
**AMERICAN BAR ASSOCIATION
YOUNG LAWYERS DIVISION
LITIGATION SECTION**

DIGITAL DISCOVERY

I. Introduction

Digital discovery is just discovery. When digital discovery was new, some commentators sought to carve digital discovery off from traditional discovery. But what is becoming rapidly apparent is that everyone, from a multi-million dollar corporation to a small “mom and pop” business, has gone virtual to some extent. Indeed, you would be hard pressed to find any business, no matter how small, without, at very least, e-mail and word processing. Moreover, virtually every jurisdiction and court has already faced these issues and have resolved issues in favor of allowing widespread digital discovery. Although some judges may be loathe to enter the digital arena, the vast majority have already begun to face “digital discovery issues.” For these reasons, this presentation is not as concerned with technical rules that surround digital discovery, but rather the practical issues of what discovery to seek, when to seek electronic discovery, how to get electronic discovery, and how to use electronic discovery.

II. Digital Discovery Before Filing

A. Personal Jurisdiction Through Electronic Contacts.

1. *Zippo* and its progeny – emergence of “something more”

In recent years, the law on using web pages as a basis for personal jurisdiction has rapidly developed. When web pages were rare, courts’ first response was to assess personal jurisdiction primarily on a question of interactivity. Under such a model, purely passive web sites that displayed information without more were shielded for personal jurisdiction, while entities doing business over the Internet were subject to personal jurisdiction. Between these two models were web pages deemed to be interactive to the extent that a user could send or receive information from a computer. In such cases, jurisdiction was determined by examining the level of interactivity and the commercial nature of the exchange of information that occurred on the web site. See *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119, 1123-24 (W.D. Pa. 1997).

As the case law developed, courts have refocused their inquiry on the nature and quality of commercial activity on the web site. Some courts have described this approach as demanding “something more” than interactivity. For example, in *ESAB Group, Inc. v. Centricut, LLC*, 34 F.Supp. 2d at 323 (D.S.C. 1999), the court held that even an interactive web page did not cause an entity to be subject to personal jurisdiction where plaintiff failed to demonstrate: (1) any evidence of actual commercial activity over the Internet in the forum, (2) any evidence that any forum resident ever visited the web page or purchased products based on the web site, or (3) any evidence that defendant did anything to encourage residents of the forum to visit the web site or that web site was directed at the forum more than anywhere else in the country. *Id.* at 331. See also *E-Data Corp. v. Micropatent Corp.* 989 F.Supp. 173, 177 (D.Conn. 1997) (no personal jurisdiction in the absence of evidence that the defendant’s web advertisements actually reached this forum via a Connecticut consumer); *Edberg v. Neogen Corp.*, 17 F.Supp.2d 104, 114 (D.Conn, 1998) (no personal jurisdiction absent evidence that any user in Connecticut accessed the web site or purchased products, or the web page was directed particularly at Connecticut residents); *Origin Instruments Corp. v. Adaptive Computer Systems, Inc.*, 1999 WL 76794 at *4 (N.D.Tex. Feb. 10, 1999) (Even with a moderate level of interactivity, there is no personal jurisdiction absent evidence that defendant interacted with anyone in Texas, made any sales through the web site or traveled to the forum to pursue business).

Thereafter, courts began recognizing that mere interactivity is not enough. Instead, courts examine the “nature and quality of the commercial” contacts actually occurring through the Internet. Accordingly, in *Hurley v. Cancun Playa Oasis International Hotels*, 1999 WL 718556 (E.D. Pa. August 31, 1999), a court refused to

find personal jurisdiction over a Georgia corporation even though defendant accepted and confirmed reservations over the web site, publicized a 1-800 number and provided an e-mail address. The court concluded that even though the web site was interactive, there was no evidence of a single Pennsylvania resident, other than attorneys for plaintiffs, visiting the defendants' web page. In addition, the record was devoid of even a single instance of a deliberate contact between defendant and Pennsylvania. Finally, the record lacked evidence that the web page was directed at Pennsylvania any more than any other state. *Id.* at 3.

In *Brown v. Geha-Werke GmbH, Shredex, Inc.*, 1999 WL 803750 (D.S.C. September 29, 1999) the mere fact that defendant's web site advertised its products and provided an e-mail address was insufficient to form a basis for personal jurisdiction. No evidence was offered that *Geha-Werke* ever serviced customers in the forum or provided them with regular advice. Accordingly, the nature and quality of contacts failed to satisfy due process concerns.

The weight of authority shifted towards the view that even a moderately interactive web site does not establish personal jurisdiction in any forum in which it is accessible. Rather, "something more" had to be demonstrated by the party seeking jurisdiction, namely commercial activity of a nature and extent that supports personal jurisdiction as a matter of due process. Mere potential is insufficient to establish general personal jurisdiction. *Millennium Enterprises, Inc. v. Millennium Music, LP*, 33 F.Supp. 2d 907, 921 (D.Or. 1999).

This approach has routinely been applied since these initial cases were decided in 1999. In a recent search, the U.S. District Court for the state of Utah applied this approach as recently as January 2002. *iAccess, Inc. v. Webcard Technologies, Inc.*, 2002 WL 99651 (D. Utah) (No personal jurisdiction because defendant did not direct activities at Utah and no evidence linked sales, including the sale in question, to the website).

2. Now back to basics.

In the 2002 Updates to *Wright and Miller*, 4A Fed. Prac. & Proc. Civ.3d § 1073.1, the authors note the development of the *Zippo* sliding scale analysis but question as to whether this test really should supplant the traditional notions of personal jurisdiction. As the authors note, "We do not believe that the advent of advanced technology, say, as with the Internet, should vitiate long-held and inviolate principles of federal court jurisdiction... thus, the analysis applicable to a case involving jurisdiction based on the Internet (or any other modern technology) should not be different at its most basic level from any other personal jurisdiction case." *Id.* at pp. 1-2.

Rather than jump to the *Zippo* analysis, *Wright and Miller* urge courts to follow the pattern of a traditional general jurisdiction analysis and only then an analysis of specific personal jurisdiction. As for general jurisdiction, the question remains whether a defendant has continuous and systematic contacts with the state in question. In this analysis, *Wright and Miller* rightfully point out that *Zippo* has no real utility.

With regard to specific personal jurisdiction, courts should then consider only (1) Did the plaintiff's cause of action arise out of or result from the defendant's forum-related contacts? (2) Did the defendant purposely direct its activities toward the forum state or purposefully avail itself of the privilege of conducting activities therein? (3) Would the exercise of personal jurisdiction be reasonable and fair? *Id.* at 3 (citations omitted). Essentially, *Wright and Miller* urge a return to traditional notions of specific personal jurisdiction, notwithstanding the fact that the contacts are internet-related.

It is the second factor of traditional specific personal jurisdiction analysis in which *Zippo* falls - the nature of the website (passive or interactive) determines to great extent whether the defendant purposefully availed itself of the privilege of conducting activities. Examples cited by *Wright and Miller* of efforts on websites avoiding purposeful availment (and, effectively, interactivity) include:

- the use of disclaimers, such as the website is intended for a limited audience
- statements on the web site directed only at residents of a limited geographic area
- design of the web site so that it will not interact with users of the forum state

- a self-description that the web site is only “informational”
- an absence of evidence of the website being contacted by residents of the forum state
- the use of forum-selection or choice-of-law agreements that specify a state other than the forum state

In contrast, *Wright and Miller* provides the following examples of situations in which purposeful availment is likely to be found:

- income generated through the internet activity from the forum state
- knowledge by defendant that the internet activity will do substantial harm to the plaintiff in the forum state
- a high number of hits from the forum state
- the indiscriminate responses by the defendant to every email sent to the forum state
- content that evidences targeting members of the forum state
- the ISP being located in the forum state

Id. at 4.

While *Wright and Miller* is hardly binding law, the position of the authors does seem to reconcile the adherence to the *Zippo* standard without clear foundation in traditional due process analysis. Indeed, much of the time parties will engage in both internet and non-internet contacts and, thus, require that the two analyses be blended regardless of the distinct approaches. Although it is too early to tell, it appears that applying *Zippo* within traditional due process analysis is likely to gain broader acceptance as this approach is more widely disseminated.

III. Digital Discovery Issues Early in Litigation

A. Preservation of Evidence Letters.

Because the information stored on computers changes every time a user saves a file, loads a new program or does almost anything else on his or her PC, it is critical that litigants put all parties on notice that they will be seeking electronic evidence through discovery. The sooner the notice is sent the better. A letter should identify, as specifically as possible, the types of information to be preserved and note the possible places that information may exist. If necessary, parties seeking discovery should obtain a protective order requiring all parties to preserve electronic evidence and setting out specific protocols for doing so. In the letter, the party seeking discovery must:

- Specify information & possible location(s): data files, emails, audit trails, computer logs, network file or e-mail servers, mainframes, PC and work stations, offline storage, etc.
- Specify types of electronic media and other documents to be preserved: database and related structural information, replaced computers, hard drives or storage media.
- Identify key individuals by name or capacity & include secretaries, assistants, and consultants.
- Advise regarding danger of inadvertent destruction and duty to preserve.
- Request immediate backup and archive of copies of all relevant data.
- Send a similar letter to your own client; expect reciprocity and application of same standards.
- Follow-up with more specific requests as knowledge of issues and adversary’s records increases.

B. Take key “electronic discovery” depositions.

This is the single best tool for finding out the types of electronic information that exist in an adverse party’s computer systems. But who to depose?

- CTO
- Tech support staff & former employees
- Persons with access to computers or files

- Persons handling operations, maintenance, and backup
- Independent contractors
- Head of department or CIO may not be most knowledgeable

IV. Conducting *Digital Discovery During the Heart of a Case*

A. Written Digital Discovery Requests (Fed. R. Civ. Pro. 34).

1. Technical Issues in Written Digital Discovery.

Requests for production should specify in technical terms the form of production and provide instructions. Include definitions, instructions, and specific questions about electronic evidence in written discovery. In drafting discovery requests, definitions should be broadened to include language specifically directed at electronic evidence. For example, the definition of “writing” in a document demand might be expanded to include the following: data stored in a computer, data stored on removable magnetic or optical media (e.g., magnetic tape, floppy disks, and recordable optical disks), e-mail, audit trails, digitized pictures and video (e.g., data stored in MPEG, JPEG, and GIF formats), and digitized audio.

Although, the recipient of a document demand is under a duty, at the reasonable expense of the demanding party, to translate data stored electronically into a “reasonably usable form” the demanding party should think twice before availing itself of this option. (Fed. R. Civ. Pro. Rule 34(a) “translated...into reasonably usable form”). Requesting documents in “computer readable form,” where available, will result in the production of the material on disk. This can greatly speed review of the material produced because disks can be quickly searched electronically using readily available software.

In arranging for production of evidence on disk, the program used to create the information must be identified. In most instances, the responding party will volunteer this information as part of the production. If the information is not given voluntarily, an interrogatory can be used to identify the program.

2. Methodology for Written Digital Discovery

In cases involving digital discovery, a methodology has been developed following a series of recent federal cases including *Playboy Enterprises v. Welles*, 167 F.R.D. 90 (D.Colo. 1996), *Northwest Airlines, Inc. v. Local 2000 International Brotherhood of Teamsters, AFL-CIO, et al.*, Civil Action No. 00-08 (D.Minn. Feb.2, 2000), and *Simon Property Group, L.P. v. MySimon, Inc.*, 2000 WL 863053 (S.D. Ind. June 7, 2000) . As noted by Kenneth J. Withers¹ in his article *Computer-Based Discovery in Federal Civil Litigation*, the approach widely accepted is:

- The parties agree on a neutral, third-party expert who will actually carry out the inspection as an officer of the court.
- The parties, with expert assistance, agree on the scope of the inspection, including target computers or servers; target individuals, departments, or data collections; date ranges; search terms; or other scope-defining criteria. They also agree upon the form of eventual production.
- The expert creates a “mirror image” of the computer data using accepted computer forensic procedures that preserve the integrity of the original evidence.
- The expert executes the search on the “mirror image” and identifies relevant data according to the agreed-upon specifications.
- The expert runs over the responsive data with the respondent’s counsel.
- Respondent’s counsel reviews the responsive data for relevance and privilege.
- Respondent’s counsel produces relevant, non-privileged data to the requesting party in the form agreed upon by the parties.

¹ Mr. Withers material can be found at www.kenwithers.com/articles.

3. Money Issues in Written Digital Discovery – Who Pays?

Surprisingly, this issue remains unresolved, at least on a formal basis. As a general rule, parties bear their own costs for discovery. Rule 26(b)(2) provides that Courts may reallocate costs considering “burden or expense of the proposed discovery.” Yet this hardly provides much guidance in the context of digital discovery.

The ABA’s Section on Litigation has also chimed in on its position. Section 29(b) of the Section of Litigation’s Civil Discovery Standards, adopted by the ABA House of Delegates in 1999 provides that the requesting party “generally should bear any special expenses” incurred for the production of electronic materials. Where parties cannot agree, the ABA recommends that courts consider the cost of the production relative to the expenses and benefits to each party, and whether the producing party has “any special or customized system for storing or retrieving the information.”²

Realistically, however, most discovery disputes are resolved by some agreement with, perhaps, limited court involvement. Overall, the phrase “be careful what you wish for” may have more relevance than any court rule. This is because whatever a party demands is often met with a reciprocal identical request.

Fear of such a request has lead many litigators to utilize a cold war mentality with regard to digital discovery, *i.e.* a legitimate fear of Mutally Assured Destruction (MAD). This usually takes the form of extensive and overbroad written discovery requests with definitions that incorporate all “communications” whether in “electronic, optical, digital, etc. form” These requests are often objected to or simply ignored by the opposing party. Then, when it is time to address discovery shortcomings, parties fail to “pull the trigger” and instead compromise by limiting digital discovery to that which is easily obtained. While this is commonplace and often blamed on cost control, it unfortunately does a disservice to clients. As office become more paperless, this MAD mentality is the equivalent of proposing only to open half of the filing cabinets in responding to discovery. It just no longer is an option in any case.

4. Case Law Examining Scope of Rule 34 Discovery

The following were part of the presentation *Digital Evidence: From the Office to the Courtroom* presented at the 2001 ABA Annual Meeting of the Section of Litigation.³

Casenotes of Important Decisions Regarding Discovery of Digital Evidence

Dunn v. Midwestern Indemnity, 88 F.R.D. 191 (D.C. Ohio 1980).

Holding: Court ordered an evidentiary hearing to evaluate the extent of the burden of a discovery request seeking extensive computer information from the defendant. The court emphasized that cost, time and impracticality are not reason enough to stop discovery where the information sought is relevant.

National Union Electric Corporation v. Matsushita Electric Industrial Co., 494 F.Supp. 1257 (D.C.Pa. 1980).

Holding: Plaintiff required to have computer experts create a computer-readable tape containing data previously provided in printed form. Court held that production of computer tape was not a mere replication of the documents. Further, since the information sought was properly discoverable and defendants were willing to pay any necessary costs, the court saw no reason to deny their request.

In re Brand Name Prescription Drugs Antitrust Litigation, No. 94 C. 897 MDL 997, 1995 WL 360526 (N.D.Ill. Aug. 6, 1998).

Holding: Court upheld an electronic discovery request to turn over 30 million pages of electronic mail at a cost of \$70,000. The court balanced the “undue burden” on the defendant against the plaintiffs’ entitlement to the production of such documents and concluded that the plaintiff class need not bear the costs caused by the defendant’s choice of electronic storage.

² Longo, Amy J., *Taking a Byte Out of Electronic Discovery – Tips for the Cyber Litigator*, Litigation News, November 2001, Vol. 27, No. 1.

³ No author was identified in the materials.

Williams v. Owens-Illinois, Inc., 665 F.2d 918 (C.A.Cal. 1982).

Holding: The court of appeals upheld trial court order that denied plaintiffs' request for the actual computer tapes since the information on the tapes was included in already discovered material.

Fennell v. First Step Design, Ltd., 83 F. 3d 526 (1st Cir. 1996)

Holding: The court held that discovery of files on a computer hard drive may be appropriate in some cases, but was not appropriate because the plaintiff failed to show a "particularized likelihood of discovering appropriate information."

Danis v. USN Communications, Inc., No. 98 C 7482, 2000 U.S. Dist LEXIS 169800 (N.D. Ill October 23, 2000).

Holding: Plaintiffs filed motion alleging that defendants were responsible for supervised, or permitted the destruction of crucial evidence electronically stored. The court held that while plaintiffs had shown that the document preservation requirement was not fully met, plaintiffs had fallen far short of substantiating their assertions that the individual defendants engaged in intentional destruction.

Bills v. Kennecott Corp., 108 F.R.D. 459 (D.C.Utah 1985).

Holding: Court refused to shift the cost of discovery of computer tape and printout of computer data holding that parties requesting cost-shifting must show "undue" expense or burden.

Sattar v. Motorola, 138 F.3d 1164 (7th Cir. 1998).

Holding: In this appeal of a religious discrimination case, plaintiff complained that the district court erred in refusing to compel Motorola to produce 210,000 pages of hard copy e-mails at its own expense. The district court's solution - some combination of downloading the data to computer disks or a hard drive, loaning Sattar the appropriate software, and allowing Sattar access to the Motorola system - was reasonable. If none of these were feasible, the court also approved the district court's order to split the cost of copying between the two parties.

Linnen v. A.H. Robbins Company, Inc., 1999 WL 462015 (Mass. Super. 1999).

Holding: Plaintiffs in this wrongful death suit sought restoration of back-up tapes containing electronic mail. Plaintiffs further alleged that defendant, Wyeth-Ayerst Laboratories, engaged in spoliation by continuing its practice of recycling back-up tapes after a court order and discovery request which protected the destroyed data. The costs of restoration was likely exceed \$1 million. The court began with the presumption that a discovery request for data in electronic form is not materially different from a request for data on paper. "To permit a corporation such as Wyeth to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results." Accordingly, the court imposed sanctions on the defendant because of its non-cooperation and delay in discovery and further held that the defendant engaged in spoliation by continuing to recycle back-up tapes after the court order protecting the tapes.

5. Special Types of "Document" Requests to Consider

a. Backup Tapes.

One of the most fertile sources of evidence is the routine backup created to protect data in case of disaster. This information is normally stored on high-capacity tapes, but may exist on virtually any type of media. Backup tapes normally contain all of an organization's data, including e-mail, as of a certain date. Common procedures call for full backups to be made weekly, with the last tape of the month saved as a monthly backup. While weekly backups are normally rotated, monthly backups are saved anywhere from six months to several years.

When collecting backup tapes in discovery, make sure to gather information on how the tapes were made. This inquiry must include both the procedures followed and the specific hardware and software used to make the backups. Over time, hundreds of different backup methods have been used; in some

cases, it may be impossible to restore backups without using the same software and/or hardware that was used to create them. In addition, determine:

- Written and unwritten policies and practices
- Locations of storage
- Schedules of tape rotation, retention, reuse, index, storage
- Type of backup: full, differential, or incremental
- Timing: monthly, weekly, permanently, incrementally
- Archives: files, backup
- Individual practices in addition to system wide backup

b. Computer Disks

Data that has been selectively saved by users to diskettes or other portable media is another fertile, but often overlooked, source of evidence. Users save data to diskettes for any number of reasons. They create “ad hoc backups” of key documents or files; they copy e-mail files to prevent them from being deleted in automatic purging routines. Finally, users will use diskettes to save data they do not want to keep on company computers.

The users who create them keep disks indefinitely. Collecting and examining all diskettes created by key witnesses is an essential step in a thorough examination of all electronic evidence.

6. Computer System Discovery – Examples

The following are sample discovery and questions to 30(b)(6) witnesses were prepared by Computer Forensics, Inc., a consulting company specializing in electronic discovery. All discovery listed can be found at their website at www.forensics.com.

Litigants are reminded that the number of questions allowed in discovery, whether in state or federal court, is subject to numerical limitations. Accordingly, use of all the following interrogatories and production requests could impair efforts to conduct traditional (and often more productive) discovery. As with all recommendations in these materials, pick and choose as is relevant to the instant case.

a. Interrogatories

1. Describe in detail all of your computer systems, including, but not limited to, the number and types of computers and the type(s) of operating system(s) and application software packages used.
2. For each of the following persons [name key witnesses] provide a detailed description of every computer system(s), he or she uses for [identify subject matter, employer’s name or other] including desktop computers, personal digital assistants (PDAs), portable, laptop, and notebook computers. If individuals use home computers for business purposes, please include information concerning these systems. Please reply as specified below:
 - (a) computer type, brand, model and size of hard drive.
 - (b) brand and version of all software, including operating system, private and custom developed applications, commercial applications and shareware.
 - (c) communications capability, including, but not limited to, terminal to mainframe emulation, data download and/or upload capability to mainframe, and computer to computer connections via network, modem and/or direct connection.
3. Provide the following information for each computer network in operation in the organization:
 - (a) brand and version number of the network operating system in use;
 - (b) quantity and configuration of all network servers and workstations;

- (c) identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the network;
- (d) brand name and version number of all application and other software residing on the network, including, but not limited to electronic mail applications.

4. Provide the following information for each mini- and mainframe computer system used in the organization:

- (a) brand and version number of the operating system in use;
- (b) identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the mini- and/or mainframe system;
- (c) name and description of function of all application and other software residing on the network, including, but not limited to electronic mail applications.

5. Describe in detail all inter-connectivity between DEFENDANT A's computer system, DEFENDANT B's computer system, (ETC.). This description should include all possible ways in which electronic data is shared between organizations, the method of transmission, type(s) of data transferred and the names of all individuals possessing the capability for such transfer, including lists and names of authorized outside users of the [producing party's] electronic mail system.

6. Please provide the following information concerning data backups performed on all computer systems used in the organization:

- (a) descriptions of any and all procedures and/or devices used to backup the software and/or data, including, but not limited to, name(s) of backup software used, tape rotation schedule, type of tape backup drives including name and version number;
- (b) are multiple generations of backups maintained? If so, please describe how many and whether the backups are full or incremental;
- (c) is backup storage media kept off-site? If so, where is such media kept? Describe the process for archiving and retrieving off-site media;
- (d) is backup storage media kept on-site? If so, where is such media kept? Describe the process for archiving and retrieving on-site media;
- (e) who conducts the backup;
- (f) what information is backed up; and,
- (g) please provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup and a description backup content.

7. May users store voice mail messages? If so, please provide the following information:

- (a) Do users have the option of storing voice mail messages?
- (b) If users can store messages, how long do they remain on the system? How many messages may be stored by the user?
- (c) Are voice mail messages automatically purged? If so, describe the destruction schedule.

b. Requests for Production

1. Written policies, procedures and guidelines as they relate to computers, electronic data, and electronic media as they relate to:

- (a) File naming conventions and standards

- (b) Diskette labeling standards
 - (c) Back up tape rotation schedules
 - (d) Electronic media retention/destruction schedules
 - (e) Corporate policies concerning employee use of company computers and data
2. Organization charts for entire company. [To gain information about the structure and chain of command for Information Services departments or divisions.]
 3. Back up tapes containing relevant material - identify individuals or work groups if appropriate, and type of data requested (i.e. e-mail, voice mail) for the time period of _____ to [the present?].
 4. Exact copies (sometimes referred to as image copies, evidentiary copies) of relevant hard drives on desktop, laptop, notebook, palm top or personal digital assistant computers.
 5. Exact copies (sometimes referred to as "diskcopies") of relevant diskettes.

c. Questions for Deposition of Custodian of Electronic Records

System Profile

1. Describe the types of computer system(s) used by your company in the course of business
2. Describe/identify the type of software used on your computer system(s)
3. Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup and upkeep of the computer system.
4. Does the staff [or inquire of key witnesses] have home computers used for business purposes? (If yes, repeat questions 1-2).
5. Are passwords or encrypted files used on any of the computer systems? If yes:
 - (a) Describe how files are protected
 - (b) Who could provide access codes if required?
6. Have you modified your use of computers to comply with recent discovery requests?

Backup and Retention

7. List all computer systems in the organization that are backed up.
 - (a) Describe the backup program(s) used. (Ex: ARCserve, StorageExpress, Maynard, Tecmar, etc.)
 - (b) Give details of your backup procedures.
8. Have you modified your backup procedures to comply with recent discovery requests?
9. Are files ever deleted from the computer system(s)?
10. Are archival backups ever created? If yes:
 - (a) What files have been archived?
 - (b) Where are the archival backups maintained?
11. Describe any disaster recovery plans in place now and for the relevant time period.

Maintenance and Access

12. Are utility programs used on computer(s) in the office? (Ex: Norton Utilities, MacTools, network maintenance programs) If yes:
 - (a) Which program(s)?

- (b) Has the program been used to permanently “wipe” files? (When?)
- (c) Has the program been used to de-fragment, optimize or compress drives? (When?)
- 13. How do those outside of the company access the computers?
- 14. How are office computers secured?
- 15. Have any computer hardware been upgraded in the past 12 months?
- 16. Has any computer software been upgraded or replaced on office computers in the past 12 months?

Chain of Custody/Authentication

- 17. Are individual directories purged when an employee leaves the company?
- 18. Are passwords and access codes revoked when an employee leaves the company?
- 19. Are workstations reassigned to incoming employees? If yes:
 - (a) Are hard drives wiped or re-formatted for the new user?
 - (b) Are hard drives backed up before the new user takes system?
- 20. Describe how used or replaced equipment is disposed of or sold
- 21. Describe how used disks or drives are treated before destruction or sale. (Degaussed? Shredded?)
- 22. Have you used outside contractors to upgrade either hardware or software? (If so, please identify)
- 23. Are changes or modifications made to software recorded? (Electronically? Are hard copy logs kept?)

B. Deposition Issues for All Witnesses

1. Determination of All Witness’ Computer Usage.

In addition to the discovery directed at the computer system, each witness must be questioned about his or her computer use. Individual users’ sophistication varies widely; knowing how each witness uses his or her computer and organizes and stores data may lead to sources of information not revealed by the discovery directed at general system usage. This discovery should also focus on the secretaries and other people assisting key witnesses. Often, documents drafted by the key witness are stored on an assistant’s computer.

Perhaps the most overlooked source of electronic evidence is the home computer. Data usually ends up on these machines in one of two ways: First, it can be transferred to and from the workplace on diskettes or other portable media; second, an employee may be able to log on to the company network from home. In this latter situation, the home computer acts just like the employee’s office workstation. Laptop computers, which are often shared among a number of users, are also good sources of evidence.

V. Presenters

Jeffrey A. Brauer, Esq.
Vice Chair – YLD Litigation Section c/o
Hahn Loeser & Parks LLP
3300 BP Tower
200 Public Square
Cleveland, Ohio 44114
(216) 274-2371
fax: (216) 274-2571
email: jabrauer@hahnlaw.com
www.hahnlaw.com

Richard E. Weber, Esq.
President
Advocate Solutions
65 E. Wacker Place
Suite 2300
Chicago, IL 60601
(312) 857-9800
fax: (312) 857-9801
email: rew@advocatesolutions.com
www.AdvocateSolutions.com

Sponsoring Section: ABA YLD Litigation Section

ABA Spring YLD Conference
Denver, Colorado
May 2002