if so, in what format?

Review Software: Threading
Can the vendor organize data for review by responsive threads?
Can the vendor place threads in coding order, longest part of the thread first?

Review Software: Reporting
Can the client create custom data reports and query on the fly without assistance from the vendor?
Can a user save database reports?
List file formats to which the review software can export data reports.
Does the software monitor reviewer activity in the database?
Does the software keep a chain of review record, *i.e* ., who coded a record, what was coded, when that record was coded, and whether it was changed?

Review Software: Searching
Identify the search engine used by the review software.
Provide the maximum number of search terms that can run against a database simultaneously.
Can a user upload a search list, or does a user have to type search terms manually?
Can search results be foldered for review automatically or does vendor have to folder search results manually?
Can user searches be saved?
Can search results be saved in folders or lists?
If the search engine employs advanced search and retrieval technologies, identify which (*e.g.* , context, concept, fuzzy, taxonomies, ontologies, etc.).
If the search engine employs advanced filtering methods, identify which.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Can the software search document relationships?
Can the software search e-mail strings?

Training
Does the vendor provide a user manual?
Does the vendor provide training?

Hosting
Describe your storage infrastructure for hosting a litigation review database.
What backbone database does the vendor use to host a review database?
Describe bandwidth allotments and load balancing.
Describe your server infrastructure.
What is the maximum number of users that have actively coded data in a single database simultaneously?
Describe methods of user access to the database (the Internet, Citrix, Special plug-in, HTTP client, etc).
How is the hosted system backed up?
Describe what hardware and software solutions are in place for disaster recovery.
What are the estimated bandwidth requirements for review scaled at 25 reviewers, 50 reviewers, 200 reviewers?
What are the minimum recommended server requirements if hosted internally?
Are there firewall issues accessing a vendor hosted system; if so, what are they?
Where is the data hosted? Is it hosted redundantly?
On what type of drive arrays are the databases hosted?
What are the vendor's uptime statistics? Are they audited?
At what rate can the vendor host pre-processed data provided on external drives or via FTP (in gigabytes per hour)?

Production
Identify which file formats the vendor supports for production to opposing party (Concordance, Summation, etc.).
Can the vendor produce a database with native files?
Does the vendor use an MD5 hash to ensure authenticity post-production?
Does the vendor offer bates stamping for image-based productions?
Does the vendor have any capacity limitations for production?
What is the vendor's throughput for imaging, bates stamping, and building a load ready database to produce to opposing party (files per day or gigabytes per day)?
What types of media can the vendor provide for production?

Consulting
Does the vendor charge for any services related to processing, hosting, review or production?
If so, for which tasks does the vendor charge separately?
Does the vendor have the capability to acquire data onsite from client servers or from individual PCs?
What does the vendor charge for onsite data acquisition?

Security
Which data carrier provides service to your systems?
Provide bandwidth available for hosting, secure FTP file transfers, etc.
How is access restricted to hosted data?
Describe the vendor's security infrastructure.
Describe the vendor's security at their physical facilities.

Staffing & Relationship Management
How many employees does the vendor have?
How many project managers does the vendor employ?
How many data technicians does the vendor employ?
Where are the vendor's offices located?
Do all office locations have production and processing facilities?
Describe how the vendor manages its client relationship with staffing.
Does the vendor subcontract or use temporary staff; if yes, for which tasks?
Does the vendor run a conflicts check?
Please provide resumes of the principle sales liaison, the principle project manager, the principle security officer, and the principle director of IT that would be dealing with client.
Under what terms can client terminate a contract with the vendor?
How does the vendor resolve contract disputes?
Please provide your taxpayer ID and financial statements for the last two years.
Has the vendor or any of its affiliates been a party to litigation?
If so, are any of these lawsuits with current or former clients?
Please provide past cases and performance on those cases.
Please provide references from at least three law firms AND two fortune 500 companies AND one government agency.
Does or has the vendor ever outsourced to third parties?
What does/did the vendor outsource and where did/does the vendor outsource to?
What happens in the event the vendor cannot complete the job or has an unforeseen disruption of business?

Pricing
Basic Processing
Enumerate units used to bill for electronic file processing (images, documents, gigabytes provided, gigabytes extracted, post-culled data extracted, etc.).
How much does the vendor charge per unit for electronic file processing?
If the vendor has the ability to keyword cull data prior to processing, provide the fee per billable unit.
Does the vendor charge any other fees for electronic file processing that would fall outside of the per unit charge (password cracking, exception handling, deduplication, etc.)?
How does the vendor define normal and expedited processing?
Does the vendor charge extra for expedited turnaround?
Post-Processing

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

If the vendor does not host the data, does the vendor charge for the export or migration of data to another system?
What does the vendor charge for the media that holds post-processed files?
What does the vendor charge for client-provided media that holds post-processed files?
Does the vendor charge for a media-less transfer of post-processed files via secure FTP?
Database Hosting
What unit does the vendor use to bill for the hosting of processed electronic files (gigabytes or documents per unit of time)?
How much does the vendor charge per unit to host processed electronic files?
Does the vendor charge any other fees for electronic file hosting that would fall outside of the per unit charge (set up fees, staging, loading, loading third-party images, etc.)?
Does the vendor charge extra for expedited hosting?
How does the vendor define normal and expedited hosting?
Does the vendor charge a licensing fee for access to the hosted system?
How does the vendor bill for licensing and at what price (per concurrent user, enterprise license, both)?
Production and Export
Does the vendor charge for data or metadata output; if so, how much?
Does the vendor charge for assigning bates or control numbers to images; if so, how much?
Does the vendor charge for imaging documents to TIF or PDF format; if so, how much?
What does the vendor charge for the media that holds the post-review production databases?
What does the vendor charge for transferring files to client-provided media that holds post-review production databases?
Does the vendor charge for a media-less transfer of built databases via secure FTP?
Does the vendor charge for the OCR of scanned images; if so, how much?
Other Services
Does the vendor charge billable hours outside of standard processing and hosting rates; if so, for what tasks and at what rates?
Does the vendor charge for training?
Does the vendor charge for technical support?
If the vendor outsources, does the vendor add any service charges to the outsourced bill; if so, how much?

Published by Pike & Fischer, A BNA Company.

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

http://ddee.pf.com

Reprinted from Vol. 5, No. 11 | November 2005

TALKING TECH

Automated Document Review Proves Its Reliability

By Anne Kershaw

Pushed by cost, time, regulatory and ethical considerations to embrace change sooner rather than later, law firms and clients are increasingly experiencing the impact of electronic discovery technologies. Staying ahead of the curve on these offerings is key to the effective management of discovery, providing the most reliable and cost effective case management for clients. While we have not yet reached the brave new world of completely automated document review, independent evidence suggests that automated techniques can do a significantly more accurate and faster job of reviewing large volumes of electronic data for relevance, and at lower cost, than can a team of contract attorneys and paralegals.

We discuss below a substantial study that we conducted, comparing automatic relevancy assessment to relevance assessments made by people. It demonstrated that using an electronic relevance assessment application and process reduced the chances of missing relevant documents by more than 90 percent.

Changing Landscape

Traditional methods of document review are typified by manual review using contract attorneys, entry level lawyers or paralegals. The individuals who are part of the review team are increasingly challenged by the sheer volume of data typically generated and stored by almost every organization that uses computer technology. Indeed, in some cases, it is simply not humanly possible to read all of the potentially relevant e-mail and documents within the time parameters set by the court.

Recent technological developments in the area of automated document review for relevance assessment are solving these problems, paving the way for profound and fundamental changes in the way discovery is conducted. In addition, technology can further level the playing field for smaller firms, by providing the ability to conduct large scale review with far fewer resources. While in the past lawyers may have been slow to embrace new technologies, all counsel would be well served to take early notice of the area of electronic document assessment.

Driving Change – Better Results for Less Cost, in Less Time

While law firms ultimately will derive many benefits from advanced document analysis technologies, large data producers such as universities, corporations, and government, are generally the leading proponents of their adoption. These data producers are driven in large measure by the enormous costs associated with conducting manual discovery in large document cases, which can easily encompass tens of millions of electronic documents.

Some companies are already starting to mandate that law firms use specific advanced technologies, even paying consultants to help make this transition successful; courts handling large cases may soon follow suit. In the future, more companies will, as a matter of course, tell counsel not only that they have to use technology, but identify which vendor they are required to retain. Law firms, large and small, would be well served to embrace these technologies before they are sent scrambling to do so by clients and courts.

Cost is certainly a principal driver in this shift. Automated document assessment solutions are cheaper, in most cases, than paying for an equivalent manual review capacity. Data collections often run into many gigabytes or even terabytes of data. Considering that one terabyte is generally estimated to contain 75 million pages, a one-terabyte case could amount to 18,750,000 documents, assuming an average of 4 pages per document. Further assuming that a lawyer or paralegal can review 50 documents per hour (a very fast review rate), it would take 375,000 hours to complete the review.

In other words, it would take more than 185 reviewers working 2,000 hours each per year to complete the review

Reprinted with permission from *Digital Discovery & e-Evidence*, Volume 5, Number 11, pages 10-12. Copyright © 2005 IOMA, Inc. Published by Pike & Fischer. For more information on *Digital Discovery & e-Evidence,* call 800-255-8131 ext. 248.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

within a year. Assuming each reviewer is paid $50 per hour (a bargain), the cost could be more than $18,750,000.

Electronic document review and assessment applications can now reliably identify the relevant documents first, and sort them according to subject matter. This dramatically reduces the volume of data requiring review by professionals for privilege and confidentiality and makes that review process substantially more efficient and cost effective.

"It is quite usual to see cases where we reduce the amount of data to be reviewed by 80 to 90 percent," reports Jonathan Nystrom, Vice President of Sales with Cataphora, a vendor of advanced electronic discovery services. "Only the time and cost savings possible using the latest electronic discovery tools make it even possible to undertake such a project," he adds.

A recent study that appeared in *Digital Discovery & e-Evidence* showed that, for a smaller case with 30 gigabytes of data, manual review could cost $3.3 million. The study described how a more advanced electronic approach could reduce that cost by 89 percent, to less than $360,000. (See "Document Analytics Allow Attorneys to be Attorneys," Chris Paskach and Vince Walden, *DDEE*, August 2005, page 10.)

Moreover, further cost savings can be realized by using the same technology, and often many of the same findings, across multiple cases over time. For example, a pharmaceutical company, for which litigation is a way of life, will often be required to produce very similar evidence in case after case. "Automation can measurably reduce these costs of doing business," comments Nicolas Economou, from electronic discovery services company H5 Technologies.

For large data producers, the consistent and repeatable processes provided by advanced review technologies are important, in addition to their accuracy, speed, and cost advantages.

Finally, the ability to see the fact pattern in the case earlier, thanks to the speed of automated review and the advent of electronic document analytics, provides better insight as to when early settlement might be appropriate, eliminating the costs of prolonging the matter unnecessarily. Such analysis also helps attorneys assess the benefits and trade-offs of producing documents in native format versus tiff images with fielded text.

Electronic Discovery's Old Guard

Many different types of tools have been developed over the years that provided limited support for electronic discovery. For example, a common approach has been to put imaged data (e.g. tiff files) and text into a database where the information can be examined using keyword searches.

Unfortunately, keyword searches are limited in their effectiveness. Not all documents of importance necessarily contain a candidate keyword and, at the same time, any chosen keyword will likely occur in many documents that are not of interest. As a result, documents of interest constitute a small minority of those located. The problem then remains, how to find the desired documents among the many that have been returned. Attempts to refine keyword searches by, for example, adding Boolean constraints (i.e., some combination of "ANDs" and "ORs"), do not usually provide much significant improvement.

The most advanced tools available today offer vastly improved capabilities. Legal teams can use such tools to locate relevant documents much more efficiently than ever before. And this evidence can be found much earlier in the proceedings. Getting more relevant information early in the process puts attorneys in a much better position to determine case strategy and gives them a much stronger basis from which to negotiate with the opposing side.

The State of the Art

Many vendors today provide the capability to use statistical techniques to determine which documents are "similar" according to specified criteria or exemplars and to group them together. This can help reviewers focus their efforts and provides huge time and cost savings over the course of a review. However, it is important to validate the accuracy of such automated categorization vis-à-vis the responsive specifications.

In many instances two documents may objectively be very similar to one another, yet one may be responsive and the other not. For example, in a particular matter, a document discussing the sale of a particular product may be responsive only if the sale in question occurred in the United States. Yet documents that relate to sales in the U.S. may be very similar to documents relating to sales abroad. In this example, it is very easy to see how two virtually identical documents, which would be grouped together by this technology, could fall on opposite sides of the responsiveness line.

Another approach is the use of what some vendors call "ontologies" or "word communities." They capture information about the words and phrases that model a particular area of knowledge. For example, in a case relating to alleged insurance fraud, an ontology might address particular industry practices that are potentially relevant to an investigation, or certain insurance-specific vocabulary that could be indicative of a responsive document.

Ontologies can provide a means of very accurately pinpointing relevant information. Equally valuably, they can be used to identify irrelevant materials, including junk e-mails, which can then be removed from consideration, thereby decreasing the amount of potential evidence that has to be reviewed. Additionally, much of the information captured by ontologies can be reused from matter to matter.

Contextual review is another example of advanced electronic document assessment. This technology uses the context between different documents to help reviewers determine the importance and relevance of a piece of potential evidence.

"Traditionally, context has meant looking at context *within* a document," comments Cataphora's Nystrom. "By contrast, we now have the ability to look at context in the form of the relationships *among* documents. Seeing potential evidence in the context in which it was originally created and used makes it much easier for reviewers to make accurate assessments of its relevance and importance, and to do so very quickly."

Some of these tools also provide litigation support managers with increased control over the review. They can then ensure that the review is completed on time and within budget. To help managers do this, advanced tools can provide information about how much of the evidence has been reviewed, and how much remains. Review managers can then determine whether they have enough resources to get the job done on time and to make adjustments at the earliest possible opportunity. It is even possible to monitor the speed and effectiveness of individual reviewers, tracking how much evidence each reviewer has processed. Review managers can also see which reviewers are finding the largest numbers of relevant documents, and how accurate their review decisions are.

Electronic Document Assessment for Relevancy Really Works

Historically, human review has been the gold standard for initial relevancy assessment. Yet it was rarely, if ever, tested for accuracy. The advent of electronic relevancy assessment processes and applications now allows for the comparison of these techniques against human review. We conducted such a study and found not only that the electronic assessment for relevancy was highly accurate, but also that people reading documents to assess relevancy missed close to half of the relevant documents.

Our study began with a set of 48,000 documents, which were to be coded for relevance to three responsive categories. The software was set up in accordance with the vendor's standard practices, which included interviewing the attorneys and reviewing documents to gain an understanding of the relevance criteria for the case and training the software accordingly. In parallel, six reviewers were trained to conduct a manual review of a stratified random sample of 43 percent of the corpus.

The software and the reviewers separately reviewed the documents and the results were compared. We assumed that where the software and the humans agreed, the determination was correct. Where there was a discrepancy (a document marked responsive by one approach and not by the other), the document was re-examined by the same reviewers to determine (in some cases with some debate and arbitration) who was correct, the software or the human reviewer.

At the end of day, after all the numbers were crunched, the human reviewers were shocked at how many documents they missed and were similarly startled at how well the software achieved the objective of locating relevant documents. Across all three codes, the software, on average, identified more than 95 percent of the relevant documents, with a high of 98.8 percent for one of the codes. The people, on the other hand, averaged 51.1 percent of the relevant documents, falling as low as 43 percent for one of the codes.

These findings makes sense considering that document review work is extremely difficult, that people have subjective views of relevancy, and people can be easily distracted from the work by fatigue or thoughts of lunch and other matters. The software process, on the hand, consistently assesses every document and never gets tired.

In sum, the results of our study demonstrated that the use of a particular software application and process reduced the risk of missing a responsive document by 90 percent. Moreover, the effectiveness of the electronic process improves as it is tweaked throughout the quality assurance process. These results may be surprising to those who have an abiding belief in the quality of traditional manual review, but they are probably an accurate — maybe even optimistic — reflection of the performance of an average review room, particularly if the case is large and complex and review is being conducted, as it so often is, against an aggressive deadline.

The legal world may not yet be ready for fully automated review, and there will long remain a role for expert human review. Nevertheless, advanced technologies can be used to focus review efforts on those documents that are most likely to contain relevant information. At the very least, such tools can be used with some confidence to root out obviously non-responsive materials, allowing review to focus on what is left. That alone can provide considerably increased efficiency, reduced costs and superior results.

What this Shift Means for Lawyers

The newest technologies open the door to successful handling of much larger volumes of electronic evidence than has ever been possible before. Faced with the advent of these tools, attorneys have the choice to either embrace them, or take the risk that competing firms will take business away from them.

Automated document review and analysis provides significant new opportunities for attorneys in law firms and in corporate legal departments. Legal review can be a more efficient, less costly, and a more proactive process that aids the legal team in managing the case.

There is every sign that the competition will become more intense. Technology can level the playing field by giving smaller firms the same review capability as larger firms, and business as usual will not be an adequate response. All law firms, large and small, must prepare for the impact of the new technologies.

Copyright © IOMA, Inc. Published by Pike & Fischer

November 2005
Copyright © IOMA, Inc. Published by Pike & Fischer

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Anne Kershaw is the founder of **A. Kershaw, P.C. // Attorneys & Consultants,** a nationally recognized litigation management consulting firm providing independent analysis and innovative recommendations for the management of all aspects of volume litigation challenges.

Ms. Kershaw provided electronic discovery survey data and testimony before the Federal Civil Rules Advisory Committee. In addition, she is a principal author of *Navigating the Vendor Proposal Process: Best Practices for the Selection of Electronic Discovery Vendors* and a contributing editor to *The Sedona Conference Glossary For E-Discovery and Digital Information Management (May 2005 Version)*, both projects of the Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production RFP+ Group (www.thesedonaconference.org).

Further information regarding Ms. Kershaw's resume, career and practice is available on www.AKershaw.com.

Copyright © IOMA, Inc. Published by Pike & Fischer

ACC Association of Corporate Counsel

Electronic Discovery Trends and Best Practices

Sonya L. Sigler
General Counsel
Cataphora

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Trends & Best Practices

- New FRCP - December 1, 2006
- Preservation
- Collection
- Review
- Production
- Investigation

Federal Rules of Civil Procedure

- Effective December 1, 2006
- Electronically Stored Information - Rule 34
- Meet & Confer - Rule 16
- 30(b)6 Depositions
  - IT Person
- Inadvertent Disclosures - Rule 26
  - Claw back

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Rule 37 (f) - Safe Harbor?

Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system.

Preservation

- Duty to Preserve
- Complying with Litigation Holds
  - Corporate Counsel Role Widened
  - Document Retention Requires More Attention
- Pull & Park Phenomena
  - Backup Tapes
  - FRCP - Safe Harbor - Rule 37

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Electronic Data Collections Are…

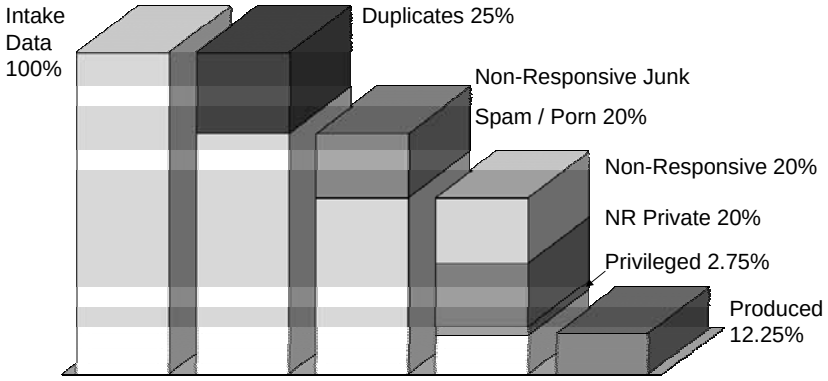
- Volatile
  - Can change without your awareness
- Free-ranging
  - Not always located where you expect
- But, most importantly…
  - Prolific
    - Can duplicate rapidly

How Electronic Collections Are Different

- *Much larger data collections, but that's not all*
  - Meta data - Each item contains much data about itself, both hidden and visible
  - And there are *many* very small items
- Duplicates - Collections are often very largely redundant
- Mixture of informal and formal, personal and professional, highly useful and highly useless content, cryptic content

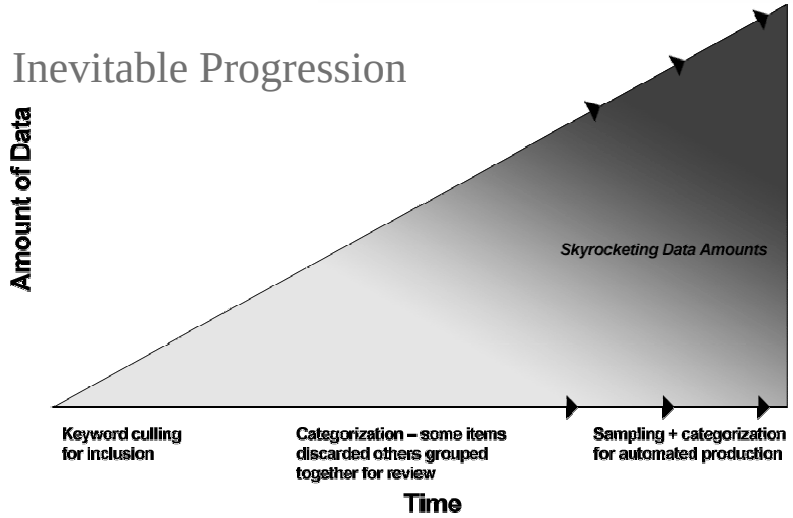
This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Getting to Reviewable Data



These figures vary based upon the data set received

Inevitable Progression

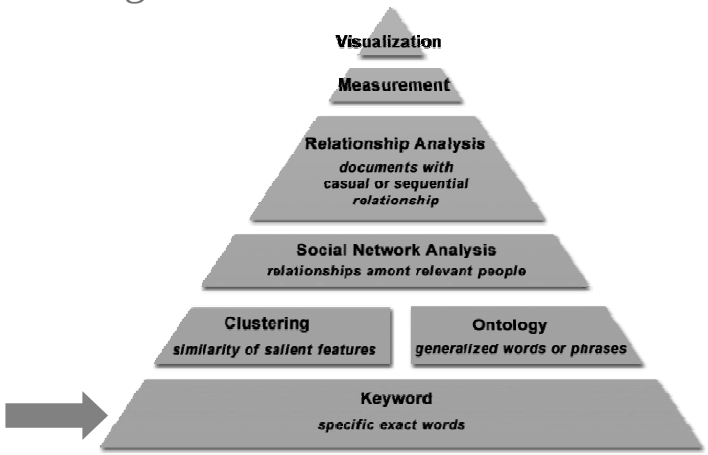


This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Review - Relevancy Assessment

- Beginning to End No Longer Tenable
  - 600 GB (10GB/60 custodians)
  - 100 reviewers almost 1 year to review it all
- Keyword searches, culling
- Categorization of Data
- Technology-Assisted Review
  - Categorization
  - Sampling

Culling Methods

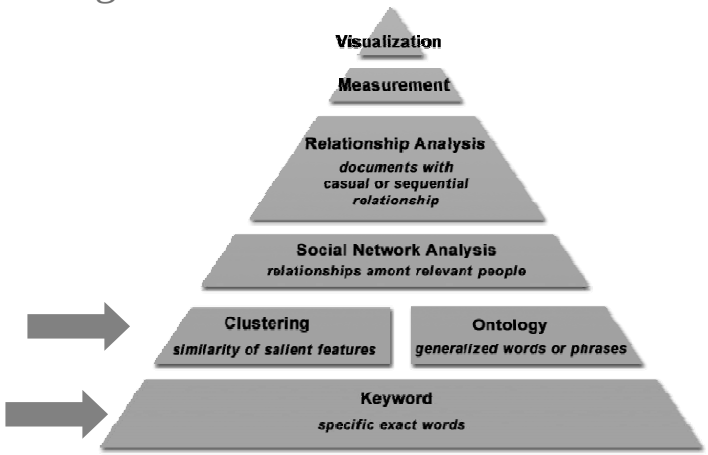


This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Categorization of Data for Review

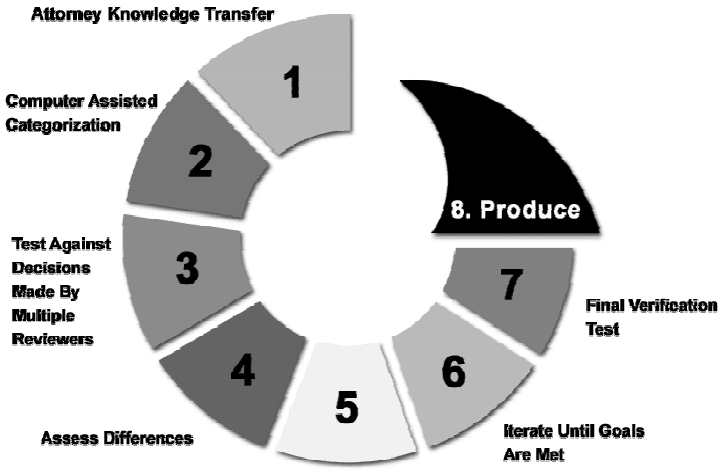
- Categorize Entire Data Set
  - Spam/Porn/System Files
  - Personal/Private Data
  - Non-relevant Business Data
- Business Data
  - Relevancy Assessment
  - Privilege Review
- Keyword Analysis - Overlap, Holes

Categorization Methods



This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Technology-Assisted Review



Production

- Native
  - Unique ID
- FRCP Default - Rule 34
  - Requesting Party Specifies or Parties Agree
  - Ordinarily Maintained or Reasonably Usable
  - Not More than One Format
- Shared Database

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

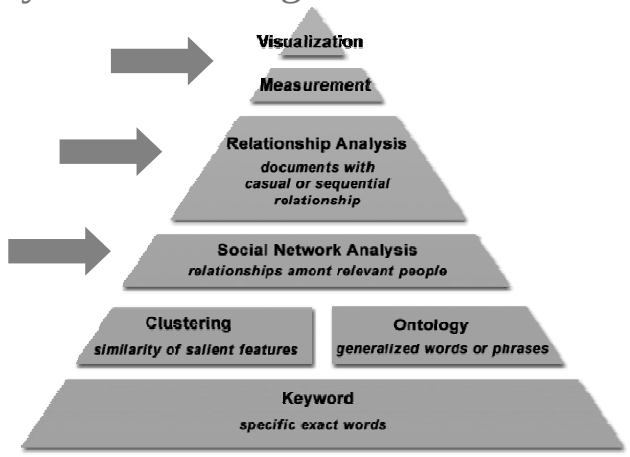
What can you learn from the data beyond review?

Analtyics & Investigation - Making Sense of the Data

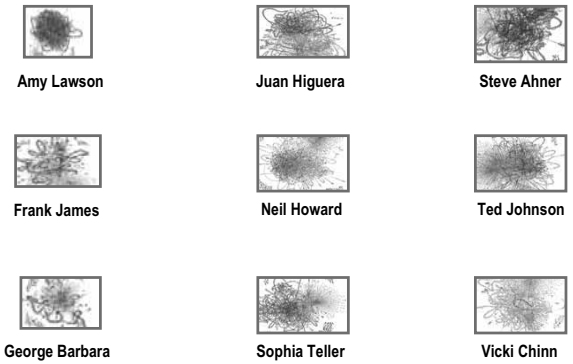
- Patterns/Variations
  - Counting (tally)
  - Analytics
  - Visualizations

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Analytics & Investigation Methods



Text Deletions



This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Best Practices Extends Defensibility

- How do you defend a process that is new to you?
- How do you attack a process that is new to you?
- Invite Vendors and Law Firms to Share Approaches

Learn About Methodologies

- Sedona - Best Practices - Selecting an Electronic Discovery Vendor
  - RFI
    - Seek Information from Companies
    - Due Diligence
  - RFP
    - See Proposals from Companies
    - Vendor Comparison
  - RFI/RFP Process is to Facilitate Decision Making
    - Not Replace Your Judgment
- Sedona - Search & Retrieval Sciences - Coming

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Best Practices for You

- Familiarize Yourself with New FRCP
- Figure Out What Process Works for You and Your Company
  - Preservation and Collection
  - Review and Production
  - Analytics & Investigation
  - Document It!
- Be Informed - RFI/RFP Process

204: Leading Through the Electronic Discovery Quagmire (Part 1): Nuts & Bolts Best Practices

Miriam Smolen
Associate General Counsel
Fannie Mae

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

THE REAL COSTS OF
ELECTRONIC EVIDENCE VENDORS

Checklist to assess total costs and compare vendors

Single vs. Multiple Vendors

- ✓ Consider using different vendors for various aspects of the project
  - ✓ One vendor for data collection and culling
    - ✓ Goal to reduce volume of data to be loaded
  - ✓ One vendor for loading and review tool
- ✓ Might be more cost effective to use vendor that can integrate with in-house applications to reduce loading and hosting costs
  - ✓ Cost of vendor continuing to support application used in-house

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

General Fees

- ✓ Set up costs
  - ✓ Fixed fee or
  - ✓ Hourly (consider a cap on fees)
- ✓ User license fees (per month/period of months)
  - ✓ Who monitors activity level of user accounts to ensure non-active users accounts closed
  - ✓ Is there a professional services fee associated with the monitoring
  - ✓ Is there a fee for deactivating inactive accounts or for reactivating inactive accounts
- ✓ License subscription fees

Training Costs

- ✓ Live training
  - ✓ Day rates vs. hourly rates
  - ✓ Travel/per diem travel costs
  - ✓ Is vendor willing to waive charges for certain number of training sessions
- ✓ Web-based training
  - ✓ Session fee vs. hourly fee
  - ✓ Will vendor provide free web-based training

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Data Loading and Processing Costs

- ✓ Identify what terminology vendor using and what activities are included in price
  - ✓ Conversion to format used by vendor
    - ✓ Does vendor require conversion of native images to TIFF prior to loading.
    - ✓ If production going to be subset of total volume loaded, not cost-efficient to use vendor who requires conversion to TIFF
  - ✓ Processing
  - ✓ De-duplication
  - ✓ Loading to vendor application
- ✓ Are services bundled together for one fee, or assessed separately
  - ✓ If separate fees, need to calculate total of all services to understand real cost
  - ✓ If not all data requires conversion or de-duplication, may want to unbundle services to gain lower processing cost for certain data

- ✓ Loading costs
  - ✓ Native – usually $$ per gigabyte
    - ✓ Are costs variable depending on source of data
    - ✓ Can cost be reduced if loading pre-processed data (such as data coming from another e-vendor)
  - ✓ TIFF/PDF images
    - ✓ Additional cost for data extraction?
    - ✓ Additional cost for OCR (optical character recognition so data is searchable?
    - ✓ Additional cost for conversion of single page TIFF to multiple page TIFF
- ✓ At what stage in the process are costs assessed
  - ✓ Prior to de-duplication or post de-duplication
  - ✓ Is duplication done across custodians (thus loading on one unique copy) or within custodians (thus resulting in multiple copies across database and increase total volume of data)

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

- ✓ Other processing/loading issues
  - ✓ Are there fees for password cracking
    - ✓ Charge per file or per hour of service
  - ✓ Are there unique charges depending on how data received by vendor
    - ✓ Are there additional charges for data transfer by FTP because vendors need dedicated bandwidth, servers etc.
  - ✓ Are there incremental load charges
    - ✓ Some vendors charge additional cost if data received in multiple small batches
  - ✓ Load charges during first month – when are charges assessed. Fees should be pro-rated
- ✓ Common for volume discounts. Negotiate reduced rates as volume increases.

Hosting Costs

- ✓ Hosting of data typically charged per volume measure on monthly basis
  - ✓ Per gigabyte for native data
  - ✓ Per page for TIFF/PDF
- ✓ Negotiate
  - ✓ Sliding scale for higher volumes
  - ✓ Waiver of hosting costs for period of time

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Best Practice to Reduce Hosting Cost

- ✓ Reduce volume of data as much as possible
- ✓ Review sources of data prior to loading to exclude duplicate data
- ✓ Use vendor which is able to hold unique copy of document with the ability to:
  - ✓ Import multiple source information linked to the document
  - ✓ Import multiple custodian information linked to the document
  - ✓ Import production history
  - ✓ Re-populate the document to multiple custodians or sources if document needs to be produced multiple times.

Hosting Shared Databases

- ✓ Use shared databases to produce documents to opposing party, or share documents with aligned parties
- ✓ Does vendor have ability to share documents among parties without sharing coding fields? Dependant on security of fields
  - ✓ If not, will new database be set up for sharing and will new hosting charges be applied for duplicate set of data
  - ✓ Will there be costs associated with transferring data to new database

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Costs of Archiving Data

- ✓ If case is dormant for period of time, does vendor have ability to archive data for reduced hosting fee
- ✓ Is there a cost for re-activating database

Costs of Production

- ✓ Costs of production dependant on format
  - ✓ Conversion to TIF/PDF
  - ✓ OCR charge
  - ✓ Per page charge for produced version
  - ✓ Negotiate sliding scale for large volume of productions
- ✓ Reduced rate to reproduce earlier production
- ✓ Additional costs
  - ✓ Cost of production media (CD, DVD, hard drive)
  - ✓ Bates numbering and legends
  - ✓ Shipping costs
- ✓ Paper production costs (per page)

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Professional Services Fees

- ✓ Professional Services Fees usually charge per/hour with sliding scale based on job level
  - ✓ Case administrator should cost less per/hour than project manager or technical engineer
- ✓ Very unpredictable costs. Always much higher than anticipated
- ✓ Certain services could be preformed by other persons such as in-house counsel, outside counsel litigation support personnel, or consultant
  - ✓ Need to analyze whether there is cost savings is use non e-vendor personnel for certain tasks

Professional Services -- Tasks

- ✓ Professional Services may include:
  - ✓ Set up of database, coding fields, metadata fields
  - ✓ Overseeing processing and loading of data (processing/loading fees typically do not cover the professional service support of process)
  - ✓ Help desk: i.e. account resets, small technical issues
  - ✓ Develop, run and save searches
  - ✓ Assignment of batches or folders of documents to reviewers
  - ✓ Sweeping completed review batches or folders
  - ✓ Running reports
  - ✓ Pre-production tasks (i.e. repopulating production data)
  - ✓ Reviewing that coding is proper
  - ✓ QC review flow and productions
  - ✓ Training sessions
  - ✓ Responding to requests from multiple parties using database
  - ✓ Services to support counsel performing in non-efficient manner (i.e. counsel requesting broad searches then printing documents for review)

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Cost Savings in Professional Services fees

- ✓ Sliding fee scale for level of experience
- ✓ Commit to blocks of hours for reduced fee
- ✓ Commit to dedicated support person(s) for set fee/time period
- ✓ Build in certain level of support, or hours of support, into loading charges
  - ✓ Larger upfront cost, but able to use services without concern of unpredictability of costs
  - ✓ Reduces incentive for good service

Non-financial Professional Services Issues

- ✓ Response times
- ✓ Availability of appropriate personnel
- ✓ Competence
- ✓ Training new employees on your project (and your dime)
- ✓ Off hour availability of personnel
- ✓ Impact of system upgrade

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Termination Costs

- ✓ When case terminates, what are costs for closing down database?
  - ✓ Is there a cost for removing client data from system and returning it to client
    - ✓ Professional Service hours
    - ✓ Media cost
    - ✓ Saving coding in some form
  - ✓ Is there a cost for transferring the data and work product to another vendor

Service Level Agreements

- ✓ Service Level Agreements provide for certain level of service guaranteed by financial penalties
  - ✓ Otherwise the only "penalty" may be termination of contract which is usually not possible mid-case
- ✓ Possible topics
  - ✓ Availability of system
  - ✓ Response times of professionals
  - ✓ Navigation time (doc to doc or page to page depending on size of document)
  - ✓ Security of documents in shared database
  - ✓ Missed production or other deliverables deadlines

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

Electronic Discovery: Verizon Case Study

Patrick L. Oot
Director of Electronic Discovery And Senior Counsel
Verizon

Overview

- Controlling Costs
- Building an In-house Team
- Verizon's National EDD Vendor RFP
- Proactive Keyword Search Terms
- Internal v. External Processes

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

STRATEGY:
CONTROLLING E-DISCOVERY COSTS REQUIRES OWNERSHIP OF COSTS

Build A Team

CONTROLLING COSTS: BUILD A TEAM

- Verizon as Non-traditional Corporate Client
- Electronic Discovery Group Formed in 2005 at the Direction of the Vice President of Litigation
- Charged to Develop a Uniform Policy Governing the Collection, Retention, Review, and Production of Electronic Data, While Reducing Vendor Costs and Minimizing Risks
- Responsible for Creating Technical Solutions to Discovery Problems
- Team includes Vice President of Litigation, two attorneys, IT Liaison, and support staff

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

BUILD A TEAM – SMALLER COMPANY

- Find Internal Resources
  - Stakeholders, Budgets Effected, Current Experts
- Find External Resources
  - Consultants, Outside Counsel, and Vendors
- Train Internal Resources
  - CLE Events- Trade Shows – Law School Classes
- Proactive Education
  - The Sedona Conference - Round Table Events

VERIZON E-DISCOVERY TEAM: MISSION STATEMENT

Meet Litigation Obligations

Save Money

Don't Annoy the Business People

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

STRATEGY: CONTROLLING E-DISCOVERY COSTS

Know the Process

OBJECTIVES:UNDERSTAND HOW YOUR DATA MOVES

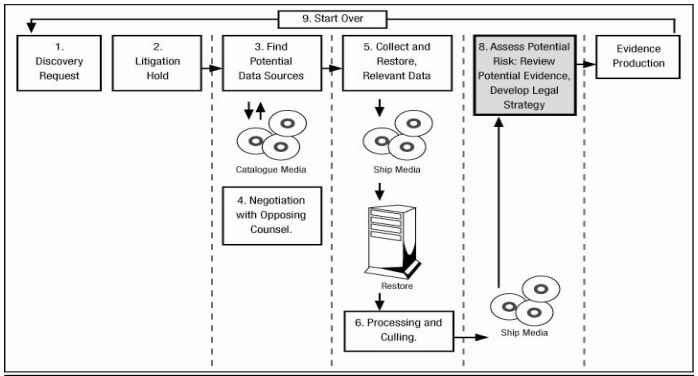
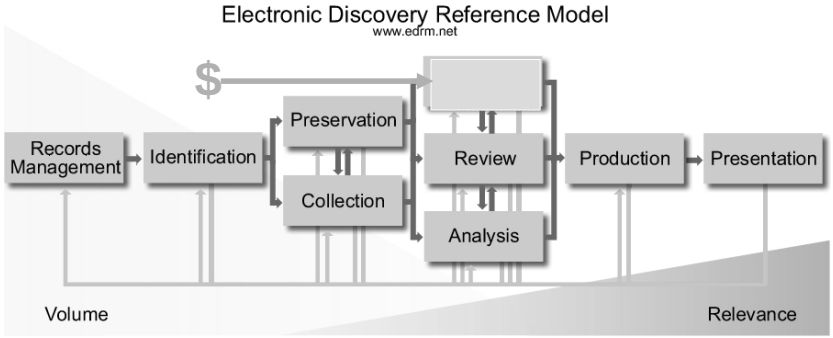


Diagram A: Typical E-Discovery Process

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

UNDERSTAND KEY BILLING POINTS: WHAT CAN A FIRM DO TO POINTS



Develop strategies to create efficiencies in each cost center while maintaining strong oversight on goal driven project management.

IMPACT: Facts and Figures at Verizon

$7,593,007.95

Facts and Figures at another Fortune 500 company (similar matter – same number of custodians)

$42,000,000.00

Cost of Electronic Discovery Charges and Contract Attorney Review
Medium Sized 82 Custodian Matter

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

STRATEGY:
CONTROLLING E-DISCOVERY COSTS REQUIRES OWNERSHIP OF COSTS

Build A Team

BUILD A TEAM – SMALLER COMPANY

- Find Internal Resources
  - Stakeholders, Budgets Effected, Current Experts
- Find External Resources
  - Consultants, Outside Counsel, and Vendors
- Train Internal Resources
  - CLE Events- Trade Shows – Law School Classes
- Proactive Education
  - The Sedona Conference - Round Table Events

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

ACC Association of Corporate Counsel

CONTROLLING COSTS FOR E-DISCOVERY

Annual National Electronic Discovery Services RFP

ACC Association of Corporate Counsel

STRATEGY:
BARGAINING POWER OF A NATIONAL RFP

Save $380,501.64

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

STRATEGY:
CONTROLLING E-DISCOVERY COSTS

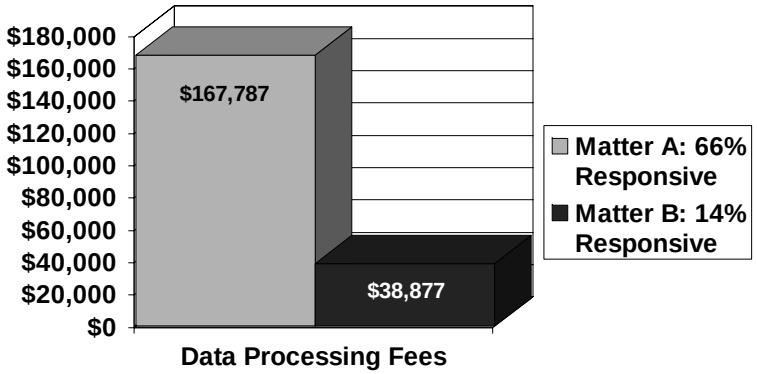
Mind the Terms

STRATEGY: PROACTIVELY SELECT KEYWORD SEARCH TERMS

Pay for the Hits Not the Misses

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

PROACTIVELY SELECT KEYWORD SEARCH TERMS



INTERNAL RESOURCES OR OUTSIDE VENDORS?

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

UNDERSTAND KEY BILLING POINTS: WHAT CAN A FIRM DO IN-HOUSE?

Collection	Processing
Hosting	Review

Develop strategies to create efficiencies in each cost center while maintaining strong oversight on goal driven project management.

AVOID PROCESSING FEES

Central Archive

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

SAVE PROCESSING FEES

Litigation Ready Data

LITIGATION READY DATA

Save $1,054,352.00

Data processing for a recent medium-sized matter with 82 custodians

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).

CONSIDERATIONS FOR BRINGING CERTAIN PROCESSES IN-HOUSE

- Does your workload support internalization?
  - Is It cost effective?
- Can your staff handle the additional burden?
  - If you build it, will they come?
- Can your organization incur the capital expenditure for IT equipment?
  - Projected savings often hit different budgets.
- Who will manage the new equipment?
  - IT, Legal, or an External Contractor?
- What other organizations might be interested?
  - Consider Legal, IT, Compliance, and Security.
- What types of projects are best suited for vendors and consultants?
  - Consider your litigation strategy before you internalize certain processes.

This material is protected by copyright. Copyright © 2006 various authors and the Association of Corporate Counsel (ACC).