# I. ELECTRONIC DISCOVERY: DEFINITIONS AND USES

## A. What Is Electronic Discovery?

Electronic discovery includes requests for and production of information that is stored in digital form.[1] In short, electronic discovery is the discovery of electronic documents and data.[2] Electronic documents include virtually anything that is stored on a computer such as e-mail, web pages, word processing files, and computer databases.[3] Electronic records can be found on a wide variety of devices such as desktop and laptop computers, network servers, personal digital assistants and digital phones.[4] Documents and data are "electronic" if they exist in a medium that can only be read by using computers such as cache memory, magnetic disks (for example computer hard drives or floppy disks), optical disks (for example DVDs or CDs), and magnetic tapes.[5] Electronic discovery is frequently distinguished from traditional "paper discovery," which is the discovery of writings on paper that can be read without the assistance of computers.[6]

## B. Why E-Discovery Can Be Valuable in Litigation

With the advancement of technology, electronic discovery is not only valuable in litigation, it is essential. Electronic evidence is affecting virtually every investigation today whether it is criminal or civil.[7] Usually, there are no longer "paper-trails" that establish who did what and when.[8] Instead, electronic evidence is providing the clues to understanding what actually happened.[9] Consider these statistics regarding the electronic evidence explosion:

- "In 2002, the International Data Corporation estimated that 31 billion e-mails were sent daily. This number is expected to grow to 60 billion a day by 2006.
- Most companies store up to 70 percent of their records in electronic form.
- Within ten years, the total number of electronic records produced on the planet could be doubling every sixty minutes."[10]

- "Ninety-three percent of all business documents are created electronically, and most are never printed."[11]

- By 2005 corporations are expected to generate 17.5 trillion electronic documents annually.[12]

One example of how electronic discovery can be valuable in litigation is in the civil suit brought by New York Attorney General Eliot Spitzer against the insurance brokerage arm of Marsh & McLennan charging the company with price fixing and collusion in October of 2004.[13] The complaint accused Marsh "of steering clients to favored insurers and working with major insurers to rig the bidding process for property-casualty insurance coverage."[14] Spitzer relied on pivotal internal e-mails and memoranda in which insurance executives were alleged to have openly discussed actions focused on maximizing Marsh's revenue and insurance companies' revenue, without any regard to their clients, who ranged from large corporations to school districts and individuals.[15]

One Marsh executive is alleged to have solicited an insurance company's participation in a phony bid meeting so that Marsh could maintain the illusion of competition, while at the same time steering business to another insurance company that had already agreed to pay kickbacks.[16] In his e-mail to the insurance company, the executive stated: "This month's recipient of our Coordinator of the Month Award requests a body at the rescheduled April 23 meeting . . . He just needs a live body . . . Given recent activities perhaps you can send someone from your janitorial staff – preferably a recent hire from the U.S. Postal Service."[17] Even if there was an innocuous reason for the e-mail, a jury would be likely to view it skeptically.[18]

### C. How Does Electronic Discovery Differ from Traditional Methods of Discovery?

Electronic discovery differs from traditional methods of discovery in that electronic documents present unique opportunities for obtaining information and special problems during document production.[19] There are numerous ways that producing electronic documents is different from production of paper documents. These differences can be grouped into several categories.

### 1. Greater Volume and Locations

First, the volume and number of locations of electronic documents is much greater than that of conventional documents.[20] As discussed above in section (I)(B), the number of electronic documents in existence and constantly being created is staggering. Part of the reason that the volume of electronic documents is so high is that electronic documents can be more easily duplicated than paper documents.[21] For example, e-mail users often send the same e-mail to numerous recipients, and then that e-mail is forwarded on to others.[22] Moreover, the search locations for electronic documents include far more locations than the filing cabinets typically involved with paper documents. Electronic documents are contained in computer hard drives, network servers, backup tapes, e-mail servers, outside computers, servers and backup tapes, laptop and home computers, and personal digital assistants.[23]

### 2. Durability

In some ways electronic documents can be difficult to maintain, and in others, they can be almost impossible to destroy. Since computers automatically recycle and reuse memory space, overwrite backups, change file locations and otherwise maintain themselves automatically, electronic documents can be easily damaged or altered without any human intent, intervention or even knowledge.[24] On the other hand, while a shredded paper document is basically irretrievable, "deleting" an electronic document usually does not mean that the document is actually erased.[25] Instead of erasing the data in the disk directory, it changes to a "not used" status, which allows the computer to write over the "deleted" data.[26] By searching the disk itself rather than the disk's directory, this "deleted" information can be retrieved at anytime until the computer writes over this data. Therefore, data is recoverable long after it has been "deleted" by the user, even if the computer user or the computer itself does not know of its existence.[27]

### 3. Metadata and System Data

Electronic documents contain additional information that paper documents cannot provide including metadata and system data.[28] Metadata is information imbedded in an electronic file that contains information about the file such as the date of creation, author, source, and history.[29] Metadata will be more fully discussed in section IV. System data refers to computer records about the computer's use, such as when a user logged on or off, the web sites the user visited, passwords used, and documents that were printed or faxed.[30]

### 4. Obsolescence

The frequent obsolescence of computer systems due to changes in technology also creates unique issues in electronic discovery that are not presented in the recovery of paper documents.[31] When turnover in computer systems occurs, "neither the personnel familiar with the obsolete systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when this 'legacy data' needs to be accessed."[32]

## D. Distinguishing Between Electronic Litigation Support (E-Production) and E-Discovery

Electronic litigation support includes the tools that can be used to manage electronic data once it is received during electronic discovery. A search of the world wide web returns numerous references to products to assist with the management of facts and documents in today's litigation. While these products proclaim various "bells and whistles," most products provide the following general functions:

- Finding, reviewing and managing documents
- Annotations, on-line redaction, customizable document folders, automated Bates numbering and document branding
- Searching testimony, linked exhibits and relevant documents

- Production options that include exporting documents to CD or other media

These applications provide help not only with organizing and managing documents but also in maximizing the advantages associated with the migration of business away from file cabinets to electronic media storage.

To effectively manage electronic data, you must first ask for and demand that the opposing party produce the documents in the original electronic media. To do so may require the retention of a computer forensic expert, who can help to (1) retrieve information from backup tapes or legacy ("old and out of use") systems, from standard systems to arcane or uncommon file types, and to (2) narrow the set of potentially responsive documents to avoid wasting resources or being inundated with useless information. The type of data management tool to be used will dictate the file format to be requested in discovery so that the electronic data is produced in a form that is immediately useable.

The importance of asking for the original electronic media is readily apparent. The electronic copy of a document contains useful information not available in the paper copy, such as metadata, which is discussed supra.

Although the costs associated with the use of these programs may make it impractical for use in smaller cases, some type of fact and document database is essential for cases with large amounts of documents, especially where electronic files are being produced. Recognizing the need, the market has responded with a number of different programs. These programs, however, can be broken out into two basic types: (1) those requiring software on the user's workstation and dedicated hardware, and (2) those that have web-based repositories. Summation (www.summation.com)[33] and Applied Discovery, Inc. (www.applieddiscovery.com) are examples of each. Which application you ultimately choose will depend on a variety of factors, including:

- Resources (both monetary and technical) - Do you have on-site staff and available electronic storage space?

- The number of users and their locations - Do you have multiple offices involved, does your client want direct access?

- The volume and form of the documents - How many documents do you have in paper form only, does the volume make it unmanageable to have hard copies only?

- The complexity of the matter - Will you need to create numerous customized files, how many people will be reviewing documents?

- The location of depositions and the trial - Will you have access to the internet?

Regardless of which application you ultimately choose, some general best practices exist for getting the most out of your data management system. While no two cases are identical, optimal use of a data management system depends on good data collection protocols and a sound and a thoughtful data management plan.

### E. Advantages and Disadvantages to Electronic Discovery

Despite all of the difficulties that electronic discovery presents, there are a few advantages. Electronic discovery can help realize significant litigation efficiencies.[34] Through automated methods, some forms of electronic documents and electronic media can be searched quickly and fairly accurately.[35] For some electronic documents, software may be capable of searching through far more documents than human beings could ever review manually.[36] Moreover, as discussed supra, metadata and system data provide additional information about electronic documents and actions of computer users that are not available with traditional paper discovery.

There are numerous disadvantages to electronic discovery. Attorneys must devote considerable time and effort to understanding and developing new approaches to electronic discovery even when they are quite experienced and skilled in traditional, paper discovery. The volume and dispersion of electronic documents can make them difficult to find.[37] The complexity of dealing with unfamiliar technology may necessitate calling in computer forensic experts to help with electronic discovery.[38] Clients and adversaries can be sanctioned for improper document retention practices based on rapidly evolving criteria.[39] Furthermore, electronic discovery can increase discovery costs many times over.[40]

## F. Who Pays for E-Discovery?

Ordinarily, there is a presumption under the American Rule that each party will bear its own costs of production.[41] However, courts are becoming more likely to shift part of the costs to the requesting party under certain circumstances.[42]

### 1. Shifting the Costs of Producing Discovery in the Requested Format

If the discovery does not already exist in the requested format, then a court may order the producing party to convert the discovery into a reviewable electronic format. The court, however, may order this conversion only if the requesting party agrees to pay part or all of the costs:

- Clever View Investments, Ltd. v. Oshatz, 2006 U.S. Dist. LEXIS 5006 (S.D.N.Y. Feb. 8, 2006) Defendants ordered to pay 40% of the cost of copying document they requested after plaintiff demonstrated that at least some of the documents were available by other means.

- Portis v. City of Chicago, 2004 U.S. Dist. LEXIS 24737 (Dec. 7, 2004). Court ordered defendant to pay 50% of plaintiff's cost to gain access to database created by plaintiffs.

- Wiginton v. CB Richard Ellis, Inc., 229b F.R.D. 568, 2004 U.S. Dist. LEXIS 175722 (N.D. Ill. Aug. 10, 2004). The defendant employer sought to shift some or all of the costs of recovering backup e-mails produced to plaintiff employees. The court found that the presumption that the responding party pays for discovery was partially overcome, and three-quarters of the discovery costs should be shifted to the plaintiffs.

- In re Bristol-Myers Squibb Sec. Lit., 205 F.R.D. 437, 440-441 (D.N.J. 2002). The court held that the requesting party pay for its electronic copies of discovery but not the costs of creating the original electronic version.

- Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1996 WL 22976, 1996 U.S. Dist. LEXIS 563 (S.D.N.Y. Jan. 23, 1996). The court rejected the plaintiff's argument that it did not have the resources to pay for the conversion and ordered the plaintiff to pay the defendant's costs in extracting the data.

- In re Air Crash Disaster at Detroit Metro. Airport on Aug. 16, 1987, 130 F.R.D. 634, 636 (E.D. Mich. 1989). The court ordered the plaintiff to convert a simulation program and data on a nine-track magnetic tape if the defendant agreed to "pay all the reasonable and necessary costs that may be associated with the manufacture of the computer-readable tape."

As can be seen, courts have not been consistent in requiring the requesting party to pay the whole cost associated with reproducing the discovery in an electronic format. Therefore, a requesting party should be clear in its discovery requests the format of documents it is requesting and a producing party should produce the discovery in the format the data is kept in the normal course of business.

### 2. Shifting the Costs Associated with Collecting and Producing Electronic Evidence

The costs associated with collecting and producing electronic data also may be shifted to the requesting party when the producing party argues that the requested production would be an undue hardship or that the expense outweighs any benefit in the discovery. This willingness to shift costs differs from the early approach taken by courts that the additional costs in producing electronic data stemmed from the decision of the responding party to store the data electronically and therefore should not be shifted to the requesting party. Dunn v. Midwestern Indemnity, 88 F.R.D. 191 (S.D. Ohio 1980).

Courts currently consider two different, but related, sets of factors in determining whether to shift part or all of the costs associated with discovery to the requesting party:

- Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 429 (S.D.N.Y. 2002). The court considered the following eight factors: "(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 incentives to do so; and (8) the resources available to each party."

- Zubulake v. UBS Warburg, 217 F.R.D. 309, 320 (S.D.N.Y. 2003). The court modified the above Rowe factors to prevent "undercut[ting] th[e] presumption" that the responding party should bear the cost of production. The Zubulake factors are as follows: "(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." Id. at 322.

Judges, however, do not vigorously apply the Zubulake factors in all cases to determine whether to shift costs. For example, in OpenTV v. Liberate Tech., 219 F.R.D. 474 (N.D. Cal. 2003), the court applied the Zubulake factors and determined that factors one and two relating to the marginal utility and factors three and five relating to the costs weighed against shifting the costs to the requesting party. Id. at 478-79. Factor six was neutral and only factors four and seven weighed in favor of shifting the costs. Id. The court ordered the parties to evenly split the costs of production "[b]ecause of the undue burden and expense involved in extracting and copying the source code . . . . The [c]ourt finds that because the parties are similarly situated, they are to split equally the cost of extraction of the source code . . . ." Id. at 479. The responding party also was to bear the cost of copying the source code once extracted because "the responding party should always bear the cost of reviewing and producing electronic data once it has been converted to an accessible form." Id. (citing Zubulake, 216 F.R.D. at 290).

The future of shifting the costs associated with extracting and producing electronic data remains unclear. Parties, on both sides, should be prepared to argue the burden, expense and benefit of the discovery if the issue becomes a factor.

### G. Negotiating the Parameters of E-Discovery with the Other Side

Early on in the case, before the Rule 26 conference, both parties are required to meet and negotiate regarding electronic discovery to avoid disputes over scope, burdens and costs.[43] The party or parties seeking electronic evidence should use the conference to determine what electronic evidence might exist and what computer and expert resources may be necessary in order to obtain the evidence.[44] One approach is to have the respective parties' technical people come to the meet-and-confer session (possibly under the cloak of an appropriate protective order, so that the meeting does not turn into a surprise deposition), which can eliminate confusion and expedite the process of formulating a realistic discovery plan.[45] Another idea is to have your expert informally interview the opposition's most knowledgeable information specialist.[46] In the meeting, the producing party has an incentive to face discovery questions early and determine to the extent possible the scope of the duty to preserve evidence.[47] In addition, the parties can narrow the task of dealing with electronic information early by stipulating to what electronic information must be retained and what may be ignored.[48]

### H. When Is It Time to Call in the Experts?

Before determining whether it is appropriate to hire an expert, it is necessary to determine whether electronic discovery will be involved in a case in the first place. In some cases, electronic discovery is not at issue. If electronic discovery has not been requested by the other side, an attorney must first decide whether to raise the issue at all based on what electronic data may be recovered and how valuable such data might be.

Once electronic discovery is at issue, a computer forensic expert may be an extremely useful and even essential addition to a litigation team when considering, seeking, or producing electronic discovery.[49] For most legal professionals, their technical proficiency has not matched the pace of the increased role that technology plays in the ways that businesses are transferring and storing information.[50] The decision of whether to hire an expert involves a cost-benefit analysis. Attorneys facing this decision must first examine internal resources and decide whether they have the time and expertise to do the electronic discovery. Since any request for electronic discovery is likely to be similarly requested by the opposition in retaliation, it is necessary to determine how complex both the client's and opponent's systems are.

The practitioner must have a working knowledge of the information system that is the target of the search. This knowledge includes the file types and storage media. Common storage media include:

- DVD
- CD-ROM
- Hard drives (IDE, SCSI, USB, Firewire)
- Laptop Computers
- Desktop Computers
- Zip drives
- Jaz drives
- Floppy diskettes
- Backup Tapes (DAT, DLT, AIT)
- PDAs and Cell Phones

Common file types include:

- **E-mail programs** - such as Microsoft Outlook, Microsoft Outlook Express, Microsoft Mail, Lotus Notes, Lotus cc:Mail, Eudora, Novell Groupwise, UNIX mail, and AOL

- **Spreadsheet Programs** - such as Microsoft Excel, Lotus 1-2-3, QuatroPro

- **Database Programs** - such as Microsoft Access, Paradox

- **Word Processing Programs** - such as Microsoft Word, Corel WordPerfect, Lotus WordPro

- **Presentation Programs** - such as Microsoft PowerPoint and Lotus Freelance

- **Project Management Programs** - such as Microsoft Project

- **Computer Aided Design Programs** - such as Microsoft Visio

- **Programming Languages** - such as C++, Java

- **Multiple Image File Formats** - such as text files, image files (TIFF, JPG, JPEG, GIF, EPS, PCX, BMP, WMF), HTML or compressed file formats

In addition, there must be an assessment of the complexity of the case including what types of parties are involved (such as a large corporation or an individual), what kinds and how much data is likely to be relevant to the case, how many witnesses will be involved, and how significant the case is (how much is at stake)? What are the risks involved with not retaining an expert? What are the expected benefits of hiring an expert? Consulting IT sources and a forensic expert may help in making this assessment. Once the decision to retain an expert is made, it is best to obtain that expert as early as possible so that the expert can help to formulate a discovery plan.

## I. Key Terminology You Should Know[51]

Active Data: Active Data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction.

Analog: Describes the recording format of real events. Analog devices such as older video and audio recording devices record real events in real time using film or audiotape. This is different from digital, where digital devices record real events into 1's and 0's for computer use.

ANSI (American National Standards Institute): Is the institute that develops standards for items like computers and software that are purchased or sold by the government.

API (Application Program Interface): Is a term used to describe the "hooks" available to "integrate" programs with each other. For example API's are available for Microsoft Access™ to integrate or communicate with an image application program.

Application: Software programs, such as word processors and spreadsheets that most users use to do work on a computer.

Applications Program Software: Are computer programs that perform a wide range of tasks and generally designed for specific purposes. Microsoft Word™ and WordPerfect™ were designed for word processing, Summation™ for database and full text document search and retrieval, and Lotus 123™ for a spreadsheet. They are also referred to as a application or program.

Archival Data: Archival Data is information that is not directly accessible to the user of a computer system but that the organization maintains for longterm storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

Archiving: Is the process of putting data on disks for long-term storage. Back-ups are used to ensure data is saved in case of data loss.

Artificial Intelligence (AI): Is the field of computer science in which computers are programmed to exhibit characteristics of human intelligence. It attempts to model the way humans think.

ASCII (Acronym for American Standard Code: ASCII is a code that assigns a number to each key on the keyboard. ASCII text does not include special formatting features and therefore can be exchanged and read by most computer systems.

Back-up: To create a copy of data as a precaution against the loss or damage of the original data. Most users backup some of their files, and many computer networks utilize automatic backup software to make regular copies of some or all of the data on the network. Some back-up systems use digital audio tape (DAT) as a storage medium.

Back-up Data: Back-up Data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster.

Back-up Tape: See Disaster Recovery Tape.

Back-up Tape Recycling: Back-up Tape Recycling describes the process whereby an organization's back-up tapes are overwritten with new back-up data, usually on a fixed schedule (e.g., the use of nightly backup tapes for each day of the week with the daily back-up tape for a particular day being overwritten on the same day the following week; weekly and monthly back-ups being stored offsite for a specified period of time before being placed back in the rotation).

Bandwidth: The amount of information or data that can be sent over a network connection in a given period of time. Bandwidth is usually stated in bits per second (bps), kilobits per second (kbps), or megabits per second (mps).

Bernoulli Box: Is a storage disk system that uses fluid dynamics to keep the disk floating in the air as data is accessed or written to the disk.

Binary: Mathematical base 2, or numbers composed of a series of zeros and ones. Since zero's and one's can be easily represented by two voltage levels on an electronic device, the binary number system is widely used in digital computing.

BIOS (Basic Input/Output System): Are instructions that tell the computer how to control the information between computers and peripherals.

Bit: A measurement of data. It is the smallest unit of data. A bit is either the "1" or "0" component of the binary code. A collection of bits is put together to form a byte.

Bitmap: Represents characters or graphics by individual pixels or dots. They are arranged in columns and rows and can be altered with paint programs. Bitmap graphics, also called raster graphics, are images created with pixels.

Blowback: Is a slang term for printing images off of a CD-ROM disk.

Boot/Reboot: Is the start up procedure for a computer.

Bps (bits per second): Is the transmission speed between two computers.

Browser: Is software, like Internet Explorer™, that is used to view web pages on the Internet or Intranet. It is the client's software used to view sites located on servers running web server software.

Bulletin Board Service (BBS): Is the early forerunner to group computing systems. They permit users to exchange e-mail, retrieve files and share other computer functions between individuals who share common interests.

Burn: Slang for making (burning) a CD-ROM copy of data, whether it is music, software, or other data.

Byte: Eight bits. The byte is the basis for measurement of most computer data as multiples of the byte value. A "megabyte" is one million bytes or eight million bits or a "gigabyte" is one billion bytes or eight billion bits.

1 gigabyte = 1,000 megabytes

1 terabyte = 1,000 gigabytes

Cache: A type of computer memory that temporarily stores frequently used information for quick access.

CAD (Computer Aided Design): Is a computer program that assists in designing products, buildings, houses, highways and so forth.

CD-ROM: Data storage medium that uses compact discs to store about 1,500 floppy discs worth of data.

CGI (Common Gateway Interface): Is the standard used for connecting web pages with underlying data. A CGI script has the capability of calculating mortgages, accessing databases for reports, etc.

Character: Is equal to a byte or 8 bits and is a single letter or number.

Character Recognition: Or OCR is the ability of a scanner to convert printed text into ASCII text for use in a computer program such as a word processor.

Chat (online): Is the real-time simultaneous communication between two or more people using a computer.

Client/Servers: Is a type of computing that intelligently divides tasks between clients and servers. Client/server networks use a dedicated computer called a server to handle file, print and other services for client users, usually desktop computers. This system is contrasted with mainframe computers.

Communications Program: Is software that controls the transfer of data from one computer to another.

Compact Flash (CF): Is a popular memory card developed by SanDisk (www.sandisk.com) and uses flash memory to store data on a very small card.

Compatibility: Describes the capability of a piece of hardware or software to operate with another piece of software or hardware. For example word processing files from WordPerfect™ are not compatible with the Microsoft Word™ word processor, unless a conversion program is first used.

Compression: A technology that reduces the size of a file. Compression programs are valuable to network users because they help save both time and bandwidth.

Computer: Is an electronic machine that enables one to input, manipulate, store and output electronic information.

Computer File: Is a collection of computer commands and information stored in a file.

Computer Forensics: Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

Computer Forensic Expert: Provides expertise regarding the generation, storage, recovery, location, discovery and disclosure of computer evidence.

Cookie: Small data files written to a user's hard drive by a web server. These files contain specific information that identifies users (e.g., passwords and lists of pages visited).

CPU (Central Processing Unit): Is the main core of a computer. Often called the brain of the computer, it controls the interpretation and execution of computer instructions.

Cursor: Is the small dash or image on the computer screen that constantly blinks and moves when the mouse or other pointing device is manipulated.

DAT: Digital Audio Tape. Used as a storage medium in some backup systems.

Data: Information stored on the computer system, used by applications to accomplish tasks.

Data Communications: Is the transfer of data between two computer points.

Database: Is simply a collection of mutually related data or information stored in computer record fields. It is data that has been organized and structured for a particular purpose such as an employee benefit system.

Database Management Systems (DBMS): Is the task of managing data in databases and retrieving information from that database.

Data Mining: "Data Mining" generally refers to techniques for extracting summaries and reports from an organization's databases and data sets. In the context of electronic discovery, this term often refers to the processes used to cull through a collection of electronic data to extract evidence for production or presentation in an investigation or in litigation. Data mining can also play an important role in complying with data retention obligations under an organization's formal document management policies.

Data Transfer Rate: Is the rate of data transfer from one device to another. The higher the transfer rate, the faster the access to the data.

De-Duplication: De-Duplication ("De-Duping") is the process of comparing electronic records based on their characteristics and removing duplicate records from the data set.

Deleted Data: Deleted Data is data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

Deleted File: A file with disk space that has been designated as available for reuse. The deleted file remains intact until it has been overwritten with a new file.

Deletion: Deletion is the process where data is removed from active files and other data storage structures on computers and rendered inaccessible except using special data recovery tools designed to recover deleted data. Deletion occurs in several levels on modern computer systems: (a) File level deletion: Deletion on the file level renders the file inaccessible to the operating system and normal application programs and marks the space occupied by the file's directory entry and contents as free space, available to reuse for data storage. (b) Record level deletion: Deletion on the record level occurs when a data structure, like a database table, contains multiple records; deletion at this level renders the record inaccessible to the database management system (DBMS) and usually marks the space occupied by the record as available for reuse by the DBMS, although in some cases the space is never reused until the database is compacted. Record level deletion is also characteristic of many e-mail systems. (c) Byte level deletion: Deletion at the byte level occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file's content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.

Desktop: Usually refers to an individual PC - a user's desktop computer.

Device Drivers: Control attached peripheral devices such as a mouse, scanners and other devices.

Digital: Storing information as a string of digits - namely "1"s and "0"s.

Digital Cameras: Are cameras that translate real events or pictures directly into digital data.

Directory: Is the location where files and subdirectories are located on the computer.

Digitize: Is the process of converting information such as a document into binary code. Documents can be converted into a digital format using a scanner.

Disaster Recovery Tape: Disaster Recovery Tapes are portable media used to store data that is not presently in use by an organization to free up space but still allow for disaster recovery. May also be called "Back-up Tapes."

Disc (disk): It may be a floppy disk, or it may be a hard disk. Either way, it is a magnetic storage medium on which data is digitally stored. May also refer to a CD-ROM.

Disc Mirroring: A method of protecting data from a catastrophic hard disk failure. As each file is stored on the hard disk, a "mirror" copy is made on a second hard disk or on a different part of the same disk.

Disk Drive: Is a device that enables a computer to read and write data on a disk.

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.

Document: See Rule 34 of the Federal Rules of Civil Procedure.

Document Retrieval:  Is the ability to locate, retrieve and view a document on a computer screen.

DPI (Dots Per Inch):  Is a measurement of output resolution and quality.  It measures the number of dots per square inch.  A 600 dpi document is sharper than a 200 dpi document but requires more storage space.

DVD (The Digital Versatile (Video) Disk):  Is the next-generation optical disk standard that has a storage capacity upward of 8.5 gigabytes of data and can store two hours of movies on a side.

Electronic Discovery Software:  Is software that extracts application data and metadata from computer files.

Electronic Mail:  Electronic Mail, commonly referred to as e-mail, is an electronic means for communicating information under specified conditions, generally in the form of text messages, through systems that will send, store, process, and receive information and in which messages are held in storage until the addressee accesses them.

Encryption:  A procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it.

Ethernet:  A common way of networking PCs to create a LAN.

Expansion Cards:  Are integrated circuit cards that can be added to your computer to expand its capabilities.  For example, a network card can be added to your computer to give it the capability to connect it to a network.

Extranet:  An Internet based access method to a corporate intranet site by limited or total access through a security firewall.  This type of access is typically utilized in cases of joint venture and vendor client relationships.

Fax/Modem:  Is a device that can send or receive faxes.

Fiber Optic Cable: Is cable made from thin strands of glass through which data is transported. It is an excellent conduit to transfer data for medium or long distances, but is more expensive than normal cable.

Field: Is the location on a database computer input form to collect specific data such as name, address, phone number and social security number.

Field Name: Is the labeled area such as "Last Name," "First Name," "Address" and "Social Security Number" on a database input form.

File: A collection of data of information stored under a specified name on a disk.

File Extension: A tag of three or four letters, preceded by a period, which identifies a data file's format or the application used to create the file. File extensions can streamline the process of locating data. For example, if one is looking for incriminating pictures stored on a computer, one might begin with the .gif and .jpg files.

File Format: Defines the way the data is stored in a computer file and subsequently displayed on a screen or in print.

File Name: Is the name given to a computer file. Each computer file has a name associated with it.

File Server: When several or many computers are networked together in a LAN situation, one computer may be utilized as a storage location for files for the group. File servers may be employed to store e-mail, financial data, word processing information or to back-up the network.

File Sharing: One of the key benefits of a network is the ability to share files stored on the server among several users.

Filtering: Is the process of reducing the size of the electronic file population by limiting computer information to specific criteria like keywords, names, dates, etc.

Firewall: A set of related programs that protect the resources of a private network from users from other networks.

Fixed Disk: Is another name for a hard drive.

Floppy: An increasingly rare storage medium consisting of a thin magnetic film disk housed in a protective sleeve.

Forensics: See computer forensics.

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.

Form: Is a computer database input screen that contains fields where information is to be entered. After information is entered, it is called a record. See record.

Fragmentation: On a disk occurs when parts or pieces of a single file are distributed to many different locations on a disk.

Fragmented Data: Fragmented data is live data that has been broken up and stored in various locations on a single hard drive or disk.

FTP (File Transfer Protocol): An Internet protocol that enables you to transfer files between computers on the Internet.

Full Text: Is the "full" or complete text of a document. This term usually refers to a document that has been converted for use on a computer. A "full text" document can be searched for individual words, names, dates and other information in the document.

Full Text Search: Is the capability of searching text files for words, phrases or patterns of characters. An image cannot be full text searched. It has to be retyped or OCR'ed into the computer.

GB (Gigabyte):  Is 1,073,741,824 bytes or 1024 megabytes.  This unit of measurement reflects computer memory or disk storage.

Graphics:  Are primarily computer pictures and drawings.

GIF (Graphic Interchange Format):  A computer compression format for pictures.

GUI (Graphic User Interface):  A set of screen presentations and metaphors that utilize graphic elements such as icons in an attempt to make an operating system easier to use.

Groupware:  Is software designed to assist groups in working together using computers.

Gooey:  (Slang for GUI):  Stands for Graphical User Interface.

Handwriting Recognition:  Is the technology that converts human handwriting into machine-readable ASCII text.

Hard Disk:  A peripheral data storage device that may be found inside a desktop as in a hard drive situation.  The hard disk may also be a transportable version and attached to a desktop or laptop.

Hard Drive:  The primary storage unit on PCs, consisting of one or more magnetic media platters on which digital data can be written and erased magnetically.

Hardware:  Is the physical equipment that comprises a computer system.

Home Page:  Is usually the first page of a website.  It usually contains the main menu that directs the visitor to other parts of the site that can include documents, graphics, newsletters, and other links.

HTML (Hypertext Markup Language):  A tag-based ASCH language used to create pages on the web.

Hypertext Linking:  Is the capability to link together any two separate sources of digital information and then jump to the secondary source whenever necessary.

Hz (Hertz):  Is a measurement of frequency that is defined as one cycle per second.  The higher the megahertz of a computer, the faster it will run.  A megahertz is 1,000,000 cycles per second.  Microprocessors run at speeds that are measured in MHz or millions of cycles per second.

Image:  In data recovery parlance, to image a hard drive is to make an identical copy of the hard drive, including empty sectors.  Akin to cloning the data.  Also known as creating a "mirror image" or "mirroring" the drive.

Imaging:  Is the process of using a scanner to convert a paper document into a computer electronic image.

Instant Messaging ("IM"): Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously.

Internet:  The interconnecting global public network made by connecting smaller shared public networks.  The most well known internet is the worldwide web, the worldwide network of networks which use the TCP/IP protocol to facilitate information exchange.

Intranet:  A network of interconnecting smaller private networks that are isolated from the public Internet.

IP Address:  A string of four numbers separated by periods used to represent a computer on the Internet.

IS/IT Information Systems or Information Technology:  Usually refers to the people who make computers and computer systems run.

ISP (Internet Service Provider):  A business that delivers access to the Internet.

Issue Code: Is an enhancement code used in full text or databases to indicate a specific topic or area of interest for use within litigation reports and searches.

Java: Is a programming language, owned by Sun Microsystems, that allows programmers to create web add-ons or pages that can be viewed by browsers. Generally it is used in conjunction with HTML for add-on features with web pages, though it can be used alone to create web pages.

JPEG (Joint Photographic Experts Group): An image compression standard for photographs.

KB (Kilobyte): Is a unit of measurement that equals 1,024 bytes and denotes computer memory or disk storage.

Keyword Search: A search for documents containing one or more words that are specified by a user.

Kilobyte (K): One thousand bytes of data is 1K of data.

LAN (Local Area Network): Usually refers to a network of computers in a single building or other discrete location.

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

Listserv: Is a discussion group, similar to newsgroups, where people exchange information about a variety of subjects. It uses standard Internet e-mail to exchange messages.

Load: Is when a program is copied from the hard disk into RAM memory. This occurs whenever you start a program. When you turn on your computer, the operating system program loads.

Magnetic Tape Drives: Can be external or internal and are generally used as backup devices. Magnetic tape can hold significant amounts of computer information.

Magnetic-Optic: Refers to erasable optical recording method. It is similar to a magnetic hard disk.

Megabyte (Mega): A million bytes of data is a megabyte, or simply a meg.

Memory: Is space within the computer for storing electronic data.

Menu: In a computer program, it is a list of options that you choose from to do different computer functions.

Metadata: Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or 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 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 less informative shorthand phrase "data about data," it describes the content, quality, condition, history, and other characteristics of the data.)

Megahertz: See hertz.

Microprocessor: Is the chip inside the computer that is the center of all the activity. The chip controls all the operations of a computer and is used to execute program commands. It is also known as a processor.

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.

Mirroring:  The duplication of data for purposes of backup or to distribute network traffic among several computers with identical data.

MIS:  Management information system.

Modem:  A piece of hardware that lets a computer talk to another computer over a phone line.

Mouse:  Is the primary pointing device for the Windows operating system.  When you move the mouse over a flat surface the cursor or arrow makes a movement on the screen and allows commands to be executed by pushing buttons.

MS-DOS (Microsoft Disk Operating System):  Is a user operating system.

Multitasking Operating System:  Is an operating system that enables the user to perform more than one task at a time.

Multimedia:  Is the delivery of information in multisensory ways through the integration of previously distinct media (text, graphics, computer animation, motion video, and sound).

Network:  A group of computers or devices that is connected together for the exchange of data and sharing of resources.

Network Software:  Is the operating protocol selected to run the network.

Newsgroups:  Are topic specific forums on the Internet or on local networks where people can post questions, news, and comments and/or read and respond to such postings left by other users.

Node:  Any device connected to network.  PCs, servers, and printers are all nodes on the network.

OCR:  Optical character recognition is a technology which takes data from a paper document and turns it into editable text data.  The document is first scanned.  Then OCR software searches the document for letters, numbers, and other characters.

Offline:  Not connected (to a network).

Online:  Connected (to a network).

Operating system (OS):  The software that the rest of the software depends on to make the computer functional.  On most PCs this is Windows or the Macintosh OS.  Unix and Linux are other operating systems often found in scientific and technical environments.

Optical Character Recognition:  Is the process of using a scanner and software to convert paper into a searchable machine-readable text.

Optical Drive:  Is a storage device that is written and read by a laser.  There are different types of optical disks such as CD-ROM which is read only storage media, WORM that can be written to once and read many times and WRRM which stands for write many, read many.

Parallel Port:  Is a port generally located on the back of computers and transfers data through multiple wires.  Eight bits are transferred simultaneously.  It is usually designated with the letters LPT1.

Path:  Is the directory sequence the computer must search to locate a particular file or directory.  See also directory and file.

PC:  Personal computer.

PC Cards:  Were formally called PCMCIA (Personal Computer Memory Card International Association) cards and are covered circuit boards that can be inserted into special slots on laptops. PC Cards can be hard drives, modems, network adapters, RAM (random access memory), sound cards, SCSI or cellular phone connectors and flash memory.

PDA (Personal Digital Assistant): Handheld digital organizers.

PDF (Portable Document Format): An Adobe technology for formatting documents so that they can be viewed and printed using the Adobe Acrobat reader.

Pen-Based Computing: Is a method of entering data into a computer using an electronic stylus or pen.

Pen Storage Drive: Fits into the USB port of your computer, is the size of half of a pen, and stores upwards of 10 megabytes to 1 GB of information.

Plaintext: The least formatted and therefore most portable form of text for computerized documents.

Pointer: A pointer is an index entry in the directory of a disk (or other storage medium) that identifies the space on the disc in which an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. In most cases, when an electronic document is "deleted," the pointer is deleted, which allows the document to be overwritten, but the document is not actually erased.

Port: Is a connector to a computer that allows data to be exchanged with other devices such as a printer, mouse, CD-ROM reader or external modem.

Private Network: A network that is connected to the Internet but is isolated from the Internet.

Processor: See Microprocessor

Program: See Application Program

Prompt: Is usually depicted as "C:/" or "A:/" and indicates that the computer is ready to accept input.

PST (Personal Folder File): The place where Outlook stores its data (when Outlook is used without Microsoft® Exchange Server). A PST file is created when a mail account is set up. Additional PST files can be created for backing up and archiving Outlook folders, messages, forms and files. The file extension given to PST files is .pst.

Public Network: A network that is part of the public Internet.

RAM (Random Access Memory): The working memory of the computer into which application programs can be loaded and executed.

Record: Is the name given to a database form after information has been entered.

Relational Database: Stores information in a collection of tables, each table storing information about one subject. These tables can be "related" for business or other informational purposes.

Residual Data: Residual Data (sometimes referred to as "Latest Data" or "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 file slack space; and (3) data within files that has 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.

ROM (Read Only Memory): Is the computer memory that stores instructions permanently. The ROM contains instructions that the computer uses to run properly and is executed each time the computer is turned on.

Root Directory: Is the first level direction on a computer. All other directories are subordinate to the root and are referred to as directories or subdirectories. See also Directory.

Router: A piece of hardware that routes data from a local area network (LAN) to a phone line.

Sampling: Sampling usually (but not always) refers to the process of statistically testing a data set for the likelihood of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions as to which repositories of data should be preserved and reviewed in a particular litigation, and determinations of the validity and effectiveness of searches or other data extraction procedures. Sampling can be useful in providing information to the court about the relative cost burden versus benefit of requiring a party to review certain electronic records.

Sandbox: A network or series of networks that are not connected to other networks.

Scan: Is the process of converting a document into an image or using OCR software to convert it to machine-readable text.

Scanner: Is a device that converts a document or picture into an image or machine-readable text.

Serial Port: Is the connector port on a computer that sends and receives data one bit at a time. A modem, printer or mouse can be connected to your serial port. It is usually denoted as COMI. See also parallel port.

Server: Any computer on a network that contains data or applications shared by users of the network on their client PCs.

Slack Space: Is the unused space at the logical end of an active file's data and the physical end of the cluster or clusters that are assigned to an active file.

Software: Coded instructions (programs) that make a computer do useful work.

Spreadsheet Program: Is a program that manipulates numbers and data in a table arranged in columns and rows. Lotus 123™ and Quattro™ are two spreadsheet application programs.

Stand Alone Computer: A personal computer that is not connected to any other computer or network, except possibly through a modem.

Storage: Refers to storing binary information created by the computer. The storage media stores data that is measured in bytes.

Streaming Video: Allows one to see video as it's downloading to your computer.

Subdirectory: Is a directory within another directory.

System Administrator: (sysadmin, sysop) The person in charge of keeping a network working.

Tape Backup Unit (TBU): Is a device to back up the large amounts of data on your hard drive. It is similar in appearance to an audiotape.

Terabyte: Is about one trillion bytes or more precisely 1,099,511,627,776 bytes.

Text Search: Is a technique for searching text files for occurrences of certain words or phrases.

TIFF (Tagged Image File Format): One of the most widely supported file formats for storing bit-mapped images. Files in TIFF format often end with a .tiff extension.

Transmission Control Protocol/Internet Protocol (TCP/IP): A collection of protocols that define the basic workings of the features of the Internet.

USB (Universal Serial Bus): Is a standard that supports data transfer rates of 12 Mbps.

Virus: Is a computer program that infects other programs by replicating itself. It can damage or destroy data.

Voice Recognition Technology: Refers to the capability of computer to "hear" a word and convert the word automatically to usable computer text.

VPN (Virtual Private Network): A virtually private network that is constructed by using public wires to connect nodes.

Windows: Is the Microsoft operating system that features multitasking and a graphical user Interface.

Word Processing: Is software designed to create letters, briefs or other documents.

World Wide Web: The WWW is made up of all of the computers on the Internet which use HTML-capable software (Netscape, Explorer, etc.) to exchange data. Data exchange on the WWW is characterized by easy-to-use graphical interfaces, hypertext links, images, and sound. Today the WWW has become synonymous with the Internet, although technically it is really just one component.

WYSIWYG (What You See Is What You Get): Refers to a word processor or graphics program that displays images on the screen exactly how they will appear on paper.

ZIP: An open standard for compression and decompression used widely for PC download archives. ZIP is used on Windows-based programs such as WinZip and Drag and Zip. The file extension given to Zip files is .zip.

## II. APPLICATION OF THE FEDERAL RULES AND ELECTRONIC DISCOVERY AMENDMENTS TO FEDERAL AND STATE RULES

Due to the lack of clear federal e-discovery standards regarding electronic data, it was increasingly difficult for litigators to recognize the potential practice hazards and for courts to make consistent rulings on electronic discovery issues.[52] In order to help both lawyers and courts address e-discovery issues and sidestep potential ethical landmines, the Civil Rules Advisory Committee suggested changes to Federal Rules 16, 26, 33, 34, 37, and 45.[53] The proposed amendments to the Federal Rules of Civil Procedure that address the discovery of electronically stored information were approved without comment by the United States Supreme Court on April 12, 2006. The new rules and amendments have been transmitted to Congress and will take effect on December 1, 2006, unless Congress enacts legislation to reject, modify, or defer the amendments.[54]

The Federal Standing Committee on Rules of Practice and Procedure has also approved a proposed amendment to Federal Rule of Evidence 502.[55] Proposed Rule 502 is aimed at addressing the issue of disclosure of attorney-client and work product materials that routinely occurs during litigation involving large volumes of electronic information. "The purpose of the rule is also to resolve the concern that any disclosure of protected information will operate as a subject matter waiver."[56] Proposed Rule 502 was published for public comment in August 2006.

Below are brief summaries of the amended Rules of Civil Procedure and proposed Rule of Evidence 502, as well as summaries of various U.S. District Court and State Court rules relating to electronic discovery that have recently been adopted.

### A. Discoverability of Electronic Evidence

Even before the recent revision to the Federal Rules of Civil Procedure, courts consistently ruled that electronic evidence was discoverable to the same extent as regular hard-copy discovery:

- Diepenhorst v. City of Battle Creek, No. 1:05-CV-734, 2006 U.S. Dist. LEXIS 48551, at *5 (W.D. Mich. June 30, 2006). The court stated that "the provisions of Rule 34(a) concerning inspection, copying, and testing of tangible objects are sufficient to authorize a court to order reproduction of an entire hard drive using the 'mirror image' method."

- Zhou v. Pittsburg State Univ., No. 01-2493-KHV, 2003 U.S. Dist. LEXIS 6398, at *4-5 (D. Kan. Feb. 5, 2003). Federal Rule of Civil Procedure 34 applies to electronic data compilations to the same extent as other tangible evidence, provided that the electronically stored information meets all relevancy requirements.

- Rowe Entm't, Inc. v. The William Morris Agency, No. 98 Civ. 8272, 2002 WL 975713, 2002 U.S. Dist. LEXIS 8308 (S.D.N.Y. May 9, 2002). The court stated that "Rules 26(b) and 34 for the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials."

- White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001). The court refused to suppress an e-mail from a family hard drive during divorce proceedings because "rummaging through files in a computer hard drive [is] not any different than rummaging through files in an unlocked file cabinet."

- Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999). The court allowed discovery of the defendant's hard drive because it likely contained relevant information.

- Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, 1999 Mass. Super. LEXIS 240 (Mass. Super. June 16, 1999). The court stated that "[a] discovery request aimed at the production of records retained in some electronic form is no different in principle, from a request for documents contained in any office file cabinet."

- Bills v. Kennecott Corp., 108 F.R.D. 459, 463-64 (D. Utah 1985). The court stated that "information stored in computers should be as freely discoverable as information not stored in computers, so parties requesting discovery should not be prejudiced thereby."

Therefore, all e-mails, calendar entries or electronic documents may be discoverable if "relevant to the claim or defense of any party." Fed. R. Civ. P. 26(b)(1). "Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." Id.

Courts, however, will limit a requesting party's access to storage media, other hardware or large volumes of electronic discovery if the issues in the case do not warrant such intrusive measures or the request fails to provide for protecting the producing party's privileged information:

- Bethea v. Comcast, 218 F.R.D. 328 (D.D.C. 2003). Plaintiff sought to inspect the defendant's computer system to determine if additional documents existed but defendant argued that it had previously produced all relevant unprivileged documents and that plaintiff failed to articulate any suspicion that it had withheld additional documents. The court agreed with the defendant and stated that more than mere suspicion is required for inspection of computer systems.

- In re Ford Motor Company, 345 F.3d 1315 (11th Cir. 2003). The appeals court overturned the district court order permitting plaintiff unfettered access to Ford's databases detailing, among other things, all customer contacts with Ford because the order permitted plaintiff access to information without permitting Ford to object prior to its disclosure.

- Dikeman v. Stearns, 560 S.E.2d 115 (Ga. Ct. App. 2002). The court refused to order access to plaintiff's computer system because the request was overbroad, oppressive and annoying.

### B. Form In Which The Electronic Discovery Must Be Produced

Fed. R. Civ. P. 34 requires a party to produce documents "as they are kept in the usual course of business." Therefore, the responding party typically must produce the discovery "in the format in which that party routinely uses or stores them, provided that electronic records shall be produced along with available technical information necessary for access or use."[57] Illustrative cases include:

- Nova Measuring Instruments Ltd. v. Nanometrics, Inc., No. C 05-0986 MMC (N.D. Cal. Mar. 3, 2006) Manufacturer ordered to product documents in their native file format with original metadata.

- Williams v. Spring/United Mgmt. Co., 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005) Court held that party should not have scrubbed documents prior to producing, stating "the producing party should product the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."

- In re Verisign Sec. Litig., NO. C 02-02270 JW, 2004 WL 2445243, 2004 U.S. Dist. LEXIS 22467 (N.D. Cal. Mar. 10, 2004). The trial court overruled the defendant's objections to the magistrate order requiring documents to be produced electronically in the native format.

- United States v. First Data, 287 F. Supp. 2d 69 (D.D.C. 2003). The court ordered the parties to produced "electronic documents[] in the native electronic format (or a mutually agreeable format)."

Courts may loosen the above requirement when opposing parties request access to proprietary or other confidential data:

- In re Ford Motor Co., 345 F.3d 1315 (11th Cir. 2003). The appeals court overturned the district court order permitting plaintiff unfettered access to Ford's databases detailing, among other things, all customer contacts with Ford because the order permitted plaintiff access to information without permitting Ford to object prior to its disclosure.

- Van Westrienen v. Americontinental Collection Corp., 189 F.R.D. 440 (D. Or. 1999). The court refused to grant plaintiffs unlimited access to defendant's computer system.

- Symantec Corp. v. McAfee Assoc., Inc., No. C-97-20367-JF, 1998 WL 740807, 1998 U.S. Dist. LEXIS 22591 (N.D. Cal. Aug. 14, 1998). The court refused to order the defendant to provide its entire source code to plaintiffs and the corresponding hard drives due to the volume and proprietary nature of the information.

Even when a party produces a hard copy version of electronic evidence, the party may also be required to produce the documentation in its electronic format as well. Courts beginning with National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980), have determined that Fed. R. Civ. P. 34 requires the production of the electronic format even if the requesting party already has the hard copy format. Other cases include:

- In re Honeywell Int'l Inc. Secs. Litig., No. M8-85, 2003 WL 22722961, 2003 U.S. Dist. LEXIS 20602, at *5-6 (S.D.N.Y. Nov. 18, 2003). The court required a non-party to produce documents in electronic format due to the hard copies being "essentially incomprehensible" and "insufficient because they were not produced as kept in the usual course of business."

- Storch v. IPCO Safety Prods. Co., No. 96-7592, 1997 WL 401589, 1997 U.S. Dist. LEXIS 10118, at *6 (E.D. Pa. July 16, 1997). The court found "that in this age of high-technology where much of our information is transmitted by computer and computer disks, it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff."

- Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, 1995 U.S. Dist. LEXIS 16355, at *1 (S.D.N.Y. Nov. 3, 1995). The court stated that "[t]he law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced . . . . [T]oday it is black letter law that computerized data is discoverable if relevant."

- In contrast, however, the court in Northern Crossarm Co. v. Chem.. Specialties, Inc., No. 03-C-415-C, 2004 WL 635606, 2004 U.S. Dist. LEXIS 5381 (W.D. Wis. Mar, 3, 2004), refused to order the producing party to re-produce documents in an electronic format when the requesting party did not specifically request an electronic format in its discovery requests.

### C. Amendments to the Federal Rules of Civil Procedure

#### 1. Fed. R. Civ. P. Rule 16: Pretrial Conferences, Schedule Management

Rule 16 now includes provisions for the disclosure or discovery of electronically stored information, as well as provisions that permit parties to enter into agreements protecting against waiver of privilege when electronically stored information is produced. The amendment to Rule 16(b) "is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur."[58]

### 2. Fed. R. Civ. P. Rule 26

#### a. Rule 26(a)(1)(B) Duty of Disclosure

Under this rule, parties are required to provide opposing parties with a copy of, or description by category and location of, electronically stored information. Rule 26(a)(1)(B) is intended to "parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses."[59]

#### b. Rule 26(b)(2)(B): Discovery Scope and Limits

Under amended Rule 26(b)(2)(B), a party is authorized to respond to a discovery request by identifying sources of electronically stored information that are not "reasonable accessible because of undue burden or cost." If the requesting party seeks discovery from such sources, the responding party bears the burden of showing that the sources are not reasonably accessible. Regardless, a court may order discovery of the information if the requesting party shows good cause and specify conditions for the discovery.[60]

#### c. Rule 26(b)(5)(B): Claims of Privilege or Protection of Trial Preparation Materials

If a party has produced information in discovery that it asserts as privileged or protected as work-product, Rule 26(b)(5)(B) allows that party to notify the receiving party of the claim by stating a basis for it. After notification, the receiving party must return, sequester, or destroy the information. Furthermore, the receiving party may not use or disclose the information until the claim is resolved. The receiving party does have the option of directly presenting the information to the court in order to determine (1) whether the information is privileged or protected, and if so (2) whether the disclosing party has waived these protections. During this period, the producing party must preserve the information pending the court's ruling.[61]

### d. Rule 26(f)(3) & (4): Conference of Parties

In accordance with amended Rule 26(f), parties are required to discuss during their discovery planning conference issues relating to preservation of discoverable information and issues relating to discovery of electronically stored information. This discussion should include the form in which electronically stored information would be produced, as well as issues relating to claims of privilege and work-product. It is also important to discuss their information systems so that the parties can develop an appropriate discovery.[62]

### 3. Fed. R. Civ. P. Rule 33: Answers to Interrogatories from Electronically Stored Documents

Amended Rule 33 "clarifies how the option to produce business records to respond to an interrogatory operates in the information age."[63] The amended rule adds electronically stored information as a category subject to production. Accordingly, a party may answer an interrogatory by specifying electronically stored information and allowing its inspection. The Committee Notes explain that the "responding party may be required to provide some combination of technical support, information on application software, or other assistance" to allow a party to derive an answer from the electronically stored information.[64]

### 4. Fed. R. Civ. P. Rule 34: Production of Electronically Stored Documents

"The form of producing electronically stored information is increasingly a source of dispute in discovery."[65] Amended Rule 34 provides (1) a structure and procedure for the parties to identify the production form most appropriate for litigation; (2) guidance to the responding party if no request, order, or agreement specifies the form of production; and (3) guidance to the court if a dispute does arise. The amended version also allows, but does not require, a requesting party to specify a form for producing electronically stored information. If the requesting party does not specify the form of production and there is no agreement requiring a particular form, then default forms of production are specified.[66]

### 5. Fed. R. Civ. P. Rule 37(f): Failure to Disclose and Good Faith Operation

Rule 37(f) responds to a distinctive feature of electronic information system: the routine modification, overwriting, and deletion of information that accompanies normal use.[67] Under amended Rule 37, a court cannot impose sanctions on a party for failing to provide electronically stored information lost as a result of routine and good faith operation of the electronic information system. Nevertheless, a court can impose sanctions in exceptional circumstances.

### 6. Fed. R. Civ. P. Rule 45: Subpoenas

Amended Rule 45 addresses issues of subpoenas and electronically stored information. Specifically, the rule recognizes that electronically stored information can be sought by a subpoena, which would permit inspection, copying, testing, or sampling. If a subpoena does not specify the form of the electronically stored information, the responding party is required to produce the information in its ordinary form or another reasonable form. If a party opposes production, the burden is on that party to prove that the electronically stored information is not reasonably accessible due to undue burden or undue cost. The court may nevertheless order discovery and outline conditions for discovery if the requesting party shows good cause.

"Similarly to Rule 26(b)(5)(B), if information is produced in response to a subpoena that is subject to a claim of privilege or protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified a party would be required to promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose this information until the claim is resolved."[68]

### 7. Fed. R. Evid. 502: Attorney-Client Privilege and Work Product Waiver

According to its Committee Notes, proposed Rule 502 has two major purposes. First, Rule 502 seeks to resolve disputes involving inadvertent disclosure and waiver among the courts by rejecting the view that inadvertent disclosure automatically constitutes waiver. Second, it seeks to address widespread concern about excessive litigation costs relating to the review and protection of materials that are privileged or work-product.

Under the proposed Rule 502, the inadvertent disclosure of the privileged or work-product materials does not operate as a waiver in state or federal proceedings if (1) disclosure was inadvertent and made in connection with federal litigation or administrative proceedings; and (2) the disclosing party took reasonable precautions to prevent disclosure and reasonable measures to rectify the error in accordance with procedures in Fed. R. Civ. P. 26(b)(5)(B).[69] Notwithstanding, the effect of disclosure to a state or local government agency is governed by applicable state law. The rule does provide for "selective waiver," meaning that disclosure of information to government agencies during an investigation does not constitute a general waiver of attorney-client privilege or work-product protection.

The proposed rule is intended to regulate disclosure at both the state and federal level, but does alter federal or state law on whether a communication is protected as privileged or work-product.[70] Also, the rulemaking process cannot bind the states directly, therefore the Committee has encouraged Congress to enact it via the Commerce Clause.

## D. Local U.S. Dist. Court Rules

### 1. Southern District of Ohio Local Rule 26.1(a)

Under local Rule 26.1(a), "[p]arties are encouraged to serve discovery requests upon the responding person or party by e-mail attachment or by providing a disc, in order to eliminate unnecessary retyping of questions or requests."[71]

### 1. Other District Court Local Rules

#### a. Eastern and Western Districts of Arkansas Local Rule 26.1

This rule requires parties to file a Rule 26(f) report with the court that includes information related to electronic discovery. If the parties anticipate discovery beyond data available in the ordinary course of business, then they must mutually agree on the time, scope, and cost of discovery, as well as the format, media, and procedures for production.[72]

#### b. Middle District of Florida Local Rule 3.03(f)

Under this rule, attorneys are required to use technology to the maximum extent possible throughout litigation. For example, a part should serve interrogatories on computer disk.[73]

#### c. District of Kansas

The U.S. District Court for the District of Kansas issued e-discovery guidelines for counsel in connection with Fed. R. Civ. P. 26(f) scheduling conference. The guidelines require that "[d]isclosures pursuant to Fed. R. Civ. P. 26(a)(1) must include electronic information." The guidelines also recommend that counsel become knowledgeable about their clients' electronic information systems. Further, parties who seek production of computer-based information must promptly notify opposing counsel. Lastly, the Kansas guidelines set forth issues which counsel should seek to agree upon at the Rule 26(f) conference (e.g., preservation of information, e-mail discovery, handling of deleted and archival information, allocation of costs, format and media for production, and handling of inadvertently disclosed privileged material).[74]

### d. District of New Jersey Local Rule 26.1(d)

Under the New Jersey rule, counsel has a duty to investigate a client's information storage systems prior to a Rule 26(f) conference. "Counsel must also identify a person or persons with knowledge about the client's information management systems with the ability to facilitate reasonably anticipated discovery."[75]

During the Rule 26(f) conference, counsel must stipulate to e-discovery issues (e.g., preservation and production of digital information; procedures for dealing with inadvertent disclosure; restoration of deleted information; whether legacy data is within the scope of discovery; the media, format, and procedures for producing electronic information; and the cost of preservation, production, and restoration of electronic discovery).[76]

### e. District of Wyoming Local Civil Rule 26.1(d)

The District of Wyoming's local rule requires counsel to carefully investigate their clients' information systems in preparation for Rule 26(f)'s conference. Specifically, attorneys must be knowledgeable about electronically stored information, how it can be retrieved, and the contents of client files. The rule also sets forth specific issues to be addressed at the Rule 26(f) conference, including "steps parties will take to preserve computer-based evidence, scope of e-mail discovery and agreed e-mail search protocols, whether restoration of deleted or backup data is expected, and the cost of any such restoration."[77]

#### f. Ninth Circuit District Courts

The Ninth Circuit has proposed local rules to govern discovery of electronic data and documents for U.S. District Courts within the Circuit. The proposed rules include:

- Rule 1, which imposes on parties duties to investigate, notify, and meet and confer in order to reach agreements on the scope of electronic data to be produced;
- Rule 2, which limits a party's "obligation to search for electronic data and documents";
- Rule 3, which requires production of electronic data in electronic form with unless the parties agree or court orders otherwise;
- Rule 4, which allows a responding party to conduct an electronic search of its documents; and
- Rule 5, which requires the responding party to bear the costs of production and the requesting party to bear the costs of obtaining data from "non-active" sources.[78]

### E. Ohio State Court Rules: Ohio Rules of Civil Procedure: Rules 33(A) and 36(A)

Rule 33(A) outlines procedures for serving interrogatories on another party. Specifically, Rule 33(A) requires the requesting party to provide both a printed and electronic copy of the interrogatories. The electronic copy must be on computer disk, by electronic mail, or by other means agreed upon by the parties.[79] According to Rule 33's Staff Notes, "[a] party who is unable to provide an electronic copy of interrogatories may seek leave of court to be relieved of the requirement."[80]

Corresponding amendments were made to Ohio R. Civ. P. 36(A) with regard to requests for admission.[81] Under Rule 36(A), requires the party submitting requests for admission to provide the responding party with both a printed and an electronic copy of the requests. "The electronic version must be provided in a format that will enable the responding party to readily include the requests for admissions and corresponding answers and objections in the same document without having to retype each request for admission."[82]

## F. Other States Electronic Discovery Rules

### 1. California Code of Civil Procedure § 2017

The California Code permits discovery to be conducted in an electronic media and by electronic communication. The Code also authorizes California courts to issue orders relating to the use of technology in discovery. For example, a court may issue an order requiring the parties to stipulate to certain criteria and procedures.[83]

### 2. Supreme Court of Mississippi Rule 26

Mississippi Supreme Court Rule 26 was amended to allow for e-discovery. Rule 26(b)(5) now states:

> "Electronic Data. 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 may also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information."[84]

## III. WHERE CAN YOU FIND COMPUTER-RELATED EVIDENCE? (THE COLLECTION PROCESS)

Lawyers need to have a working understanding of computers and their systems to adequately respond to and formulate electronic discovery requests. The first question must be ─ where can I find the evidence? Computer systems of your clients and adversaries are often complex and complicated. Electronic discovery requires the use of a well-thought-out and properly planned process for collecting the electronic documents and data.

The basic of the collection process for collecting electronic evidence has three separate, but equally important phases: (1) preservation and collection; (2) processing; and (3) review. The preservation phases consist of the processes for identifying and collecting the relevant electronic data from all appropriate sources. The second phase, processing of the electronic data, can include ─ depending on the amount of data and need ─ a separation of the different types of documents and data from all other electronic data on the computer system, sorting the documents and data using well thought-out strategies (e.g., by date range, author, topic, etc.), removing duplicates from the data, keyword searching the data, identifying files that may need special care to review (including files that are encrypted or password protected), converting files to a reviewable format, and transferring the documents and data to an electronic discovery review tool. During final phase ─ review ─ attorney must analyze the electronic documents and data for relevance, privilege, and redaction purposes.

The following chapter discusses the strategies for the location and collection of electronic evidence and tactical decisions that lawyers can use for developing a thorough and carefully planned collection plan to determine where you can find computer-related evidence.

### A. Understanding the Computer System

An understanding of the computer systems in question starts with knowing how the systems are arranged and used by the individual users and the company as a whole. Computer systems may consist of large computer servers that are used by many users or personal computers that work individually or that are linked through a network, or both. Lawyers should have (or acquire through initial discovery) a basic knowledge of the computer systems that are used by both the individuals and the company. For example, as a starting place, lawyers need to gather, among other things, information about:

- The servers that are used by the company;
- Date storage devices employed to store data;
- Desktop computers that are in use by individual users (including number and location);
- Other hardware devices that make up the computer network;
- Operating system(s) that run the computers;
- Applications software that are used on the hardware, such as commonly used word processing and spreadsheet programs; and
- Back-up procedures used to back-up the information and the media that is used to store the back-ups.

The best source for the above information is often the MIS (management information system) or IT (information technology) departments of the company. In these departments, frequently it is the technicians that have the day-to-day responsibility for designing and administering the computer system. Thus, it is these technicians that have the knowledge required to provide answers to the above questions. If there is no MIS or IT department, then lawyers may have to rely on the computer system consultants or vendors to gain an understanding of the computer systems. Either way, gaining an understanding about the above issues early on and throughout the process of collecting and locating the electronic evidence is the best way to prevent any serious problems later.

## B. Mining Networks and Servers (Home, File, E-Mail and Internet)

At its most basic level, the hardware and software that connect computers to each other and allow them to share data is called the "network." Common computer networks are called "local-area networks" (or LANs) when the computers on the network are located in close proximity and "wide-area networks" (or WANs) when the computers are farther apart and are connected through the use of telephone lines, cable lines or wirelessly through the use of radio waves.

It is through the use of the network that most users get access to certain services like files, e-mail, internet, and databases. Access to the services through the network can be provided in two ways. First, the network could be established so that each workstation within the network acts as a file server ("peer-to-peer model"). If the peer-to-peer model is employed (which is less common today), then lawyers should expect to find electronic evidence on any of the workstations on the network. Second, (more commonly used today) the network can be established to provide each user access through designated servers (referred to as the "client-server network" model). A client-server network normally has one or more servers to which the users can save documents. The servers are the centrally-located repositories for all of the data. The data on the servers may be stored on one or more hard drives.

### 1. Home Directories

Typically, the space on the network hard drives where the user stores information is called a "home directory." Often (but not always), the home directory is private and other users of the network cannot access documents in other user's home directories. Many client-server networks are setup so that, by default, a user's documents are automatically saved to the user's home directory on the network. In other networks, however, the user may have the option of saving documents "locally" to the hard drive on the user's desktop or laptop computer.

Home directories are often one of the best places to find electronic evidence because users often use home directories for more than just storing documents. For example, many times users will store archives of their old e-mail on the home directories (often called ".pst" files). Given the sizes of e-mails (and their attachments) that are generated by users today, companies often limit the amount of data or number of e-mails that a user can store on the e-mail server. In addition, companies often have policies whereby they save only one year of e-mail back-up tapes. If the users save their old e-mail through the use of archive .pst files and save that data in their home directories, then counsel can get access to older e-mail messages that would have been lost otherwise.

When removing data from the home directory (or any other hard drive), the person collecting the data must collect the data in such a way as to not change the last-accessed data (or other metadata) contained in the documents. If done improperly, then the last-accessed data (or other metadata) may be modified ─ raising spoliation issues. Metadata (discussed in more detail below) must be preserved along with the files. Common system tools with Microsoft Windows® can change the last-accessed dates and modify the metadata. It is important that the person collecting the information make efforts ─ where possible ─ to preserve the metadata in an undisrupted form.

### 2. File Servers, Shared Drives, or Group Shares

Most computer networks also have space on the file servers to which multiple users may save, view or edit documents. This space is often called the "file server," "shared drives" or "group shares."

One of the challenges of collecting electronic evidence from file servers is filtering the data from a single or small number of relevant users from the other data available on the file server. The user may have access to dozens of file servers, but not all of the file servers on the network. This is often the case in large companies or corporations. Even if a single file server is used by all of the custodians on the network, file servers frequently have hundreds of gigabytes (or more) of documents and are organized by topic (rather than user or custodian). Moreover, to collect all of the user's data, the file servers to which the user had or has access must be located and identified. It is often challenging to reconstruct where a user may have stored relevant data (especially when the user is not available).

Depending on the case, the collection of information from all of the file servers and the sifting of the data can be cost prohibitive. There is, however, an alternative methodology for gathering the information. Technicians experienced in the collection of electronic evidence can create a "Perl script" (which is a custom computer searching program or network-forensic tool) to search the metadata to cull out documents from the relevant users.

### 3. E-Mail Servers

The e-mail server is part of the network that provides and stores incoming mail for distribution to users and forwards outgoing mail through the appropriate channel. Most users use one of two common applications to access e-mail, either Microsoft Outlook® or Lotus Notes®. Both applications have similar functions. However, there are differences in how the electronic evidence must be collected from each application.

With the Outlook® application, the e-mail is supported by an Exchange™ server. Exchange™ mailboxes for the relevant user (or users) must be exported from the Exchange™ server into a separate file (".pst" file) for each user. The ExMerge™ utility program can be used to export the information into a separate file. When using the "Exmerge" utility, however, it is important that all of the data are collected that pertains to the custodian. For example, e-mail messages that may have been deleted from the user's inbox that still reside on the Exchange™ server must be collected.

LotusNotes® supports e-mail by using a Domino® server (formerly known as the Notes® server). If LotusNotes® is used as the e-mail application by the user, then the collection of the data is simpler as each user's e-mail box is segregated on the server in a separate file (".nst" file). The files can be easily copied. However, care must be taken to ensure that the data is not missed during the copying process. In addition, LotusNotes®'s users have the ability to encrypt or password protect the .nst files. Thus, when the data is collected, efforts must be made to obtain the encryption key and the user's password.

While the collection of information from the e-mail server is often easier than collecting data from other servers as most collection processes pose little risk that the collection will change the content of the e-mail or metadata, using a written and detailed plan to collect the data is the best way to ensure the completeness of the collection and the make certain that needed data will not be mistakenly left behind or lost later.

### 4. Internet-Based File Servers or Internet Storage Providers

Some companies, depending on the industry's or company's business model, may use internet-based file servers or internet storage providers to store company documents. An internet storage provider is an organization that is a third party that provides free and/or paid access to storage on the internet. For example, companies such as Xdrive and I-drive allow users to back-up, store and share files using their storage facilities. When collecting electronic evidence, it is important not to forget such servers or storage providers as that data, like other electronic data, is subject to discovery just like the documents and data stored on the company's servers located at the company's facilities.

## C. Individual Computers and Laptops (the Desktop Environment)

The collection of electronic evidence almost always involves the collection of documents and data from the individual user's desktop and laptop computers. While such a collection adds cost and complexity to the collection efforts, it is necessary, as the user's personal computer (whether at home or at work) holds documents and data on the "local" computer that may not be (or never have been) located on the home, file, e-mail, or internet servers. For example, older or archive e-mail is often stored on the local computers, and e-mail servers are frequently configured to delete messages as soon as the e-mails are archived as a .pst file on the local computer. In addition, many users (especially mobile users with laptops) create and sort the bulk of their documents and data locally and never save them to a network server.

Collecting documents and data from desktop and laptop computers takes a certain amount of care to ensure that critical data is not missed. For example, on Microsoft Windows® based computers, most documents and data relevant for collection (word processing, spreadsheets, and databases) are stored in the "My Documents" folder. The "My Documents" folder, however, should be merely the starting point and not the sole collection point when gathering electronic evidence from local computers. If other folders are missed, then important data that is misfiled (intentionally or otherwise) may be missed. For example, there are often critical documents and data on the local computer in the Recycle Bin, or stored in one of the program files. The development of a thorough collection plan will ensure that these documents and data are not missed.

A common (and effective) way to collect data on a local computer is to forensically image (or mirror) the entire hard drive. There are several acceptable tools available to perform such a task. By creating a forensic image (assuming that it is done correctly), the information is preserved on the hard drive as it is kept at the time that the image is done. If such an image is performed and the scope of the collection is expanded at a later date (such as searching for deleted items), then future collection efforts and analyses can be done. If an image of the hard drive is not performed and the scope of the collection expands, then documents and data that are not preserved may be lost.

While imaging the computer is the best method to preserve the data for later use, often such a method of collection is not available or is overly costly (as many system files that contain no useful information are also copied). If imaging cannot be done, then consideration must be given to the creation (and negotiation if necessary) of a list of data and document file types to be harvested from the local computer. Whether the local computer's hard drive is imaged or not, at some point, the documents and data on the hard drive must be harvested from the computer. The most efficient and effective method for harvesting the data from the computer is to develop a list of the common applications that are used by the business that may contain relevant electronic evidence. Common applications include word processing documents (Word® ".doc" files or WordPerfect® ".wpd" files), spreadsheets (Excel® ".xls" files), e-mails (Outlook® ".pst" or ".ost"), presentations (PowerPoint® ".ppt" files), or images (Adobe Acrobat® ".pdf" files). There are several others and depending on the nature of the litigation and the company, other applications and file types should be added to the list.

When harvesting the electronic evidence, care must be taken so that relevant files are not missed. Data may be "hidden" in unexpected files on the computer's hard drive. One method that can be performed to ensure that no files are missed is to use the search function on the computer to search for all files of a certain type. By searching the entire hard drive, collection of the data will be performed no matter which folder it is stored on the drive.

Finally, as employees work longer and longer hours and work continues to creep into the home life of many professionals, counsel may need to gather electronic documents and data from the personal computers and laptops used at home. Often, if users use their home computers for work purposes, then documents or data may be stored on the computers, sometimes exclusively. Thus, when seeking electronic evidence (or responding to a demand for electronic data), do not forget that work-related documents and data may be harvested from the personal computers and laptops located in the homes of certain users.

### D. Locating Evidence on Removable Media, External Devices, and Back-up Tapes

When gathering electronic evidence, counsel should also be mindful that many times users within the network will save documents and data to removable media and external devices such as CDs, DVDs, USB thumb drives, jaz drives, PDAs, and external hard drives. Similarly, back-up data should be explored when searching for electronic evidence.

The cardinal rule for both users and system administrators in large and small companies alike is to back up computer files regularly. Especially in organizations that depend heavily on computers (which includes most companies today), adherence to this rule has often become, at least in principle, customary. The result of the proliferation of back-ups has only increased complexity, uncertainty, and cost of gathering and responding to requests for electronic discovery. With the explosion of the use of back-ups there has been a drastic increase in the sources and amounts of files and e-mails that are now saved and available (through some work) for review.

In most cases, back-up data is copied by the IT department from a network drive (like the file or e-mail server) to a form of removable or external media. The purpose of such back-ups is to provide data redundancy in the event of some sort of a system failure. In addition to the back-ups that are done on the network level, users often perform their own back-ups from their hard drives to external removable media. Unlike network back-ups, which are usually generated on a regular schedule, user level back-ups may be more ad hoc and performed on an irregular basis.

Each company and server environment (e-mail, group, or file) may have different back-up policies. To gather background information about the policy, the system administrator should be a first stop in gathering electronic documents and data. While the chief technology officer may have access to the information, the system administrator is likely to have more detailed and specific information regarding how the policy is applied.

One of the first questions that must be answered by the system administrator is how often are the documents and data on the system backed up? On smaller servers, the electronic data may be backed-up in full each day for several weeks, and each back-up may be made on a separate tape. At the end of several weeks, the tapes are commonly reused and the information on the back-up tapes is overwritten. Such a system is often referred to as a back-up rotation. In contrast, in larger server environments, there may be simply too much data for the system to be backed up in full everyday. In such an environment, system administrators usually perform a full back-up of the system on a periodic basis (often on a weekend) and then perform incremental back-ups for the next six days (until the full back-up is performed). During an incremental backup, only those files that have changed are backed-up. Thus, if restoring the system from the back-up is necessary, then the administrator must use the last full back-up and all subsequent incremental back-ups to fully restore the system.

In addition to rotational back-ups, companies often retain full end-of-month, end-of-quarter, and/or end-of-year back-up tapes for several years. Many businesses do so pursuant to a comprehensive disaster recovery plan, which is becoming more and more common. These back-up tapes are usually stored off-site and are often somewhat difficult to access. Notably, as electronic discovery has become common, many companies are revising their back-up policies to retain less and less back-up data and take on the risk of a system failure − all to avoid the cost and inconvenience of litigation-related restoration and analyses.

While back-ups often provide a wealth of information, lawyers relying on back-up tapes for gathering electronic evidence should be aware that back-up policies and practices are not perfect. A lawyer that is charged with collecting electronic documents and data from back-up tapes for purposes of responding to discovery requests should be mindful that back-up policies are not always followed. For instance, even when the company employs a rotational back-up policy, back-ups that should have been discarded or overwritten are often not and the information is available. In addition, lawyers relying on back-up tapes to gather electronic data should be aware that back-up tapes often fail and the information on the tape is useless. The lesson is, be aware, the practice and back-up policy may be different. Do not blindly rely upon the back-up policy when collecting or demanding electronic discovery.

There are several challenges for counsel relying on back-up tapes. Back-up tapes can be both over-inclusive and under-inclusive at the same time. The biggest challenge is often the volume of data that is available on the back-up tapes and the massive amount of duplication among the several tapes. The duplication on the back-up tape makes the tape over-inclusive. As a general rule, the closer in time that the back-up tape is created, the more duplication there will be. Stated another way, if the users store thousands of e-mails in their in-box and the back-up is performed each day, then a three-week rotation of full back-ups could produce close to a 90% duplication rate from one day to the next. Since restoring back-up tapes is often time-consuming and costly, the added cost of removing the duplication may make restoring all of the back-up tapes for the three-week period cost-prohibitive.

Similarly, over reliance on a back-up tape is a mistake as there is no assurance that every file is backed-up on the tape. The tape will have gaps and could be under-inclusive. Such a gap will occur if the document or data file is received, reviewed, and deleted before it can be captured by the scheduled back-up. This type of a gap is common with e-mail. As companies often restrict the amount of data that a person is allowed to store on the e-mail server, users often read and delete e-mail immediately. If the company backs-up e-mail at the end of the day, then the deleted e-mail (if completely deleted) would not have been backed up and would not be available on the tape. The lesson here is that back-up tapes can be under-inclusive, as well as duplicative, so do not rely exclusively on the back-up tapes for locating electronic evidence.

Gathering electronic evidence from back-up tapes is also affected by difficulties that occur because of the way that the electronic information is stored. Back-up tapes are often stored on magnetic tapes that contain an enormous amount of data that is arranged in a linear fashion. Unless the back-up is done on optical drives, back-up tapes are rarely searchable. In addition, data on back-up tapes (whether magnetic or optical) are frequently compressed so that as much data as possible can fit on the storage media. If the data on the back-up tape is compressed, then the data will need to be decompressed and restored before it can be accessed. While decompressing the data is not difficult, it can (and often is) a time-consuming process.

### E. Discovering Evidence Using System Logs (Databases)

Electronic documents and data can be gathered from a number of databases commonly used by companies. For instance, companies often have log files (contained in databases) that contain information about data coming into and out of the companies' computers (company firewall logs), telephone calls (phone system logs), and building access (security system logs). When kept electronically, these logs are usually maintained in databases. Collecting information from databases can be a treasure trove for a litigator. There are, however, several issues that occur during the collection of electronic data from databases.

For example, while databases can be copied and produced, the copies are often useless because the database is written on a proprietary and nonpublic platform and the database will not run on anything but the native platform. Often, log files that are available in proprietary platform databases are made available in hard copy form. Such a production, however, has limited usefulness. First, there is often an enormous amount of information. In large organizations, it is common for databases to be over a terabyte (or more) in size. Even if the database can be produced in hard copy form, the information is not searchable. Moreover, there often is a high degree of contextual knowledge required about the database structure to understand how the data is organized.

### F. PDAs (Palm® and Blackberry®)

PDAs (like Palm® and Blackberry® devices) often have a wealth of electronic documents and data and these devices should not be overlooked when collecting electronic evidence. While these devices are commonly synchronized with desktop computers or with the server wirelessly, a complete synchronization may not be done. For example, there may be e-mail or a version of the document stored on the device that may not exist on the network or desktop computer. For that reason, when collecting electronic evidence, PDAs are often an important source that must not be disregarded during the collection process.

## IV. WHAT EVIDENCE IS OBTAINED THROUGH COMPUTER FORENSICS?

Computer forensics is not electronic discovery. As electronic discovery becomes more and more common in litigation, lawyers often are unaware of the differences between computer forensics and electronic discovery.

### A. Electronic Discovery vs. Computer Forensics

Electronic discovery, in its simplest form, is described as the collection, preparation, review, and production of electronic documents and data. The collection of electronic data during electronic discovery usually involves gathering information from a large number of sources. While electronic discovery specialists may be employed to assist with the collection efforts and may be called to testify regarding chain of custody issues with the collection, the electronic discovery specialist is not usually considered an expert for litigation purposes.

In contrast, computer forensics involves the use of an expert to identify, preserve, extract, interpret, and present computer-related evidence. Unlike electronic discovery, computer forensics often employ specialized tools and forensic techniques to preserve, examine, and extract data that otherwise may be lost or overlooked. The computer forensic expert provides expert opinion testimony, in addition to factual testimony regarding chain of custody issues.

**Electronic Discovery vs. Computer Forensics**

| Factors | Electronic Discovery | Computer Forensics |
|---|---|---|
| Reviewers | Usually Legal Professionals | Retained Expert |
| Number of Reviewers | Often many | One |
| Type of data | Active Data | Active, Metadata, Embedded, and Residual Data |

| Factors | Electronic Discovery | Computer Forensics |
|---|---|---|
| Recovery of Files | No | Yes |
| Analysis of Web-based data (e-mail, etc). | No | Yes |
| Encrypted and password protected files | No | Yes |
| Testimony | Fact (chain of custody) | Opinion (expert) |
| Collection Process | Done by legal professionals or electronic discovery specialists | Forensically-trained technician |

B. Finding a Computer Forensic Expert

Finding a computer forensic expert is best done the same way that litigators find other experts − references from other lawyers and legal professionals. When looking for a computer forensic expert, however, there are a few important points to keep in mind. Computer forensic experts are not licensed and there is no standardized exam to establish the credibility or competency of the expert. There is an increasing number of organizations that offer certifications in computer forensics. Like other certifications in other fields, the certification is only as good as the certification body that provides the certificate, and an evaluation of the certification process and organization must be done. Questions like (1) was there a testing requirement?, (2) was a peer review or minimum experienced threshold required?, and (3) who taught or certified the expert? must be asked.

In addition, look for computer forensic experts that have past courtroom experiences and experiences similar to the case that is at hand. Often, in the computer forensic field, experts routinely handout only certain types of cases like computer pornography cases, and an expert with that type of experience and expertise may not be appropriate for cases involving financial transactions or intellectual property infringement. Similarly, make sure that the computer forensic expert is able to communicate effectively. Computer forensics is a difficult field to communicate to a jury as it is filled with hyper-technical theory and terminology. Make sure that the computer forensic expert possesses the ability to explain the evidence in a simple and understandable fashion.

Finally, keep in mind that computer forensics can be both time consuming and expensive. Complex analyses of a computer system can cost several thousand dollars or more. Make sure that there is a clear understanding of hourly rates and anticipated expenses. Be aware of the computer forensic expert that promises impractical goals in an unrealistic amount of time. That expert will probably need to cut corners and could easily miss something because he/she did not take the time to do the job correctly.

### C. Understanding Basic Types of Data

One of the key differences between computer forensics and electronic discovery is with the collection process. Common electronic discovery processes collect active data, which include the files on a computer that are readily available and can be accessed without using special computer forensic tools and techniques. Computer forensics, on the other hand, involve collecting and analyzing much more data and usually involves review and analysis of metadata, embedded data, and residual data, including files that have been deleted or hidden and file fragments that are located in disk slack or unallocated disk space. An understanding of different types of data is important to properly understand the differences between electronic discovery and computer forensics.

#### 1. Active Data

Active data is the information that is stored either on the network or locally on the hard drive of the computer. It is usually available and readily accessible to a user of the computer through the use of the desktop or other computer connection and takes no real specialized skill to collect. The data is available from the current files on the computer and is still visible in the directories and available to the applications on the computer.  Active data includes information such as word processing documents, calendars, memo pads, task lists, address books, e-mail, and databases.

Active data may be reviewed and analyzed without the native application using simple translation applications.  More often, however, each file will need to be viewed within each computer application.  For example, e-mails will need to be viewed with applications like Microsoft Outlook® or LotusNotes®, spreadsheets with Microsoft Excel®, databases with Microsoft Access®, and word processing documents with Microsoft Word® or WordPerfect®.

Active data may be protected through the use of a password or an encryption program.  In addition, active data includes system data (logs) and data residing within the Recycle Bin, history files, temporary internet files, internet directories, cookies, system registry files, and other more obscure files that are readily available on the computer.  Active data also usually includes hidden data called metadata or embedded data.

### a. Readily Available Data

Collecting active data stored on a server or hard drive of a local computer is usually not difficult or complicated.  While the collection of readily available data is not difficult, careful collection efforts, however, must be taken to make sure that all of the data is collected.  Often (intentionally or otherwise) users store documents and data in unpredictable folders.  Therefore, during the collection process, the entire hard drive must be searched to collect relevant documents and data.

In addition, other issues may occur that need special consideration.  For example, a hard drive will contain thousands of irrelevant system files and programs. Accordingly, the forensic examiner must develop a careful protocol for harvesting the information from the computer.  A common method is to sort the files on the hard drive by relevant file extensions (e.g., .doc, .xls, .ppt, .wpt, and .pdf) and then extract only those files with the relevant extension. Care must be taken to make sure that the list of file extensions includes all of the file extensions that are potentially relevant. This is especially true as new programs are developed every day with new file extensions. In addition, large organizations often have file extensions that are unique to the company's computer environment.

Files could also be stored in a way that requires special handling. For example, large files may be compressed with a compression program. These files (usually with the file extension .zip) need to be uncompressed either before or after harvesting.

Word processing files can also be tricky to harvest. Users have the ability to save simple word processing files as text files (.txt). A .txt file is, basically, a stripped-down word processing file that has little formatting. A computer system may contain literally thousands of .txt files. Thus, care must be taken to ensure that all relevant text files are harvested from the computer systems.

Similarly, harvesting e-mail files that have been archived to the user's hard drive can be complicated. This is especially true when the user uses internet e-mail, such as AOL, Yahoo! or Hotmail. Internet e-mail programs often create a separate archive for older e-mail. With programs such as AOL, the archive program will be in a separate file for each version of AOL that is installed on the computer. In addition, e-mail programs such as Microsoft Outlook® may contain hidden files that − unbeknown by the user ─ save e-mail on the user's computer. For example, Outlook may save a .ost file on the user's hard drive. Although the user cannot access the .ost file, the file can be converted to a .pst file. The .pst file can then be viewed, which may contain archived e-mail, calendar items, and tasks.

### b. Metadata

Metadata is data that describes other data. The metadata in a document may include, among other things, information about when the document was created, when modified, last accessed, last printed, and who created the document. Not only does metadata exist in document and spreadsheet files, but metadata also exists in Window-based file systems in file allocation tables ("FAT") and master file tables ("MFT"). The purpose of this metadata is to allow the computer to determine where the saved document or data is stored. FATs and MFTs also contain metadata that includes information about when the document was created, last modified, and last accessed.

The most common form of metadata is available in Word® and WordPerfect® documents and Excel and Access files. It is important to note that the metadata in these files may be different than the metadata contained in the FAT or MFT files. For example, if a Word® document is created and modified in a Windows-based system on January 1, 2006, and e-mailed to a user on a separate system (and network) on January 3, 2006 and then saved on that user's system, then the metadata in the second users FAT/MFT file will show that the document was created on January 3, 2006. The metadata in the Word® document, however, may show that the document was actually created on January 1, 2006.

In addition, the metadata available in the Word® document is more comprehensive. The Word® document metadata will contain additional information about the last time printed, last ten "authors," and last-saved-by. All of these additional data features do not rely on the FAT/MFT system files, and thus are not changed when the document is transferred from one system to another.

E-mail is another place where metadata is commonly found. In e-mail that is sent from outside the company's network, metadata is available regarding the name of the e-mail server from which the e-mail was sent, the name of the e-mail server receiving the e-mail, the internet protocol address of the server, and the time stamps for when the e-mail was passed through the server. Such metadata is invaluable to resolving disputes regarding when a particular e-mail was sent or received. It is important to note, however, that such metadata is preserved only when the e-mail is copied in its native format. If only the visible text of the e-mail is preserved (commonly through an imaging process), then this metadata will be lost.

### c. Embedded Data

Embedded data is information that is created by the user and hidden from view within the file itself (i.e., data that is not displayed through the default view of the document). The most common type of embedded data is a redlined edit of a Word® document. There are other types of embedded data in other types of files that are commonly available such as edits, formatting commands, links to other files, hidden rows or columns in spreadsheets, or electronic notes written by authors or reviewers.

To view embedded data (like metadata), it is important to have access to the data in its native form and not in an imaged form. As electronic discovery is commonly performed by imaging the electronic documents and data, counsel should be prepared to ask for and fight for documents to be produced in their original or "native" form.

### 2. Residual Data

Residual data (also called latent data or ambient data) are data such as deleted files or other memory files like swap files, temporary files, printer spool files, and shadow files, which can often be recovered by a computer forensic expert from the hard drive of a computer.

Most people now realize that deleting a document will not remove it from the hard drive and that deleted files can now be recovered. When a file is marked for deletion, the data is not removed; rather the data is marked by the computer and made available by the file system of the computer to store other data. The data resides on the hard drive in slack space and other areas that are marked by the computer as available to store new data. Although the deleted data is not easily retrievable by the user during normal operation, the data is not actually erased until it is overwritten with new data by the computer. As long as the data is not overwritten by the computer, then the data remains recoverable.

In addition to deleted items, there are other forms of residual data available on a computer's hard drive. For example, if a user opens (but does not save) an e-mail message, the computer's operating system often automatically saves the data in the computer's cache. Cache memory can be recovered forensically and can offer very useful evidence in litigation.

Through the use of forensic tools, deleted or residual data can be recovered. For this reason, most computer forensic technicians with image or mirror the hard drive of a desktop or laptop computer. While the odds that a deleted item will be overwritten increase with the volume, frequency, and use of the computers, desktop and laptop computer often have a large amount of available space and there is often a good chance that deleted data can be recovered. Such is not the case with servers, which is why servers are rarely (if ever) imaged by the computer forensic technician. Servers often run at near-capacity and slack space is consumed quickly with the high-level of use. In addition, servers often employ compression techniques to fit more data on the servers and those techniques make it more difficult, if not impossible, to recover residual data from servers.

As the use of computer forensics becomes more common and it becomes widely known that data cannot be simply deleted on a computer, users often use programs that promise to wipe the hard drive. These programs simply overwrite the unallocated free space or slack space on the hard drive with junk data. The programs, however, are not foolproof and data is often still recoverable from the computers.

### D. Internet History, Cookies, and Instant Message Logs

A user's internet activity, including internet history, cookie information, and logs of instant messaging activity can be invaluable in litigation. Such information often contains core information relevant to a case, including the who, what, where, when, and even why.  This information is frequently readily available on the hard drive of a desktop or laptop computer.

An internet history log tracks the websites that a user accesses over a certain period of time.  Often the links to the websites are available in the dropdown box in the internet browser for quick access.  In addition, recently viewed websites are stored on the computer in the cache (also known as a web cache or browser cache).  The cache is a temporary storage area on the hard drive of a computer that stores the more recently viewed internet websites.  As a user moves from webpage to webpage, the pages are stored in the cache of the computer so that the user can quickly go back to the page without downloading it again.  Even when the web browser is closed, all of the websites are still stored in the cache.  The websites are stored until deleted manually or automatically, according to the settings for the browser.

A cookie is a small file that is automatically created and stored on the hard drive of the computer when a website is visited.  The cookie is used by the computer to store the user's information for use when the user visits the website in the future.  Using cookies, website developers are able to personalize webpage content to the user.  In addition, cookies are used to store (correctly or not) the passwords and login information of the user.  Cookies can also record the address of the website that the user previously visited (immediately before visiting the website).

While internet log files, caches, and cookies can be manually deleted by the user, they are often available because people fail to delete the information.  As a result, such information is usually the first stop for many computer forensic technicians as the information can provide a treasure trove of evidence when the investigation involves a user's internet activity.

Similarly, instant messaging files (IM) are sometimes recoverable by a computer forensic technician.  Instant messaging has become one of the most popular mediums for high-tech communication.  Instant messaging is a cross between e-mail (as it is text) and telephone (as it is instant). Depending on the instant messaging software used, retrieval of the conversation may be performed by a skilled technician. Some instant messaging programs store the sessions in memory that is deleted when the computer is turned off. If such a program is used, then the recovery of such data is difficult and often impossible. Other instant messaging programs, however, store the contents of the IM session in the cache or swap file. Data that is stored in a cache or swap file can be accessed by a skilled technician.

### E. Admissibility of Electronic Documents and Data

Electronic evidence requires the same type of testimonial foundation to be admitted into evidence as regular or hard copy evidence. This section examines the basic evidence rules regarding admissibility of documents and the special issues that arise with electronic evidence.

Although the evidentiary rules require the original writing, recording or photograph be admitted to prove the contents, duplicates may be admitted "unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Fed. R. Evid. 1003; Ohio R. Evid. 1003.

For a document, recording or photograph to be admitted as evidence, a foundation of relevance and authenticity must be established. To be relevant, evidence must make a fact in question either more or less likely. Fed. R. Evid. 401; Ohio R. Evid. 401. Authenticity requires a showing that the evidence "is what a proponent claims." Fed. R. Evid. 901(a); Ohio R. Evid. 901(a). Authenticity may be established through witness testimony, distinctive characteristics of the evidence, and the like. Fed. R. Evid. 901(b); Ohio R. Evid. 901(b).

Furthermore, to be admissible, the contents of the documents may not contain hearsay, an out of court statement offered as evidence "to prove the truth of the matter asserted." Fed. R. Evid. 802; Ohio R. Evid. 802. The Rules do prescribe twentythree exceptions to the general rule, including present sense impressions, recorded recollections, records of regularly conducted activities, and public records. Fed. R. Evid. 803(1), (5), and (6); Ohio R. Evid. 803(1), (5), and (6).

### 1. Authenticity

Pursuant to Federal Rule of Evidence 901, electronic data must be properly authenticated just like other forms of evidence. Typically, a party must show the information to be reliable or trustworthy. Several courts have held that a witness' testimony of printing e-mails or internet pages was enough to satisfy the authenticity requirements:

- Kearly v. Mississippi, 843 So. 2d 66 (Miss. Ct. App. 2002). The court held that the witness' testimony of personally receiving and printing e-mails from the defendant was sufficient to prove authenticity.
- Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002). The court refused to deem all printouts from websites inadmissible and determined that a witness authenticated documents attached to a declaration when the "pages [were] printed from the Internet . . . by [him] or under his direction."

In contrast, an Ohio court stated that "although the legal requirements for admissibility of downloaded documents may not be well-established, a party's statement that 'I downloaded these pages from the internet' is probably not sufficient to authenticate a downloaded document." State ex rel. Leslie v. Ohio Hous. Fin. Agency, 2003-Ohio-6560 (Ohio Ct. App. Dec. 9, 2003) at ¶ 70 n.1. In Leslie, the Tenth Appellate District found that at a minimum authentication for documents copied or downloaded from the internet would require:

- Web address and path of the document;
- Date and title of the document;
- Date the document was downloaded or accessed; and

- Sworn statement to the court that the copy had not been altered from that found on the website.

Id.

Several courts have found that the testimony of an expert was sufficient to establish authenticity:

- Kupper v. State, 2004 WL 60768 (Tex. App. Jan. 14, 2004). Defendant appealed his sexual assault conviction on the grounds that the e-mail messages retrieved from the deleted files on his work computer and an e-mail and photograph retrieved from the temporary internet files on his computer were inadmissible. During the trial, a police detective who was trained in computer forensics testified that she had imaged defendant's home and work computers and engaged in a computer forensic investigation in order to locate the evidence at issue. The appellate court concluded that the police detective's testimony established the appearance, contents, substance, internal patterns or other distinctive characteristics, considered in conjunction with the circumstances, authenticated the computer evidence.

- Broderick v. State, 35 S.W.3d 67 (Tex. App. 2000). The court affirmed the trial court's admission of a duplicate of defendant's hard drive in lieu of the original. The court found that the state's best evidence rule did not preclude admission because a computer expert testified that the copy of the hard drive was an exact duplicate of the contents of the hard drive.

A court's main concern in considering whether electronic evidence has been authenticated is its trustworthiness. This concern arises from the ability to easily manipulate or alter electronic documents without leaving evidence of the changes. Courts routinely refuse to admit electronic evidence due to their inability to determine whether the evidence is accurate:

- United States v. Jackson, 208 F.3d 633 (7th Cir. 2000). The appellate court affirmed the lower court's refusal to admit internet postings from "white supremacy" groups due to the failure to authenticate the evidence. The Seventh Circuit stated that to authenticate the postings, the defendant had to show that the groups and not the defendant posted the statements in question.

- St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999). The court refused to admit information from the online vessel database of the United States Coast Guard because no way exists to verify the authenticity of the information. Specifically, the court stated that "[a]nyone can put anything on the Internet. No Web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content of any Web-site from any location at any time." (emphasis in original).

### 2. Hearsay

The electronic evidence must satisfy the hearsay requirements. While e-mails are clearly out-of-court statements, printouts from internet sites have also been held to be hearsay. St. Clair, 76 F. Supp. 2d at 775 ("[A]ny evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception."). If the electronic evidence is offered to prove the truth of the statements found in the document or other format, then the evidence is hearsay and must satisfy one of the exceptions to be admitted. Bowe v. State, 785 So. 2d 531 (Fla. Dist. Ct. App. 2001). Several courts have denied admitting electronic evidence for failing to meet the requirements of one of the hearsay exceptions:

- New York v. Microsoft Corp., No. Civ. A. 98-1233, 2002 WL 649951, 2002 U.S. Dist. LEXIS 7683 (D.D.C. Apr. 12, 2002). The court refused to admit several e-mails because they were offered for the truth of the matter asserted, did not satisfy the business records exception of Fed. R. Evid. 803(6) and contained multiple layers of hearsay without establishing any exceptions to the general hearsay rule.

- Monotype Corp. v. Int'l Typeface Corp., 43 F.3d 443 (9th Cir. 1994). The court refused to admit an e-mail due to both the prejudicial nature of the information and the failure to establish an exception to the hearsay rule.

- United States v. Jackson, 208 F.3d 633 (7th Cir. 2000). The court determined that even though an internet service provider could access the information posted by customers, the web postings themselves could not be construed as business records.

Typically, the following exceptions to the hearsay rules are implicated by the use of electronic data:

- The Business Records Exception, Fed. R. Evid. 803(6); Ohio R. Evid. 803(6):

  Hardison v. Balboa Ins. Co., 4 Fed. Appx. 663 (10th Cir. 2001). The court found that Fed. R. Civ. P. 803(6) permits the admission of computer business records if a party introduces a sufficient foundation.

- Party Admissions, Fed. R. Evid. 801(d)(2); Ohio R. Evid. 803(2):

  Sea-Land Servs., Inc. v. Lozen Int'l, LLC, 285 F.3d 808 (9th Cir. 2002). The appellate court determined that the trial court should have admitted an e-mail from the plaintiff to the defendant that was written within the scope of the author's employment as a party admission.

- Present Sense Impression, Fed. R. Evid. 803(1); Ohio R. Evid. 803(1):

  United States v. Ferber, 966 F. Supp. 90 (D. Mass. 1997). Although refusing to admit e-mails under the excited utterance exception, the court found the e-mails satisfied the requirements for a present sense impression because they explained the event in question shortly after it occurred.

- Public Records Exception, Fed. R. Evid. 803(8); Ohio R. Evid. 803(8):

  Lester v. Natsios, 290 F. Supp. 2d 11, 26 (D.D.C. 2003). The court determined that e-mails offered by the defendant federal agency were public records, which "are generally admissible."

As with traditional evidence, a party offering electronic evidence must consider the hearsay implications of electronic evidence and develop a plan or strategy for overcoming the objection.

# V. EFFECTIVELY PRESERVING EVIDENCE

## A. Spoliation of Evidence

### 1. Avoiding Spoliation of Evidence

Attorneys must caution their clients to beware of the consequences of a failure to adequately preserve electronic data that is in their possession.[85] Unlike paper documents that require overt acts like shredding to be destroyed, electronic data can be destroyed through routine use of computers.[86] Merely turning on a computer can eliminate "slack" and "temporary" files, cause data to be overwritten, or change metadata.[87] By clicking on a file, its "last-accessed" date may change, which invites a suggestion that the file has been altered.[88] Attorneys can avoid spoliation of evidence by making sure that their clients understand their preservation responsibilities, informing clients of actions necessary to preserve evidence, and sending opponents preservation letters and/or seeking a preservation order. These issues will be discussed infra with greater detail.

### 2. Sanctions for Spoliation

As the reliance on electronic storage of documents and methods of communication grows, communications or drafts that individuals or companies typically did not preserve or save in the past are now preserved in e-mails and documents saved on computer hard drives, networks or other media. This large increase in potentially discoverable information, along with the numerous locations where electronic data may be stored, results in not only more potential evidence to maintain and review but also greater risk that some evidence may be lost, altered through the general course of business, destroyed as part of an adopted retention policy or destroyed intentionally. These greater risks equate to a higher risk of sanctions for discovery violations, including spoliation.

One recent example illustrating the consequences of a failure to produce electronic evidence was the ruling in a fraud case brought by New York financier Ronald Perelman against investment banking firm Morgan Stanley. Morgan Stanley repeatedly failed to turn over e-mails that were connected to a merger in 1998 between Coleman, Inc. a company owned by Perelman, and Morgan Stanley's client, Sunbeam Corporation.[89] The court ruled that Morgan Stanley had been "grossly negligent" in handling its e-mails.[90] The judge wrote, "The prejudice to [Perelman] from these failings cannot be cured."[91] As a result, the court told jurors that they could infer that Perelman was a victim of fraud.[92] In making this ruling, the judge suggested that Morgan Stanley may have withheld information because it wanted to hide the Securities and Exchange Commission's probe into its e-mail retention policies.[93] Just a week before this ruling, Morgan Stanley disclosed that the SEC was considering enforcement action against it for not properly retaining e-mails.[94]

Another recent example of the possible consequences of a failure to produce electronic evidence is the jury verdict reached in Zubulake. On April 6, 2005, the jury ordered UBS to pay $29.2 million to former saleswoman, Laura Zubulake, who had sued UBS for gender discrimination.[95] The judge had instructed the jury that it could conclude that e-mails that were destroyed contained information adverse to UBS.[96]

### 3. Requirements for an Adverse Inference

Spoliation is "[t]he intentional destruction, mutilation, alteration, or concealment of evidence."[97] As the definition suggests, courts typically require the deletion, alteration or concealment of evidence to be intentional or done in bad faith in order to merit the imposition of sanctions:

- Beck v. Haik, 377 F.3d 624 (6th Cir. 2004). The court defined spoliation to be the intentional destruction of evidence.

- Mathias v. Jacobs, 197 F.R.D. 29, 37 (S.D.N.Y. 2000) vacated on other grounds, 167 F. Supp. 2d 606 (S.D.N.Y. 2001). The court held that the destruction of evidence must be "willfull" to impose an adverse inference.

- Banco Latino, S.A.C.A. v. Gustavo A. Gomez Lopez, 53 F. Supp. 2d 1273, 1277 (S.D. Fla. 1999). The court expressly refused to extend spoliation sanctions to destruction resulting from negligent or reckless acts. The court reasoned that "mere negligence in . . . destroying the records is not enough for an adverse inference, as it does not sustain an inference of consciousness of a weak case."

- Aramburu v. Boeing Co., 112 F.3d 1398, 1407 (10th Cir. 1997). The court held that "[t]he adverse inference must be predicated on the bad faith of the party destroying the records."

- Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (citation omitted). The court stated that "a presumption or inference arises . . . only when the spoliation or destruction [of evidence] was intentional, and indicates fraud and a desire to suppress the truth, and it does not arise where the destruction was a matter of routine with no fraudulent intent."

- Vick v. Texas Employment Comm'n, 514 F.2d 734, 737 (5th Cir. 1975). The court determined that if the party simply destroys documents or records negligently, then the rationale for sanctioning spoliation does not hold.

In contrast, other courts have granted an adverse inference even if the evidence was not destroyed in bad faith:

- Rambus, Inc. v. Infineon Techs. AG, No. 3:00cv524, 2004 WL 383590, 2004 U.S. Dist. LEXIS 2988 (E.D. Va. Feb. 26, 2004), amended by, 220 F.R.D. 264. The plaintiff's employees shredded approximately two million documents as part of its document retention policy put in place after receiving notice of impending litigation. The court concluded that even if the plaintiff "did not institute its document retention policy in bad faith, if it reasonably anticipated litigation when it did so, it is guilty of spoliation" and that "even valid purging programs need to be put on hold when litigation is 'reasonably foreseeable.'"

- Martino v. Wal-Mart Stores, Inc., 835 S. 2d 1251 (Fla. Dist. Ct. App. 2003). The court stated that an adverse inference regarding the destruction of documents arises when a party has possession of self-damaging evidence and either loses or destroys the evidence.

- Wuest v. McKennan Hosp., 619 N.W. 2d 682, 687 (S.D. 2000) (citation omitted). The court stated that if a document "is unavailable because of negligence, or for some reason evidencing a lack of good faith, the jury should be given an adverse inference instruction."

- Am. States Ins. Co. v. Tokai-Seiki (H.K.), Ltd., 704 N.E. 2d 1280 (Miami County 1997). The court stated that "negligent or inadvertent destruction of evidence is sufficient to trigger sanctions where the opposing party is disadvantaged by the loss."

The Zubulake court (discussed earlier) established a three part test to determine when an adverse inference for spoliation is appropriate:

- the party with control over the evidence had a duty to preserve it at the time of destruction;

- the records were destroyed with a "culpable state of mind"; and

- the destroyed evidence was "relevant" to the party's claim or defense and a reasonable trier of fact might find that it would support that claim or defense.

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 220 (S.D.N.Y. 2002). Whether negligent or reckless actions would fulfill the "culpable state of mind" element depends upon the jurisdiction. Zubulake argues, however, that intentional destruction per se establishes the relevance required in the third element. Id.

### 4. Other Sanctions For Spoliation

Although the adverse inference instruction is the most common sanction for failing to preserve evidence, courts may award financial sanctions or even dismiss the case:

- Covucci v. Keane Consulting Group, Inc., 2006 Mass. Super LEXIS 313 (Mass. Sup. Ct. May 31, 2006) Court dismissed plaintiff's complaint after finding that plaintiff's deletion of e-mail and scrubbing of files from computer was evidence of persistent bad-faith repudiation of discovery obligations, intentional spoliation, and fraud on the court.

- Phoenix Four, Inc. v. Strategic Res. Corp., 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. May 23, 2006). Court ordered monetary sanctions to be paid by defendant following late production of several hundred boxes of printed electronic documents. Court, however, refused to order an adverse inference instruction or bar filing of summary judgment motion.

- DaimlerChrysler Motors v. Bill Davis Racing, Inc., 2005 U.S. Dist. LEXIS 38162 (E.D. Mich. Dec. 22. 2005) Monetary sanctions and adverse inference order by court after defendant failed to suspend normal document destruction procedures after filing of lawsuit.

- United States v. Phillip Morris USA Inc. f/k/a Phillip Morris Inc., 327 F. Supp. 2d 21 (D.D.C. July 21, 2004). The defendant continued to delete e-mails under its retention policy for two years after a court order to preserve all evidence and for several months even after learning that its retention policy was inadequate in light of the litigation. The court precluded the defendants from calling a key employee at trial who failed to preserve documents and ordered the defendants to pay costs, as well as $2,750,000 in sanctions.

- QZO, Inc. v. Moyer, 594 S.E.2d 541 (S.C. Ct. App. 2004). The court granted default judgment against the defendant, after he delayed in providing his computer to the plaintiff and reformatted the hard drive erasing relevant information.

- RKI, Inc. v. Grimes, 177 F. Supp. 2d 859 (N.D. Ill. 2001). The court found that the defendant defragmented his home computer to prevent plaintiff from discovering the deletion of confidential information and software. The court ordered the defendant to pay $100,000 in compensatory damages, $150,000 in punitive damages, attorneys' fees and court costs.

- Long Island Diagnostic Imaging v. Stony Brook Diagnostic Assocs., 286 A.D.2d 320 (N.Y. App. Div. 2001). The court dismissed the defendants' counterclaims and third party complaint due to their spoliation of evidence.

5. Independent Causes of Action for Spoliation

In addition to potential spoliation sanctions in the pending matter, some jurisdictions, including Ohio, also recognize an independent cause of action for the destruction of documents. In these states, a party may bring a separate case claiming damage resulting from the destruction in the previous action. To prove the tort of intentional spoliation in Ohio, a party must prove five elements:

1. "[P]ending or probable litigation involving the plaintiff,
2. knowledge on the part of defendant that litigation exists or is probable,
3. willful destruction of evidence by defendant designed to disrupt the plaintiff's case,
4. disruption of the plaintiff's case, and
5. damages proximately caused by the defendant's acts."

Smith v. Howard Johnson Co., 615 N.E.2d 1037, 1038 (Ohio 1993).

Although not recognized in Ohio,[98] some jurisdictions, including California and the District of Columbia, recognize an independent action for the tort of negligent spoliation. Typically the following elements must be shown:

- "the existence of a potential civil action;
- a legal or contractual duty to preserve evidence relevant to the action;
- negligent destruction of evidence;
- significant impairment of the ability to prove the underlying lawsuit;

- a causal relationship between the destruction of evidence and the inability to prove the underlying lawsuit; and damages."[99]

## B. Your Client's Preservation Responsibilities

All parties "are obligated to take appropriate measures to preserve documents and information . . . reasonably calculated to lead to the discovery of admissible evidence and likely to be requested during discovery."[100] The duty attaches when the party has knowledge or notice of the relevance of evidence to the dispute. A party may receive notice of the duty to preserve or the evidence's relevance through:

- Prior Litigation
- Pre-litigation Communications or Other Information
- Filing of a Complaint
- Discovery Requests
- Federal Rules of Civil Procedure
- Court Orders
- Statutes

### 1. Scope of Evidence that Must Be Preserved

Although a party has a duty to preserve all documents or other evidence that may lead to relevant information, courts acknowledge that not every e-mail or other electronic evidence can realistically be preserved once a party has notice of the duty to preserve. For example, in Concord Boat Corp. v. Brunswick Corp., No. LR-C0-95-781, 1997 33352759, 1997 U.S. Dist. LEXIS 24068, at *16-17 (E.D. Ark. Aug. 29, 1997), the court determined that the duty to preserve arose only with the filing of the complaint and not during previous antitrust litigation because "to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail."

Furthermore, the court in Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003), a decision in a leading case relating to electronic discovery, noted that "[a]s a general rule, . . . a party need not preserve all backup tapes even when it reasonably anticipates litigation." The court went on to note however, that any "unique, relevant evidence that might be useful to an adversary" must be preserved. Id. at 218. The Zubulake court also clarified that the duty extends only to the employees likely to have relevant information and that the duty generally does not extend to inaccessible backup tapes. Id. The court added, however, if a party can determine which backup tapes contain specific employees' electronic data, then those tapes must be preserved. Id.

The Zubulake court also provided a preferred data preservation procedure once the duty to preserve attaches:

- Preserve backup tapes for key employees or others with relevant information
- Retain both current and archived backup tapes identified as potentially relevant
- Catalog documents created after the duty attaches in a separate file for easy collection and review
- Take mirror images of computer hard drives.

Id.

### 2. Retention Policies

Courts commonly find that the duty to preserve relevant information overrides any company retention policies covering the document or data:

- Bradley v. Sunbeam Corp., No. 5: 99 CV144, 2003 WL 21982038, 2003 U.S. Dist. LEXIS 14451, at *38-40 (N.D. W.Va. Aug 4, 2003). The court ruled that the duty to preserve exceeds a company's duty "to do nothing more than follow its own internal policy."

- Trigon Ins. Co. v. United States, 204 F.R.D. 277, 289 (E.D. Va. 2001). The court stated "document retention policies . . . do not trump the Federal Rules of Civil Procedure or requests by opposing counsel . . . . [E]xecution of a document retention policy that is at odds with the rules governing the conduct of litigation does not protect [the party] from a finding of intentional destruction."

- Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988). The court stated that "if the corporation knew or should have known that the documents would become material at some point in the future[,] then such documents should have been preserved. Thus, a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."

### 3. Practical Advice Regarding Preservation of Data

Once a party becomes aware that litigation may be forthcoming, it should take action to preserve all documents, whether electronic or hard copy, related to the potential litigation. The following steps assist in effectively fulfilling a party's duty to preserve electronic data:

- Suspend routine document destruction or alteration required under document retention policy.

- Involve counsel in determining both issues relevant to the case and that may lead to relevant discovery.

- Send a priority memorandum, with periodic reminders thereafter, to the appropriate employees, including those in information technology, instructing them to preserve all documentation relevant to the litigation. The order should include the issues involved in the litigation and remind the employees that the data retention policy no longer applies to these issues.

- Obtain copies of all hard copy documents.

- Develop working knowledge of the technology systems to determine storage media, locations and length of storage. This knowledge should also include whether the system overwrites deleted information. Depending upon the complexity of the system, this step may also require consulting a computer forensics expert to determine an effective strategy for preserving and maintaining electronic data.

- Designate an employee to be responsible for the collection and protection of relevant documents and information.

C. Preservation of Evidence

1. Preservation of Evidence Letter

The most effective way to provide early notice to a party of its duty to preserve evidence is to send a letter to opposing counsel or the party, if prior to filing a complaint, requesting him or it to preserve all information, including electronic evidence, related to the matter.[101] This letter should contain, at a minimum, the following information:

- A description of the subject matter of the dispute.
- A very broad description of potentially relevant documents mirroring the description provided to your own client.
- A generic listing of locations where electronic data may be stored, including, but not limited to, hard drives, archival or backup tapes, laptop computers, home computers, voice-mail systems, handheld computers, networks, cell phones, proprietary online services, third-party storage repositories, and intranets.
- A request that the opposing party's document retention policy be reviewed and suspended or modified to prevent routine destruction of electronic and printed materials.
- A request that the opposing party's management information systems and information technology personnel be notified of the need to preserve data.

Finally, counsel should include the need to preserve all electronic evidence in the Conference Report required by Fed. R. Civ. P. 16 or Ohio R. Civ. P. 16. By including it in the Rule 16 Conference Report, all parties, including the court, clearly have been notified of the duty and its potential breadth. Furthermore, it is also important to send reminder notices of the continuing obligation to preserve evidence throughout the litigation.

### 2. Preservation Order

If there is a strong likelihood that an adversary is likely to alter or destroy relevant electronic evidence before production, it is advisable to seek a preservation order.[102] Such a preservation order should require the opponent to take all necessary steps to preserve electronic evidence or it should allow on-site inspection of the adversary's computers and storage media.[103]

## D. Preserving the Chain of Custody

A chain of custody for electronic evidence must be maintained and documented when collecting the data. Much like evidence in a criminal case, a proponent of the evidence must show that the electronic document or recording presented in court is the same document or recording that existed prior to the commencement of the litigation. In other words, the proponent must show that no alteration or manipulation of the data has occurred. The following information should be documented each time data is collected or shared:

- "Date, time, and place of collection or receipt.
- The name of the individual who collected or received the evidence.
- A description of what was obtained, including media-specific information.
- Media type, standard, and manufacturer.
- All movement of evidence (evidence transfer) and the purpose of the transfer.
- Physical (visual) inspection of evidence.
- Procedures used in collecting and analyzing the data.
- Date and time of check-in and check-out of media from secure storage."[104]

## VI. EFFICIENT STRATEGIES FOR DISCLOSURE AND DISCOVERY

### A. Developing Effective Search Plans

Developing a comprehensive search plan for collecting, analyzing and producing electronic data is essential to ensuring that all relevant data is obtained. The most important part of developing an effective search plan is understanding how the targeted system(s) create, store, and destroy electronic evidence.[105] It is also imperative that lawyers consider how they are going to use the digital data they obtain from their opponents. Generally, an effective electronic discovery plan should include the following steps:

- "Enforcing initial disclosure requirements;
- Participating in and gaining agreements via the Rule 16 Conference pursuant to the Federal Rules of Civil Procedure;
- Framing initial interrogatories relating to your opponents' management of e-evidence;
- Taking Rule 30(b)(6) depositions of IT representatives pursuant to the Federal Rules of Civil Procedure;
- Issuing requests for production and onsite inspections; and
- Enforcing compliance via motions to compel and motions for sanctions."[106]

### B. The Role of Depositions and Witness Examination (Deposing the Opposition's IT Experts)

After Federal Rule 26 initial disclosures, attorneys can acquire more in-depth information from their opponents through a combination of traditional discovery tools including interrogatories, requests for document production, and depositions.[107] A Rule 30(b)(6) deposition is an excellent tool that can be used to obtain more information about the layout of an opponent's computer system, which can guide further discovery.[108]

If the opponent is a company, it is best to depose the person who has the most knowledge of:

- "the number, types, and locations of computers currently in use and no longer in use
- the operating systems and application software the company is using including the dates of use
- the company's file-naming and location-saving conventions
- disk- or tape-labeling conventions
- backup and archival disk or tape inventories or schedules
- the most likely locations of electronic records relevant to the subject matter of the case
- backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time
- electronic-records-management policies and procedures
- corporate policies regarding employee use of company computers and data
- the identities of all current and former employees who have or had access to network administration, backup, arching, or other system operations during the relevant period."[109]

### C. Using Interrogatories, Requests for Production and Requests for Inspection

After obtaining the information pertaining to electronic data from the 30(b)(6) deposition, attorneys should refine their discovery requests to obtain relevant data from the locations and systems that were identified in the deposition.[110] Under the amended Federal Rules of Civil Procedure, it is essential that requests for electronic data be carefully crafted.[111] A request that asks for "all electronic data" is likely to result in an objection founded on burden or expense.[112] Accordingly, electronic discovery requests need to be specific as well as demonstrate an understanding of the creation, storage, and destruction of electronic data.[113]

Depending on the issues in a particular case, the types of electronic data that may be useful to obtain from an opponent will vary. "However, you should consider the following categories of evidence when crafting your requests for production:

- e-mail (sent, received, or drafted) and corresponding dates, times, recipients, and file attachments
- word-processing files
- tables, charts, graphs, and database files
- electronic calendars
- proprietary software files
- Internet browsing applications (bookmarks, cookies, history log)."[114]

When crafting interrogatories regarding electronic data, lawyers should "consider asking for:

- The identity of the individuals that searched for, located, preserved, and produced electronic data;
- A description of all steps taken to search for, locate preserve, and produce electronic data;
- A description of all relevant hardware and software; and
- The identity of the person(s) most knowledgeable about various aspects of such systems."[115]

Finally, attorneys should consider requesting a site inspection of the opponent's computer system in appropriate circumstances.[116] Such a request can be made under Fed. R. Civ. P. 34(a)(2). Onsite inspections are particularly useful when the opponent has a unique and proprietary computer system for example.[117] Data stored in a database is also often difficult to produce due to the inherent architecture of databases.[118] A document request will not typically allow access to the information being sought because a database is a grouping of data rather than a series of actual documents.[119] The best way to access database information is to inspect the database onsite with the help of a qualified database expert who will be able to formulate the proper queries to identify and obtain relevant data in a format that is usable.[120]

### D. Acquiring Electronic "Images" of Data Sources

It is important to understand the difference between copying and imaging. "Copying" limits the information that is captured to only the data that the user created and could see on the screen.[121] In contrast, "imaging" "is a bit by bit digital record of an entire hard drive, disk or tape."[122] Imaging is also known as mirror imaging or mirroring.[123] This process allows extraction of all the information that one can extract from an original.[124] Attorneys should be prepared to argue why imaging is necessary by obtaining a statement from an expert about the differences between copying and imaging because imaging catches a broader array of information, is more expansive, and can implicate concerns regarding privilege and breadth.[125]

A computer forensics expert can serve as a guide to which technique is best to use.[126] Since imaging will help address questions of authentication and issues of who created or altered a document and when and how it occurred, imaging can be especially useful in cases involving fraud or electronic evidence tampering.[127] Imaging also permits the recovery of deletions, amendments, and additions, which can be powerful evidence of spoliation.[128] Hidden text, which is not always shown on the screen or when a document is printed, can be revealed by imaging.[129] Finally, imaging permits the recovery of information about historical changes that occur when users save different version of documents.[130] This tactic can be particularly useful when considering the electronic files related to an opposing expert's reports.

## E. Production of Forensic Evidence and Findings

### 1. Authentication and Admissibility

One of the issues of dealing with electronic evidence is authentication and admissibility. All of the rules of evidence that apply to paper also apply to electronic evidence, and in many jurisdictions, it is now settled law that computer produced evidence is admissible at trial.[131] Counsel must use the same protocols for laying foundation of paper document in order to lay a foundation for a computer-printed document.[132] "This includes testimony about who created the document, when it was created, who received the document, where it was located, how it pertains to the relevant legal issues in the case, etc."[133] Caselaw has held that the testimony of the company employee who created the databases was sufficient foundation to admit database documents.[134]

### 2. Expert Testimony and Reporting

After the data analysis is complete, computer forensic engineers can help support the attorney and client's case by making customized reports about the data that was collected and produced.[135] They can also provide data for affidavits or other pleadings, give expert testimony as well as Rule 26 expert reports.[136]

#### a. Disclosure of Experts

However, in some situations, parties may not want to disclose their retained electronic evidence experts and the experts' findings and must determine if it is required under Federal Rule of Civil Procedure 26(a)(2).[137] In analyzing the rule, caselaw construing the rule, and Federal Rules of Evidence relating to experts, there is some guidance on this issue.[138] The basic questions that counsel should consider are:

- "Will any testifying expert rely on computer data provided by either party, or will the expert rely on data obtained through his or her own investigations?

- Will any testifying expert use custom, proprietary, or publicly-available software to process data, generate a report, or present to the court?
- Does counsel anticipate requesting discovery of either the underlying data or the software used by any testifying expert?"[139]

Given their similarity to other kinds of scientific or technical expert witnesses (such as medical experts, engineering experts, or fire experts), computer forensic experts are likely to fall within the gambit of the Rules and should be disclosed under Rule 26(a)(2) accordingly.[140]

The need to disclose electronic discovery experts, who assist with collection, filtering, and production of electronic evidence, is not as clear because such an expert may be used simply as a records-custodian.[141] If an electronic discovery expert is needed to establish chain of custody, then that expert is a foundational witness that does not need to be disclosed under Rule 26.[142] Failure to disclose an expert as required can result in a court finding that the expert cannot testify or provide evidence.[143] Therefore, it is best to err on the side of caution and to include electronic discovery experts in disclosures made under Rule 26(a)(2).[144]

### b. Discovery of Computer-Related Materials Relied on by Experts

Courts have consistently permitted parties broad discovery into computer-related materials that are relied on by experts at trial.[145] If an expert is given access to a computerized database and relies upon it when forming his or her opinions, it is likely that a court will require that the party produce the system, even if it contains protected work product:[146]

- Fauteck v. Montgomery Ward & Co., 91 F.R.D. 393 (N.D. Ill. 1980). The court ordered the production of a database, containing defendant's personnel records, which was created to serve as a foundation for expert testimony. Defendant claimed the protection of work product immunity; however, the court found that production of the database was necessary to assure effective cross-examination.

- Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648 (W.D. Ky. 1987). The court ordered the production of a database plaintiff's expert was relying upon, and it also required plaintiff to produce codebooks, a user's manual, and all documents used in encoding the database. However, the court refused to require production of all documents relating to the programs used to create the database or of all print-outs generated by the database because such discovery was overly broad, exceeded the proper scope of relevance, and was likely to reveal alternative methods of analyses or alternative computer programs deemed beyond the proper scope of expert discovery under Fed. R. Civ. P. 26.

- Bartley v. Isuzu Motors Ltd., 151 F.R.D. 659, 660 (D. Colo. 1993). The court allowed broad discovery of computerized accident simulations conducted by plaintiff's expert, including not only the simulation to be used at trial, but also all simulations run before deciding which simulation to use at the trial. The court reasoned that a party cannot defend against computer-aided simulations unless the party is allowed "access to the data that represents the computer's work product . . . the data [entered] into the computer, the programs used to manipulate the data and produce the conclusions, and the theory or logic employed by those who planned and executed the experiment."

- DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002). Plaintiffs sought discovery sanctions because they alleged that defendant's expert report relied on computerized transaction data that defendants withheld from plaintiffs during discovery. The discovery request that was at issue sought "[a]ll summary documents (including electronic data) relating to your leaf tobacco bids, purchases, or price paid, including but not limited to the entire Tobinet database in electronic form." Defendant's expert relied heavily on database data and other computerized data; however, plaintiffs were only provided the database data after the defendant's expert report was issued. The court held that it was unfair to plaintiffs to withhold the data and the court allowed plaintiffs to respond to the report, but did not provide an opportunity for defendant to reply.

- City of Cleveland v. Cleveland Electronic Illuminating Co., 538 F. Supp. 1257 (N.D. Ohio 1980). In an antitrust case that a city brought against an electric utility, the court found that the electric utility was entitled to pretrial production by the city of computer data and calculations, which were the basis for the conclusions in reports of experts that the city intended to call as witnesses.

- United States v. Dioguardi, 428 F.2d 1033 (2d Cir.), cert. denied, 400 U.S. 825 (1970). The Court granted a discovery request for the complete software program that was used to generate an expert's report.

Under certain circumstances, courts even allow for discovery from a non-testifying expert. Parties seeking discovery of facts known or opinions held by consulting experts who are expected to testify at trial have the burden of demonstrating the existence of exceptional circumstances.[147] This has been characterized as a heavy burden.[148] A court may find exceptional circumstances where parties seeking discovery cannot obtain equivalent information essential to preparation of the case from other sources.[149] Several cases have held that exceptional circumstances permitting "discovery of a non-testifying expert's opinion exist where the object or condition observed is not observable by an expert of the party seeking discovery."[150] Exceptional circumstances can also be shown where a non-testifying expert's report will be used as the basis for a testifying expert's opinion.[151]

- Pearl Brewing Co. v. Jos. Schlitz Brewing Co., 415 F. Supp. 1122, 1139 (S.D. Tex. 1976). Plaintiff's testifying expert relied on a computer program developed by the plaintiff's non-testifying experts. The court required production of all documents concerning the details of the computer program and allowed defendant to depose the non-testifying experts for additional information about the computer programs. The court found that there were exceptional circumstances warranting discovery of the non-testifying experts because defendant needed to fully understand the nature of the computer programs used by the testifying expert to prepare an effective cross-examination of the testifying expert and because only the non-testifying experts could interpret the computer programs used by testifying expert.

- Derrickson v. Circuit City Stores, No. DKC 95-3296, 1999 U.S. Dist. LEXIS 21100, *17-20 (D. Md. Mar. 19, 1999), aff'd 203 F.3d 821 (4th Cir. 2000). The court ordered plaintiff to disclose the data produced by the testifying expert's assistant, how the data was manipulated, and the instructions the expert's assistant entered into a computer program to produce the tables upon which the expert relied. The court did not consider the work of the expert's assistant to be the work of a "non-testifying" expert because the expert and his assistant had worked so closely together. However, the court went on to state that even if the expert's assistant was considered to be a non-testifying expert, the result would be the same because only the expert's assistant knew what he did with the data and defendant was entitled to that information under Fed. R. Civ. P. 26(b)(4)(B). In dicta, the court also noted that it was inclined to think that defendant could not only obtain underlying data but also depose and cross-examine the expert's assistant at trial.

[1] "Electronic Discovery: Questions and Answers," Civil Action, Summer 2004, at 1.

[2] "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production," Jan. 2004, at 1, available at http://www.thesedonaconference.org/publications_html (last visited Mar. 30, 2005).

[3] Id.

[4] "Electronic Discovery: Questions and Answers," *supra* note 1.

[5] "The Sedona Principles," *supra* note 2.

[6] "The Sedona Principles," *supra* note 2.

[7] MICHELE C.S. LANGE & KRISTIN M. NIMSGER, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW 2 (2004).

[8] Id.

[9] Id.

[10] Id.

[11] Kristin M. Nimsger, "Digging for E-Data," Trial, Jan. 2003, at 1.

[12] US News & World Report, Feb. 2000.

[13] Thor Valdmanis, Adam Shell & Elliot Blair Smith, "Marsh & McLennan accused of price fixing, collusion," USA Today, Oct. 15, 2004, at 1, available at http://www.usatoday.com/money/industries/insurance/2004-10-15-spitzer-insurance_x.htm (last visited Mar. 30, 2005).

[14] Id.

[15] Id. In January of 2005, Marsh & McLennan agreed to pay $850 million in restitution to settle the insurance charges against it. The Associated Press, "Marsh & McLennan settles insurance charges," available at http://www.msnbc.msn.com/id/6889406/ (last visited Mar. 30, 2005).

[16] Dulce J. Foster, "The Virtual Smoking Gun: The Role of E-Mail in White Collar Cases," available at http://www.fredlaw.com/articles/whitecollar/whit_0501_djf.html (last visited Mar. 30, 2005).

[17] Id.

[18] Id.

[19] "The Sedona Principles," *supra* note 2, at 3.

[20] Ken Withers, "Is Digital Different," Civil Action, Summer 2004, at 9.

[21] "The Sedona Principles," *supra* note 2, at 3.

[22] "The Sedona Principles," *supra* note 2, at 3.

[23] Withers, *supra* note 13.
[24] Withers, *supra* note 13.
[25] "The Sedona Principles," *supra* note 2, at 4.
[26] "The Sedona Principles," *supra* note 2, at 4.
[27] "The Sedona Principles," *supra* note 2, at 4.
[28] Withers, *supra* note 13.
[29] Withers, *supra* note 13.
[30] Withers, *supra* note 13.
[31] "The Sedona Principles," *supra* note 2, at 5.
[32] "The Sedona Principles," *supra* note 2, at 5.
[33] Summation has released WebBlaze, a browser based product permitting access to the database without installing the application. WebBlaze may be integrated with certain versions of the Summation product to provide internet access to case data hosted internally.
[34] Lesley Friedman Rosenthal, "Electronic Discovery Can Unearth Treasure Trove of Information or Potential Land Mines," New York Bar Association Journal, Sept. 2003, at 32.
[35] "The Sedona Principles," *supra* note 2, at 5.
[36] "The Sedona Principles," *supra* note 2, at 5.
[37] "The Sedona Principles," *supra* note 2, at 5.
[38] William "Mo" Cowan & Kwabena Abboa-Offei, "A Practical Guide to Conducting Electronic Discovery," The Practical Litigator, Jan. 2005, at 34. This topic is more fully discussed in section (I)(I).
[39] Id. This topic is more fully discussed in section (IV)(A).
[40] Id. This topic is more fully discussed in section (I)(F).
[41] Rosenthal, *supra* note 34, at 35.
[42] Rosenthal, *supra* note 34, at 35.
[43] David K. Isom, "Electronic Discovery: New Power, New Risks," Utah Bar Journal, Nov. 2003, at 12.
[44] Id.
[45] Kenneth J. Withers, "Electronic Discovery Disputes: Decisional Guidance," Civil Action, Summer 2004, at 5.
[46] Cowan, *supra* note 38.
[47] Isom, *supra* note 43.
[48] Isom, *supra* note 43.
[49] Cowan, *supra* note 38, at 34.
[50] Cowan, *supra* note 38, at 34.
[51] "The Sedona Principles," *supra* note 2, at 51-52; Lange, *supra* note 7, at 241-49; MICHAEL R. ARKFELD, ELECTRONIC DISCOVERY AND EVIDENCE G-1-G13 (2004).
[52] Kristin M. Nimsger & Michele C.S. Lange, "E is for Evidence: Examining Recent E-Discovery Developments, Winter 2005, at 9.
[53] Nimsger & Lange, *supra* note 52; Jakob Z. Norman, "Electronic Discovery: Best Practices, New Rules, and a Tight Budget," The Young Lawyer, Mar. 2005.
[54] LexisNexis Applied Discovery Court Rules, "Update on Draft Electronic Discovery Amendments to the Federal Rules of Civil Procedure" available at http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp (last visited Aug. 31, 2006).
[55] LexisNexis Applied Discovery Court Rules, "Proposed Rule of Evidence 502" available at http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp (last visited Aug. 31, 2006).
[56] Id.
[57] Jicarilla Apache Nation v. United States, 60 Fed. Cl. 413, 416 (Fed. Cir. 2004).
[58] Committee on Rules of Practice and Procedure, "Proposed Amendments to the Federal Rules of Civil Procedure," at 25 available at (last visited Aug. 31, 2006).
[59] Id. at 28.
[60] Id. at 40.
[61] Id. at 52.
[62] Id. at 31.

[63] Id. at 62.
[64] Id.
[65] Id. at 64.
[66] Id.
[67] Id. at 81.
[68] LexisNexis Applied Discovery Court Rules, *supra* note 58.
[69] LexisNexis Applied Discovery Court Rules, *supra* note 59.
[70] Id.
[71] S.D. Ohio Civ. R. 26.1(a).
[72] LexisNexis Applied Discovery Court Rules, "State and Local District Court Rules" available at http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp (last visited Aug. 31, 2006).
[73] Id.
[74] Id.
[75] Id.
[76] Id.
[77] Id.
[78] Id.
[79] Ohio R. Civ. P. 33(A)
[80] Ohio R. Civ. P. 33, Staff Notes
[81] Id.
[82] Ohio R. Civ. P. 36(A), Staff Notes
[83] LexisNexis Applied Discovery Court Rules, *supra* note 75.
[84] Id.
[85] Nimsger, *supra* note 11, at 4.
[86] Nimsger, *supra* note 11, at 4.
[87] Nimsger, *supra* note 11, at 4.
[88] Nimsger, *supra* note 11, at 4.
[89] Ameet Sachdev, "E-mails Become Trial for Courts: Costly Electronic Discovery 'Part of Potentially Every Case in the 21st Century,' Chicago Tribune, April 10, 2005, at 1.
[90] Id.
[91] Id. at 3.
[92] Id.
[93] Id.
[94] Id.; Shira Ovide, "SEC Considers Action Against Morgan Stanley," Dow Jones Newswires, April 7, 2005, at 1.
[95] Gail Appelson, "U.S. Jury Says UBS Must Pay $29.2 Million for Bias," MSNBC, April 6, 2005, at 1.
[96] Sachdev, *supra* note 5, at 4.
[97] Black's Law Dictionary 1409 (7th ed. 1999).
[98] White v. Ford Motor Co., 142 Ohio App. 3d 384, 388, 755 N.E. 2d 954 (2001).
[99] Adam I Cohen and David J. Lender, Electronic Discovery: Law and Practice § 3.04[A][2] (citing Bart S. Wilhoit, Comment, Spoliation of Evidence: The Viability of Four Emerging Torts, 46 U.C.L.A. Law Rev. 631, 644 (1998)).
[100] Madden v. Wyeth, No. 3-03-CV-0167-R, 2003 WL 21443404, 2003 U.S. Dist. LEXIS 6427, at *3 (N.D. Tex. Apr. 16, 2003).
[101] A sample preservation letter can be found at http://www.krollontrack.com/library/sampleclient.pdf (last visited Mar. 31, 2005).
[102] Cowan, *supra* note 38, at 36.
[103] Cowan, *supra* note 38, at 36. *See, e.g.*, Armstrong v. Executive Office of the President, 821 F. Supp. 761 (D.D.C. 1993); Sega Enter., Ltd v. MAPHIA, 948 F. Supp. 923, 927 (N.D. Cal. 1996); Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90, 109-14 (Colo. 1996).

[104] LexisNexis Applied Discovery Fact Sheet, "5 Steps for Gathering Electronic Data Effectively" available at http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_5StepsDataGathering.pdf (last visited Mar. 31, 2005).
[105] Nimsger, *supra* note 11, at 2.
[106] Lange, *supra* note 7, at 29.
[107] Nimsger, *supra* note 11, at 2.
[108] Nimsger, *supra* note 11, at 2.
[109] Nimsger, *supra* note 11, at 3.
[110] Nimsger, *supra* note 11, at 3.
[111] Nimsger, *supra* note 11, at 3.
[112] Nimsger, *supra* note 11, at 3.
[113] Nimsger, *supra* note 11, at 3.
[114] Nimsger, *supra* note 11, at 3.
[115] Cowan, *supra* note 38, at 37-38.
[116] Cowan, *supra* note 38, at 37.
[117] Lange, *supra* note 7, at 38.
[118] Lange, *supra* note 7, at 38.
[119] Lange, *supra* note 7, at 38.
[120] Lange, *supra* note 7, at 38.
[121] Cowan, *supra* note 38, at 37.
[122] Cowan, *supra* note 38, at 37.
[123] Lange, *supra* note 7, at 246.
[124] Cowan, *supra* note 38, at 37.
[125] Cowan, *supra* note 38, at 37.
[126] Cowan, *supra* note 38, at 37.
[127] Cowan, *supra* note 38, at 37.
[128] Cowan, *supra* note 38, at 37.
[129] Cowan, *supra* note 38, at 37.
[130] Cowan, *supra* note 38, at 37.
[131] Lange, *supra* note 7, at 75.
[132] Lange, *supra* note 7, at 75.
[133] Lange, *supra* note 7, at 75.
[134] Lange, *supra* note 7, at 75-76. People v. Markowitz, 721 N.Y.S. 2d 758 (N.Y. Sup. Ct. 2001).
[135] Lange, *supra* note 7, at 93.
[136] Lange, *supra* note 7, at 93.
[137] Lange, *supra* note 7, at 31.
[138] Lange, *supra* note 7, at 31.
[139] Lange, *supra* note 7, at 31 (citing Kenneth J. Withers, "Computer Based Discovery in Federal Civil Litigation," Federal Courts Law Review, Oct. 2000).
[140] Lange, *supra* note 7, at 31.
[141] Lange, *supra* note 7, at 31.
[142] Lange, *supra* note 7, at 31.
[143] Lange, *supra* note 7, at 31.
[144] Lange, *supra* note 7, at 31.
[145] Mark D. Robins, Computers and the Discovery of Evidence - A New Dimension to Civil Procedure, 17 J. Marshall J. Computer & Info. L. 411, 428 (1999); Devin Murphy, Electronic Commerce in the 21st Century: Article the Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need to Know, 27 Wm. Mitchell L. Rev. 1825, 1832 (2001).
[146] ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE 8-17 (2005).
[147] Hartford Fire Ins. Co. v. Pure Air on the Lake Ltd. P'ship, 154 F.R.D. 202, 208-09 (N.D. Ind. 1993).
[148] Id.
[149] Id.

[150] Id. quoting Delcastor, Inc. v. Vail Assocs., Inc., 108 F.R.D. 404, 409 (D. Colo. 1985).
[151] Hartford Fire Ins. Co., 154 F.R.D. at 208.