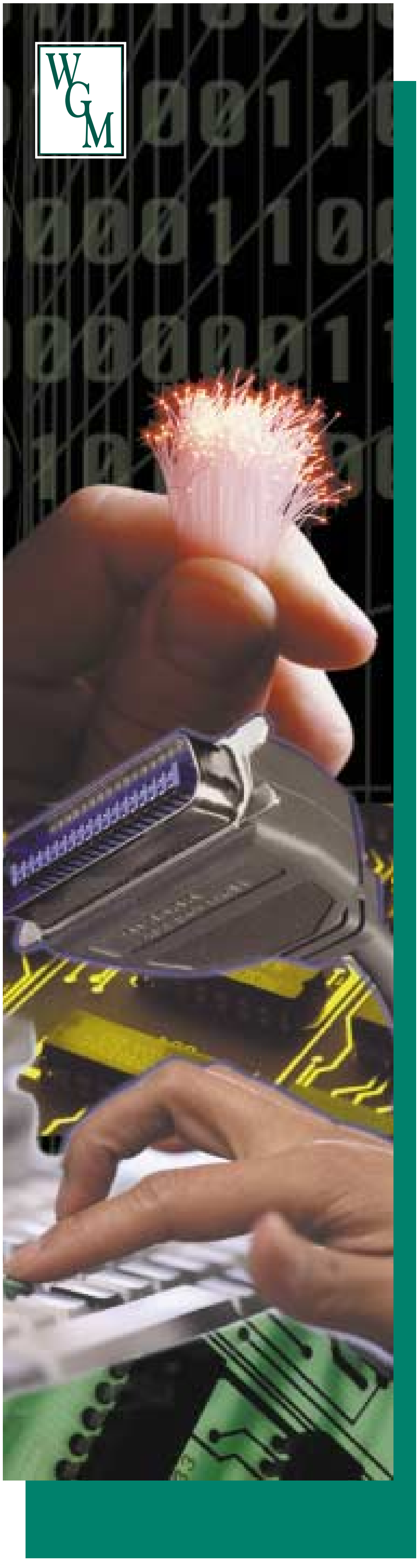

Electronic Discovery Practice Guidelines

By
Adam I. Cohen
David J. Lender

Weil, Gotshal & Manges LLP

Contents

Introduction: Why is electronic discovery important and how is it different from traditional discovery of paper documents? 1

Prepare for electronic discovery by developing a general understanding of your client’s computer systems 2

Lay the groundwork for successful electronic discovery 4

Conduct electronic discovery in a manner calculated to obtain all required information while avoiding discovery disputes and controlling costs 7

E-mail communications may raise questions regarding attorney-client confidentiality and privilege 12

Computerized litigation support systems raise work product issues in electronic discovery 13

E-mail can be especially damaging and special practices should be applied 14

Effective electronic discovery often requires expert assistance 15

Electronic information may raise unique evidentiary issues 15

Appendix A: Examples of relevant case law A1

Appendix B: Computer terms and issues relevant to electronic discovery B1

▼ Introduction: Why is electronic discovery important and how is it different from traditional discovery of paper documents?

The nature and volume of electronic information generated in the course of contemporary business operations and communications significantly increases both the opportunities and risks of discovery, primarily because:

- Electronic information that has been "deleted" by common programs is often not erased and may be recoverable;
- Common computer programs often generate numerous copies of electronic documents without the knowledge of the user;
- "Back-ups" of many types of electronic information periodically made to guard against systems failures are often retained and archived;
- Electronic versions of E-mails and word processing documents may reveal information (such as draft versions, "bcc" recipients, etc.) that exists only in electronic form and not on hard copies;
- Even when voluminous, electronic information may be easier to search and analyze than paper documents;
- People are often casual and careless when communicating via E-mails as opposed to hard copy memoranda and correspondence.

▼ Prepare for electronic discovery by developing a general understanding of your client's computer systems

Specifically, obtain information regarding:

▼ **potential locations for electronic information** including, for example:

- ***diskettes*** in office or home,
- ***hard drives*** in office or home, portable drives, laptops off-site,
- ***files on network servers,***
- on and off site ***backup files***, etc.

Consider recommending a survey to be completed by employees regarding computer use, including home computer and handheld personal organizer device use.

▼ **whether your client has a retention policy** or regular practices governing electronic information and what procedures, if any, are in place to enforce such policy or practices

- if your client does not have such a policy, advise your client to establish an electronic information retention policy, and to
  - ▾ weigh the costs and benefits of requiring permanent erasure of certain records after a certain period of time has elapsed;
  - ▾ extend the retention policy to all copies of electronic files, including, *e.g.*, ***archival*** E-mail, ***back-ups*** of ***hard drives*** and ***network files;***
  - ▾ monitor the effectiveness of the retention policy and see that it is enforced — once litigation commences, it is too late to learn that:
    - – information was not deleted pursuant to the deletion policy, or
    - – information that should have been preserved has been destroyed.
  - ▾ avoid policies that would call for the selective purging of information
    - – that may be looked at skeptically by a court if the policy is challenged in litigation
    - – make sure that the retention policy compares well with business and industry practice

Prepare for electronic discovery by developing a general understanding of your client’s computer systems

Specifically, obtain information regarding (cont’d):

- **how electronic information is stored and organized**
  - period of time existing storage/organization system has been in effect, including:
    - daily, weekly, monthly backup procedures;
    - how back-ups are stored; when and what storage media are recycled;
    - what versions of applications reside on older backed-up information, etc.
  - treatment of deleted information:
    - is it designated to be overwritten? or
    - does the system automatically overwrite deletions with garbled data or random characters?
    - does system include undelete program that can restore deleted files?
- **cost and effort involved in locating electronic information** of various types and converting it into readable form
- **corporate policies and practices regarding use of E-mail** and review of employee E-mail

▼ assure the preservation of electronic information by taking early precautions

- put your adversary on notice
  - that information contained on computer systems may be relevant to the dispute
  - that your adversary should take immediate steps to preserve such information
    - Prepare notice letter to adversary identifying:
      - the type of electronic information to be preserved (*e.g.*, E-mail, data files created by word processing, electronic calendars, etc.)
      - the scope of locations where such information may exist (*e.g.*, servers, hard drives, off-site data storage, etc.)
      - Be sure that the request for preservation
        - states that no potentially discoverable data should be deleted or modified;
        - states that procedures that may alter (including erase) computer data should be suspended;
        - instructs the recipient to take affirmative steps necessary to prevent deleting, overwriting, defragmenting and compressing, which may erase or alter data; and
        - requests confirmation from your adversary in writing that they agree to comply with your letter.
      - Specifically, be sure to request the preservation of:
        - ***Archived back-up tapes.*** The notice should specify that if archive tapes are rotated, the relevant tapes should be removed from the rotation. If back-ups are made to hard drives, the hard drive should be preserved as well;
        - ***Local hard drives and network drives, floppy disks and other types of removable drives***, such as CD and DVD drives of the people who have knowledge of relevant facts and those who work with them, such as assistants;
        - ***Information on portable computers*** such as laptops and palmtops, as well as home computers if these are used for work purposes;
        - ***Data from computers*** that were used during the relevant time period that are no longer in use, but the drives of which were not erased, or "wiped."

- Also consider:
  - seeking a document preservation order from the court,
  - raising scope of electronic discovery during initial Rule 16 conference,
  - stipulating to waive or enlarge number of depositions, interrogatories and document requests, as provided by local rule, to allow for sufficient preliminary discovery regarding electronic information,
  - specifically emphasizing that electronic information be included as part of the Rule 26 initial disclosures, which explicitly include "data compilations."

▼ **Recognize that electronic discovery is a two-way street** and can be expensive for both sides. Accordingly:

- evaluate at the outset the relative importance and goals of electronic discovery and re-evaluate this issue as the case develops.
- evaluate the risks of exposing your client's electronic information to discovery before aggressively pursuing such discovery from your adversary.
- be prepared to address the same types of requests from your adversary as you serve on them.
- make sure to discuss and agree on electronic discovery strategies with client early in light of the potentially high costs.

Lay the groundwork for successful electronic discovery

- **Prepare discovery plan** at start of case that instructs client regarding:
  - the collection of electronic data,
  - the form of production (electronic and/or hard copy), and
  - the manner of preservation.
- **Once litigation is anticipated**, advise the client not to continue to delete or erase information pursuant to ordinary course of business policies.
  - Consult with client immediately and evaluate the possible need to suspend policies that cause periodic destruction of electronic information.
  - Remember that anticipated, not merely pending, litigation triggers certain obligations regarding retention and preservation of electronic information.
  - **Duty to preserve arises** once party knows or reasonably should know that information is:
    - relevant to anticipated or pending action;
    - reasonably calculated to lead to the discovery of admissible evidence;
    - reasonably likely to be requested during discovery; or
    - the subject of pending discovery request.

- Prior to conducting full-blown electronic discovery, **consider serving initial discovery requests**, such as interrogatories or a Rule 30(b)(6) deposition notice, **to determine nature and extent of adversary's electronic information.**

  - Initial discovery should be directed at developing an understanding of your adversary's computer systems and electronic information storage systems. To this end, it is helpful to obtain:

    - an organizational diagram of the information systems group, to identify those with knowledge and control/access over various aspects of the systems, as well as
    - a schematic overview of the computer systems, to explain the flow of information and the various components of the systems.

  - A Rule 30(b)(6) deposition should be taken of the individual with the greatest knowledge about the computer system. Information that should be elicited at such a deposition includes:

    - a detailed description of the relevant hardware and software,
    - the systems architecture,
    - data storage methods,
    - back-up systems and schedule for rotating back-up media,
    - whether data is password protected,
    - whether data compression is used, and
    - all steps taken in response to the notice to preserve letter.

- **Consider involving forensics expert** early on in the discovery process to provide assistance with such tasks as:

  - framing discovery requests;
  - analyzing electronic data; and
  - searching for and recovering "deleted" documents that may still exist in computer memory.

▼ Conduct electronic discovery in a manner calculated to obtain all required information while avoiding discovery disputes and controlling costs

▼ **In framing discovery requests** for electronic documents:

- make sure that the requests are broad enough to cover the required electronic information;

- however, avoid overly broad document requests that will result in legitimate burden objections from your adversary and protracted and costly motion practice. Consider narrowing requests by providing specific keywords to be used in database searches, a list of directories and servers to be searched, or a list of key personnel or date ranges to limit searches.

- Recognize that electronic information exists in many forms (*e.g.*, E-mail, electronic calendars, handheld personal organizer device entries, computer logs), and specifically identify the types of documents required;

- Request that search for documents encompass archival and back-up copies of electronic information;

- Request electronic copies,

  - including prior versions and/or drafts of word processing documents, E-mail, and other important documentation, so that information which does not appear in hard copy can be reviewed, *e.g.*, "comments" and "bcc" fields.

  - Request electronic files associated with spreadsheets, which will show data entry formulas. This will help you better understand the spreadsheet and allow you to manipulate the data if necessary.

- Request that electronic discovery be provided in specified data formats (*e.g.*, ASCII, Microsoft Word) and physical media (*e.g.*, CD-ROM, diskette) that can be used by your experts or client. If this request is denied, request software needed to view or access the data to be produced.

- Consider requesting ***mirror images*** of hard drives (not merely a printout of the contents or copies of the files).

  - Such a request may be met with objections that the request is overly broad, that the drives in question contain personal and/or confidential information that is not relevant to the case, and that the request is not likely to lead to any admissible evidence.

  - However, because data on the drive changes each time a file is created, saved, deleted, etc., a mirror image must be obtained in order to ensure full preservation of data. Then, the mirror image can be reviewed to determine what is properly discoverable. It should be possible to craft a protective order that ameliorates the objecting party's concerns.

▼ Conduct electronic discovery in a manner calculated to obtain all required information while avoiding discovery disputes and controlling costs

- Request copy of adversary's electronic information retention policy.
- To ensure that you get all pertinent information in connection with E-mail, consider requesting that E-mail be downloaded onto disks without further processing by adversary, or request on-site discovery of E-mail.
  - ▾ E-mail contains valuable information embedded in the electronic version of the document that does not necessarily appear in hard copy form – such as time, revision stamps, names of those with access, and author's name.
  - ▾ Also consider serving subpoenas on third party E-mail providers who may possess back-up copies of E-mail.
- Consider requesting inspection of your adversary's premises and computer equipment. *See* FRCP 34(a)(2) (permits entry "for the purpose of inspection and measuring, surveying . . . testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b)").
  - ▾ Sometimes electronic discovery warrants a visit to the adversary's site. A site visit could be necessary, for example, where the adversary simply does not have the expertise necessary to recover the data from its own systems, or where spoliation of data has become an issue.
  - ▾ Inspection may allow you to uncover deleted files, file and directory information about the dates of revisions, and information regarding who accessed what files and when.
  - ▾ In making such requests, be sensitive to disrupting responding party's business – otherwise, will likely lead to objections.
  - ▾ Consider reasonable ways in which to minimize the burdens to the producing party, such as:
    - – an offer to pay costs of information recovery,
    - – making "mirror image" of hard drive to be utilized for document recovery.
  - ▾ Recognize that case law seems to turn, in part, on whether you can establish a likelihood of discovering the purged information – expert affidavits will be critical to this issue.
  - ▾ Consider hiring a neutral third party computer expert to conduct on-premises electronic media discovery. Expert should not touch adversary's computer, but should instead direct adversary's own employees to perform the search for data. This will help avoid potential claims of spoliation or of damaging systems or data.

▼ Conduct electronic discovery in a manner calculated to obtain all required information while avoiding discovery disputes and controlling costs

- Take steps to ensure that produced data is not altered by adversary.
  - Consider certifying information by using "digital notary" to create unique electronic fingerprint of each file at a particular point in time and saving in a "certificate" file. This allows detection of any subsequent changes to the file.
  - Consider coding produced data so that it is "read-only" and cannot be altered.

- If necessary, enter into **Protective Order** to address concerns related to confidentiality and trade secrets.

- Consider unique issues related to electronic discovery, such as potential obligations to:
  - produce both electronic and hard copy versions of documents,
  - recover or even create electronic versions of computer data,
  - produce proprietary software needed to read electronic data,
  - provide assistance in helping adversary read and understand electronic data,
  - give adversary access to hard drives to allow opponent to attempt to retrieve "deleted" files, and
  - bear the costs in collecting and producing electronic data.

- Consider working with adversary to stipulate to protocol regarding these issues so as to avoid the additional costs associated with protracted discovery disputes.

▼ **In responding to requests for electronic information**, analyze whether you have any legitimate burden objections. Under the applicable case law, the extent of the burden will be the key factor in determining whether objections to requests will survive motions.

- If burden is severe, consider seeking protective order, or to shift costs of production to requesting party. *See* FRCP 26(b)(2) (court can limit discovery if "the burden or expense of the proposed discovery outweighs its likely benefit. . . ."); FRCP 26(c) (protective order can be entered to protect a party from "undue burden or expense").
- Analyze the following factors in evaluating likelihood of shifting costs to requesting party (*see Bills v. Kennecott Corp.*, 108 F.R.D. 459, 464 (D. Utah 1985):
    - ▼ whether the amount of money involved is excessive;
    - ▼ whether the relative expense and burden in obtaining the data is substantially greater for the requesting party than the responding party;
    - ▼ whether the amount of money required to obtain the data would be a substantial burden to the requesting party;
    - ▼ whether the responding party is benefited by the production.
- If discovery disputes are litigated:
    - ▼ come forth with factual proffer (*i.e.*, affidavits) establishing burden;
    - ▼ consider alternatives to requested production that can minimize burden.

▼ E-mail communications may raise questions regarding attorney-client confidentiality and privilege

- ▼ Check judicial decisions and state ethics opinions in jurisdiction at issue to determine treatment of E-mail communications vis-à-vis attorney-client confidentiality.

- ▼ Because there is generally some uncertainty regarding whether Internet communications are privileged, consider:
  - using encryption when sending outgoing E-mails;
  - implementing network security measures (*e.g.*, intrusion detection software);
  - obtaining Protective Order that covers inadvertent disclosure; and/or
  - not using Internet E-mail for confidential communications.

- ▼ At a minimum, send E-mails with privileged and confidential legends to establish that there is no intent to disclose the information to third parties.

- ▼ Do not send drafts to, or otherwise communicate with, experts by E-mail, as this may render the information discoverable.

Computerized litigation support systems raise work product issues in electronic discovery

- To increase the likelihood that a court will find a computerized litigation support system, such as Lotus Notes, protected by the work product doctrine:
  - have attorneys involved in all aspects of setting up the database system;
  - include and interweave work product with non-work product information so that it is difficult to disentangle the work product from the non-work product;
  - do not maintain the system as a mere repository of scanned factual documents or other raw facts;
  - do not include every document in the litigation in the system, but instead have the attorneys select the documents that are imaged and accessible through the system;
  - do not provide your expert access to the system, or allow your expert to rely on the system in connection with his or her opinions, unless you are prepared to produce it to your adversary — if the expert relies on the system, it will likely be discoverable; and
  - do not create the system separate and apart from the litigation context.
- If ordered to produce the database:
  - seek to have the requesting party pay a share of the cost in setting up the database; and
  - seek to limit the production to general, non-work product information about the documents (such as names of senders and recipients).

▼ E-mail can be especially damaging and special practices should be applied

- Encourage clients to set up E-mail policy regarding the creation and retention of E-mail.
  - E-mail system should automatically purge all historic E-mail, consistent with business needs.
  - Retention policy may help in establishing that a particular E-mail message was generated and retained in the ordinary course of business to satisfy the business records exception to the hearsay rule. *See* FRE 803(6) (business records exception to hearsay rule).
- In setting up retention policy, do not retain unnecessary copies of E-mail on back up tapes. This will just subject client to huge discovery burdens in litigation.
- Encourage clients to set up E-mail policy that distinguishes between official and unofficial E-mail.
  - Policy should require employees to treat business E-mail like business memoranda, and
  - distinguish between official and unofficial E-mail.
    - Such a policy will help reduce the risk that unofficial E-mail can be used against client in litigation.
    - Distinguishing between E-mail may also assist client in introducing business E-mail as business records. *See* FRE 803(6).
- Recommend that employees are educated about all E-mail policies to make sure that they are understood and followed.
- Advise client to monitor effectiveness of E-mail policies and procedures and implement steps to enforce them.
- In reviewing E-mail, do not work with the original files. Otherwise, you may alter electronic information, such as last date of access.

▼ Effective electronic discovery often requires expert assistance

▼ Consider involving computer expert early on in the case to:

- assist in framing discovery requests for electronic information, particularly identifying sources of data the other party may not necessarily search unless specifically identified;
- assess what storage/retrieval techniques should be employed to respond to such requests from your adversary and determine the most cost-effective manner of doing so;
- assist in ensuring preservation of discoverable evidence; and
- examine software and storage media to extract relevant evidence and determine whether such data has been erased or corrupted.

Electronic information may raise unique evidentiary issues

- Analyze rules regarding the admissibility of electronic information. The few reported decisions on the subject have held that E-mail is not a business record under FRE 803(6).

- To increase likelihood of E-mail being admitted as business record, implement E-mail retention policy that mandates that only "official" E-mail is retained.

- Conduct Rule 30(b)(6) deposition to lay foundation for admissibility of electronic information.

- Conduct pretrial discovery regarding the design and reliability of the computer systems and of the handling and protection of original data from alteration.

- Focus on chain of custody issues and electronic methods of verifying authenticity of electronic information.

I. General Obligation To Produce Electronic Documents

FRCP 34: specifically applies to “data compilations from which information can be obtained . . . through detection devices into reasonably usable form.”

Anti-Monopoly, Inc v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995) (“today it is black letter law that computerized data is discoverable if relevant.”).

Seattle Audubon Society v. Lyons, 871 F. Supp. 1291 (W.D. Wash. 1994) (ordering production of E-mail).

Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993) (respondent failing to produce properly requested raw computer data is subject to sanctions, even though such data is not available in hard-copy form).

Santiago v. Miles, 121 F.R.D. 636 (W.D.N.Y. 1988) (“A request for raw information in computer banks is proper and the information is obtainable under the discovery rules.”).

Bills v. Kennecott, 108 F.R.D. 459, 462 (D. Utah 1985) (“Computers have become so commonplace that most court battles now involve discovery of some type of computer-stored information.”).

II. Document Retention – Sanctions for Failing to Retain Documents

Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. Ct. 1999) (court sanctioned defendant for recycling back-up tapes by ordering that jury would be instructed that an adverse inference may be drawn from the fact that documents were destroyed and awarding all fees and costs associated with electronic discovery issue).

Proctor & Gamble Co. v. Haugen, 179 F.R.D. 622 (D. Utah 1998) (court fined P&G $10,000 for failing to save its corporate E-mail communications from individuals specifically identified by P&G as having knowledge; refused to give adverse inference instruction).

Lauren Corp. v. Century Geophysical Corp., No. 96CA0554, 1998 Colo. App. LEXIS 12 (Jan. 22, 1998) (court imposed a presumption at trial that party had improperly used software on machines other than those described in the licenses and awarded attorney's fees and costs).

Prudential Ins. Co. of Am. Sales Practice Litig., 169 F.R.D. 598 (D.N.J. 1997) (court imposed sanctions against party, including awarding cost and fees and fining party $1.0 million, for failing to act quickly and efficiently to prevent destruction of electronic data).

Cabinetware Inc. v. Sullivan, 22 U.S.P.Q.2d 1686 (E.D. Cal. 1991) (court ordered default judgment as sanction where party destroyed electronic documents).

Computer Associates Int'l, Inc. v. American Fundware, Inc., 133 F.R.D. 166 (D. Colo. 1990) (in litigation regarding misuse of CA source code, court ordered sanction of default judgment where AF continued its practice of destroying previous versions of source code well after the litigation commenced, including after CA filed motion to compel).

National Assoc. of Radiation Survivors v. Turnage, 115 F.R.D. 543 (N.D. Cal. 1987) (court imposed sanctions, including awarding costs and fees and appointing special master to oversee and monitor discovery, where agency altered and destroyed computer records in the regular course of business).

III. Document Production Issues

A. Can you be required to produce both electronic and hard copy versions of documents?

1. Ordering Production

Anti-Monopoly, Inc v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995) (holding that computerized form of documents were discoverable even if hard copies were produced, and even if producing party had to create electronic version).

In re Air Crash Disaster at Detroit Metropolitan Airport on August 16, 1987, 130 F.R.D. 634, 636 (E.D. Mich. 1989) (ordering party to duplicate and produce computer-readable version of data despite fact that data was produced in hard copy; however, because the computer version did not exist, requesting party was ordered to pay costs associated with the manufacture of computer-readable tape).

Daewoo Electronics Co. v. United States, 650 F. Supp. 1003 (Ct. Int'l Trade 1986) (ordering party to produce computer files in format that was readable to requesting party, and provide assistance as was necessary to enable requesting party to process the data).

National Union Electric Corp. v. Matsushita Electric Industrial Co., 494 F. Supp. 1257 (E.D. Pa. 1980) (ordering plaintiff to create and produce electronic tape of documents even though plaintiff had produced printout of documents).

Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972) (ordering party to produce both computer cards or tapes and printouts of documents).

2. Denying Production

Williams v. Owens-Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) (denying request for production of computer tapes where party already produced hard copies of wage cards: "While using the cards may be more time consuming, difficult and expensive, these reasons, of themselves, do not show that the trial judge abused his discretion in denying appellants the tapes").

B. Are electronic databases protected from discovery?

1. Ordered Protected

Shipes v. Bic Corp., 154 F.R.D. 301, 309 (M.D. Ga. 1994) (in-house legal department computer database, used to manage claims and created in anticipation of litigation, protected from discovery).

2. Ordered Not Protected

Hines v. Widnall, 183 F.R.D. 596, 600 (N.D. Fla. 1998) (ordering production of computer imaged records kept in format that did not contain or reveal any legal theories or mental impressions of attorneys; requesting party not required to pay portion of expenses incurred in creating database, but only the cost of copying the files).

Minnesota v. Philip Morris, Inc., 1995 Minn. App. LEXIS 1602 (Minn. Ct. App. 1995) (ordering production of computerized database that did not reveal impressions, opinions, or theories of counsel).

Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648, 651 (W.D. Ky. 1987) (ordering production of computerized database created from documents produced by party; party ordered to pay fair portion of fees incurred in creating database).

Fautek v. Montgomery Ward & Co., 91 F.R.D. 1980 (N.D. Ill. 1980) (ordering production of electronic database of personnel records where there was no evidence that database contained strategic legal decisions, contingent on requesting party's agreement to pay 50% of compilation costs).

C. Can you be required to recover or even create electronic version of data?

Armstrong v. Executive Office of the President, 821 F. Supp. 761, 773 (D.D.C. 1993) (ordering restoration of back-up tapes of E-mail and threatening fines of $50,000 per day to be doubled in later weeks for failure to comply; sanctions vacated at 1 F.3d 1274 (D.C. Cir. 1993)).

In re Air Crash Disaster at Detroit Metropolitan Airport on August 16, 1987, 130 F.R.D. 634, 636 (E.D. Mich. 1989) (ordering party to manufacture and produce computer-readable tape despite fact that data was produced in hard copy form; requesting party was ordered to pay costs associated with the manufacture of computer-readable tape).

National Union Electric Corp. v. Matsushita Electric Industrial Co., 494 F. Supp. 1257, 1262 - 63 (E.D. Pa. 1980) (ordering party to create a computer readable tape containing information previously produced in hard copy: “the manufacture of a machine-readable copy of a computer disc is in principle no different from the manufacture of a photocopy of a written document. . .”).

D. Can you be required to produce proprietary software needed to read electronic data?

Daewoo Electronic Co., Ltd. v. United States, 650 F. Supp. 1003, 1007 (Ct. Int’l Trade 1986) (ordering production of computerized data with computerized instructions).

Fautek v. Montgomery Ward & Co., 96 F.R.D. 141, 144-46 (N.D. Ill. 1982) (sanctioning party for not producing codes necessary to understand electronic data).

E. Can you be required to provide assistance in helping adversary read and understand electronic files?

Sattar v. Motorola, Inc., 138 F.3d 1164, 1171 (7th Cir. 1998) (ordering party that produced E-mail on tapes to provide additional assistance to enable adversary to read E-mail, including either downloading the E-mail onto a hard-drive, loaning adversary a copy of necessary software, or offering adversary access to computer system).

Daewoo Electronics Co .v. United States, 650 F. Supp. 1003, 1007 (Ct. Int’l Trade 1986) (ordering party to provide assistance as was necessary to enable requesting party to process the electronic data).

F. Can you be required to give adversary access to hard drives to allow opponent to attempt to retrieve "deleted" files?

FRCP 34(a)(2) permits entry "upon other property . . . for the purpose of inspection and measuring, surveying . . . testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b)."

1. Ordering Access

Playboy Enters., Inc. v. Welles, 60 F. Supp.2d 1050 (S.D. Cal. 1999) (where deleted E-mail could be relevant to litigation, court appointed computer expert to create a "mirror image" of defendant's hard drive that would be given to defendant's counsel so as to permit him to print out all recovered E-mail, and review the documents for privilege before production; court also ordered plaintiff to pay the costs of the information recovery).

Lauren Corp. v. Century Geophysical Corp., No. 96CA0554, 1998 Colo. App. LEXIS 12 (Jan. 22, 1998) (court ordered inspection of computers to show software was used on authorized computers).

Easley, McCaleb & Assoc., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994) (deleted files from defendant's computer hard drive are discoverable, and ordering that plaintiff's expert must be allowed to retrieve all recoverable files).

2. Denying Access

Fennell v. First Step Designs Ltd., 83 F.3d 526, 532-34 (1st Cir. 1996) (refusing to provide plaintiff access to defendant's hard drive where opposing party established burden — including concerns about confidentiality, privilege and cost — and where plaintiff failed to show a "particularized likelihood of discovering appropriate information.")

Strasser v. Yalamanchi, 669 So.2d 1142, 1145-46 (Fla. Ct. App. 1996) (quashing court order that permitted access to party's computer where requesting party did not show that it was likely to be able to retrieve purged documents, and where there was no finding that such access was the least intrusive means to obtain the information).

Lawyers Title Ins. Cp. v. U.S.F.&G., 122 F.R.D. 567 (N.D. Cal. 1988) (refusing to allow wholesale discovery of computer system without a showing that such discovery would lead to evidence that had not already been produced).

IV. Court Ordered On-Site Discovery

Gates Rubber Co. v. Bando Chemical Industries Ltd., 167 F.R.D. 90 (D. Colo. 1996) (court entered a site inspection order directing that no records be destroyed and permitted expedited discovery of computerized files).

Quotron Systems, Inc. v. Automatic Data Processing, Inc., 141 F.R.D. 37 (S.D.N.Y. 1992) (in copyright infringement and trade misappropriation case, court granted ex parte order allowing plaintiff to raid defendant's premises to prevent destruction of software before discovery could take place).

V. Who should bear the costs of electronic discovery?

FRCP 26(b)(2) (court can limit discovery if “the burden or expense of the proposed discovery outweighs its likely benefit...”);

FRCP 26(c) (protective order can be entered to protect a party from “undue burden or expense”).

Playboy Enters., Inc. v. Welles, 60 F. Supp.2d 1050 (S.D. Cal. 1999) (ordering requesting party to pay the costs of recovering deleted E-mail).

Hines v. Widnall, 183 F.R.D. 596, 600 (N.D. Fla. 1998) (ordering production of computer imaged records and not requiring requesting party to pay portion of expenses incurred in creating database, but only the cost of copying the files).

In re Brand Name Prescription Drugs Antitrust Litigation, No. 94 Civ. 897, 1995 U.S. Dist. LEXIS 8281 (N.D. Ill. June 13, 1995) (compelling production of E-mail and requiring requesting party to pay $.21 per page fee for each page selected for copying).

In re Air Crash Disaster at Detroit Metropolitan Airport on August 16, 1987, 130 F.R.D. 634, 636 (E.D. Mich. 1989) (ordering party to duplicate and produce computer-readable version of data and ordering requesting party to pay costs associated with the manufacture of computer-readable tape).

Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648, 651 (W.D. Ky. 1987) (ordering production of computerized database created from documents produced by party and ordering party to pay fair portion of fees incurred in creating database).

Bills v. Kennecott Corp., 108 F.R.D. 459, 464 (D. Utah 1985) (in determining whether to shift costs to the requesting party, court should consider (1) whether the amount of money involved is excessive; (2) whether the relative expense and burden in obtaining the data is substantially greater for the requesting party than the responding party; (3) whether the amount of money required to obtain the data would be a substantial burden to the requesting party; (4) whether the responding party is benefited by the production).

Dunn v. Midwestern Indemnity, 88 F.R.D. 191 (S.D. Ohio 1980) (defendant entitled to hearing on whether discovery request for computer records was unduly burdensome or expensive).

Fautek v. Montgomery Ward & Co., 91 F.R.D. 1980 (N.D. Ill. 1980) (ordering production of electronic database of personnel records contingent on requesting party’s agreement to pay 50% of compilation costs).

VI. Attorney-Client Privilege Issues

1. Attorney-client privilege covers E-mail transmissions

International Marine Carriers, Inc. v. United States, 1997 WL 160371 (S.D.N.Y. April 4, 1997), at *3.

Heidelberg Harris, Inc. v. Mitsubishi Heavy Industries Ltd., 1996 WL 732522 (N.D. Ill. Dec. 18, 1996), at *7.

National Employment Serv. Corp. v. Liberty Mutual Ins. Co., 1994 WL 878920 (Mass. Super. Ct. Dec. 12, 1994), at *3.

2. Attorney-Client privilege does not cover transmission

United States v. Mathias, 96 F.3d 1577, 1583 (11th Cir. 1996) (cordless telephone conversation with attorney not protected because caller had no reasonable expectation of privacy).

VII. Admissibility of E-Mail

FRE 803(6) provides that a "data compilation" "made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the . . . data compilation" is excluded by the hearsay rule.

United States v. Ferber, 966 F. Supp. 90, 99 (D. Mass. 1997) (E-mail not business record because "under no business duty to make and maintain these E-mail messages").

Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (E-mail not business record because "E-mail is far less of a systematic business activity than a monthly inventory printout").

See also United States v. Catabran, 836 F.2d 453, 457 - 58 (9th Cir.1988) (computer printouts of general ledger properly admitted under business records exception to the hearsay rule).

IX. Admissibility of Other Electronic Documents

United States v. Jackson, 2000 WL 340784 (7th Cir. 2000), at *4 (web site postings are not business records of internet service provider and also lack authenticity).

Handling electronic discovery requires some understanding of basic computer terms and issues. In evaluating discovery requests and responses and deposing technical personnel, at least a basic understanding of such terms and issues is essential. Set forth below is an "executive summary" of some of the most basic and most important terms and issues relevant to electronic discovery.

▼ "Deleted" Files

Files that have been "deleted" may not be physically erased. Rather, the space occupied by such files is merely marked as available for reuse. Until the space is used for either a new file or portions thereof, the deleted file is not altered. When the space is used, the magnetic image that is the deleted file is changed. If the deleted file is not completely overwritten, portions may be retrievable, *e.g.*, if the user saves a smaller file in the space allocated to a deleted larger file.

▼ Computer Memory

Memory is the location from which the computer's microprocessor retrieves instructions and data. The microprocessor, sometimes referred to as a "logic chip," is the part of the computer that carries out calculations according to instructions it receives. There are several different kinds of computer memory.

- **RAM**

  When people refer to computer memory, they are sometimes referring to random access memory, or RAM. During normal operation, RAM generally includes portions of the operating system and whatever programs and data are then in use by the computer. The operating

- **RAM (cont'd)**

  system, or OS, is a program that essentially acts as the "manager" for the rest of the programs on the computer. These other programs are known as "applications." Examples of operating systems are Windows 98 and UNIX. Examples of applications are word processors, database programs, Web browsers and Lotus Notes.[1] RAM resides on microchips placed near the microprocessor and can be accessed more quickly than other forms of memory. Information that is in RAM resides there only while the computer is on. RAM may be analogized to a person's short-term memory. There is a limit to how much information can be held for immediate use at any particular time. Sometimes short-term memory needs to be refreshed with information normally stored in long-term memory. When RAM needs refreshing information, the microprocessor has to retrieve information it needs from the hard disk, which is like a person's long-term memory. This slows the operation of the computer. The greater the available RAM, the faster the operation of the computer.

- **ROM**

  In contrast to RAM, read-only memory (ROM) stores data regardless of whether the computer is on. ROM generally can be read, but not written to. ROM allows the computer to "boot up" when it is turned on, by enabling the operating system to be loaded into RAM.

- **Cache**

  Another kind of computer memory is what is called cache. Cache is a term used to refer to various different kinds of temporary storage. In computer memory, cache is a temporary storage location that can be accessed quickly and is used for frequently used information. Cache

[1] Lotus Notes is an example of a type of application called groupware. Groupware is a type of program that, among other things, allows people to work together even though they are not physically located in the same place. Groupware users can share calendars, databases, and other information. Another popular Groupware program is Microsoft Exchange.

- **Cache (cont'd)**

  is also referred to in connection with storage on remote, network (such as Internet) computers; for example, where Web pages are stored on cache servers to allow quicker access than if the user had to retrieve the pages from the computer originating the page.

Storage Media

Data that is not immediately needed in RAM is stored in a variety of physical media. Familiar storage media include hard disks, diskettes, CD-ROMS, DVDs (Digital Versatile Disks) and tapes. Hard drives, diskettes and various types of magnetic tapes are known as "magnetic" media, because of the way they store information. The term "diskette" usually refers to 3.5-inch hard-cased magnetic diskettes often called "floppy disks" or "floppies." Optical media, which uses laser beams to mark the surface of the disk, includes various forms of CDs (ROM, R, RW), DVDs and other laser disks. There is another category called magneto-optical, or MO, media. MO diskettes can hold up to several gigabytes of data, in contrast to floppy disks, which store up to 1.44 megabytes.

- **Hard Disk**

  A hard disk is a storage medium that is part of what is referred to as the disk drive or hard drive. The hard disk is actually a stack of disks on which data is recorded. Data is written to, or read from, the disks as they spin. Hard disks typically contain a relatively large amount of storage space, usually measured in gigabytes, or billions of bytes, whereas RAM data is measured in megabytes, or millions of bytes. A byte is a unit of information (most computers use a byte of information for a character like a letter or number). Bytes are made up of 8 smaller units called bits, which is either a 0 or 1.

- **Tape Drives**

  Tape drives are used for backing up large amounts of data, typically for large business systems. These drives can provide an important source of data since they can provide a snapshot of a business' systems on any given day. Examples of some common tape formats are digital linear tape (DLT) and digital data storage (DDS).

- **Zip Drives**

  Zip drives are disk drives that can hold as much data as 70 floppy disks. Zip drives are commonly used to back up and archive information on personal computers, such as hard drive contents or old e-mails, but are also used to store large amounts of infrequently used information, to exchange large amounts of information with others, or to keep personal and confidential information separate from the hard drive.

Organization and Format of Computerized Information

- **Files**

  Computerized data is segregated into files. In computer parlance, a file is a collection of information that can be manipulated as a single entity. For example, it can be moved. Files are assigned unique names within organizational hierarchies, which may be called directories, folders or catalogs, depending on the operating system. Commonly, files are given a particular suffix that denotes the file format. For example, a Microsoft Word document has a ".doc" suffix.

- **File Allocation Tables and Fragmentation**

  The operating system maintains a map of the hard disk called a File Allocation Table, or FAT. The hard disk is organized into "clusters" and "sectors." Files are allocated to clusters and sectors by the FAT. As additional files are created, revised, copied and/or deleted, the operating system may allocate a file to unused clusters that are not contiguous. This is called fragmentation. In order to permit files to be read, the information that comprises files must be gathered from the various clusters on which the information is stored and assembled as a single file. A process called defragmentation re-arranges the portions of fragmented files into sequential order on contiguous clusters, which makes it easier for the computer to gather files.

- **Databases**

  Information can be collected in a database, which is a term used to refer to any organized collection of data. There are various types of computerized databases. The most common type of database, the relational databases, defines data so as to permit the reorganization and access of data in a variety of different ways. Relational databases consist of a set of tables, also called relations. For example, a database for keeping track of business orders might have a table with columns for customer contact information and another table with columns containing order information.

- **Databases (cont'd)**

  Programs can be written to "query" databases to obtain specific information. This is commonly achieved using the structured query language, or SQL. An example of a query using the example database given above would be a query for a report on all customers in a certain region who had ordered certain products.

- **Compression**

  In order to save space in computer memory, files are sometimes compressed. Compression involves the removal of information that is considered superfluous. For example, programs downloaded from the Internet are often packaged, or "zipped," into a "zip" file so they can be transmitted more quickly. Once they have been downloaded, the user "unzips" the file to install the program. Audio files are commonly compressed into a file format known as .mp3.

- **Data Formats**

  Data is maintained in certain common formats so that it can be used by various programs, which may only work with data in a particular format. There are bitmap (for graphics and audio), text and numeric data (*e.g.*, for spreadsheets) formats. The most common format for text files is ASCII (American Standard Code for Information Interchange). Each character in ASCII format is represented by a string of seven 0's or 1's. ASCII is used by UNIX and DOS-based operating systems (including Windows, however, Windows NT uses a format called Unicode). Certain IBM computers use a proprietary format called EBCDIC. While programs exist and can be written to facilitate the conversion of file formats, for example, from EBCDIC to ASCII, conversion can sometimes be a difficult and costly exercise.

▼ Networks

A network is a series of connected points, or "nodes." Networks can be connected to other networks. Networks are described in different ways. They can be described by their configuration (*e.g*., bus, star and ring), by the geographical space they cover (*e.g*., local area networks, wide area networks), by type of data transmission technology (*e.g*., TCP/IP), by type of signal carried (*e.g*., voice or data), by access to the network (*e.g*., public or private), by connection type (*e.g*., dial-up or switched), or by type of link (*e.g*., optical fiber or coaxial cable).

A local area network, or LAN, consists of a group of connected computers which share access to a more powerful computer (called a server) or processor, usually within the same office building (but not necessarily). The server generally contains applications and data that are shared by the users of the LAN.

An intranet is a private network, like the one connecting the computers of a law firm. Many LANs can be linked to form an intranet. When an intranet is shared with outside people or entities, it forms an extranet.

▼ The Four Categories of Digital Data

- **Active**

  Active data is information that is "dynamic," *i.e*., created, saved, retrieved and modified daily. Such data is created through the use of familiar applications such as word processors, spreadsheets, databases, e-mail and calendaring programs, and is generally readily accessible and available.

- **Inactive**

  Inactive data is static, not used daily and stored on disks. It includes historical files that may have been created years ago, including files such as those created by an automatic back-up feature incorporated into many familiar applications. For example, a program automatically may create a copy of a file in use, known as a "working file," to a user-defined directory (*e.g*., c: mybackups), within a specified time period (*e.g*., every ten minutes). Another example is where a copy of the original file is created whenever the original is opened, so that if you work off the old file and forget to save the document with a new name, the original is not lost.

  The popular word processing program WordPerfect has "undo" and "redo" features, which can save the last *n* items the user deleted from a document. This information is saved when the user saves the document to a disk. (This feature does not exist in Microsoft Word.) Other programs provide facilities for creating and tracking file versions. Reviewing the various versions may reveal significant information regarding the evolution of the document, *e.g*., what portions were originally present but later deleted. Still other information may reside in the electronic file without appearing in the hard copy. For example, some word processing programs have a "comments" feature which permit the annotation of a document without such annotation appearing in the hard copy.

▼ The Four Categories of Digital Data (cont'd)

- **Archival**

  This is electronic data which has been "backed up," or copied for safe keeping. Most networks are backed-up according to a schedule. "Incremental" back-ups, which back up all information from the time of the last back-up forward, are often created daily, with one copy being stored off-site. The media used to create these copies are then rotated periodically. Full network back-ups are usually made less frequently, for example on a weekly basis, during non-business hours. Again, copies are normally stored off-site. Back-ups are often limited to the data files created through the use of various applications, and do not include the applications files themselves. Note that data that has been deleted from a local or network drive may well exist in archived back-up. Because of the way back-up data is stored, it often cannot be accessed unless it is first restored to a hard disk.

- **Residual**

  This data includes data residing in the "buffer" memories of various hardware[2] such as printers and facsimile machines, as well as deleted files that have not been fully overwritten and may still be retrieved.

[2] The "physical" reality of information technology is referred to as hardware, as opposed to software, which refers to computer programs. Examples of hardware are the computer monitor, keyboard, mouse, printers, etc.

Appendix C: Selected Bibliography

1. Ian C. Ballon, *How Companies Can Reduce the Costs and Risks Associated With Electronic Discovery*, 15 Computer Law 8 (1998).
2. Steven M. Bauer, *Symposium: Lawyers on Line: Discovery, Privilege And The Prudent Practitioner*, 3 B.U.J. Sci. & Tech., L. 5 (1997).
3. David S. Bennahum, *Daemon Seed, Old E-mail Never Dies*, Wired, May 1999.
4. Kenneth R. Berman and David A. Brown, *Practical Issues in Framing And Responding To Discovery Requests For Electronic Information*, A.B.A. — Legal Educ. Natl Inst. (1998).
5. Committee on Federal Courts, *Discovery Of Electronic Evidence: Considerations for Practitioners And Clients*, The Record, September/October 1998, Vol. 53, No.5.
6. Kevin Eng, *Legal Update: Spoliation of Electronic Evidence*, 5 B.U.J. Sci. & Tech., L. 13 (1999).
7. *Federal Government Guidelines For Searching And Seizing Computers*, United States Dept. of Justice, Crim. Div., Office of Professional Dev. & Training, July 1994.
8. *Supplement To Federal Government Guidelines For Searching And Seizing Computers*, United States Dept. of Justice, Crim. Div., Office of Professional Dev. & Training, October 1997.
9. Joan E. Feldman and Rodger I. Kohn, *The Essentials Of Computer Discovery*, 1999 Computer Forensics Inc., at 51.
10. Jay E. Grenig, *Electronic Discovery: Making Your Opponent's Computer A Vital Part of Your Legal Team*, 21 Am. J. Trial Advoc. 293 (1997).
11. Tom Groenfeldt, *Net Returns: Send No Evil*, The Industry Standard, March 13, 2000 at 304.
12. Harry M. Gruber, *E-mail: The Attorney-Client Privilege Applied*, 66 Geo. Wash. L. Rev. 624 (1998).
13. David M. Hoffmeister, *Protection Of A Computer Litigation Support System*, 11 ACCA Docket 60 (1993).
14. Gregory S. Johnson, *Symposium: Emerging Technologies And The Law: A Practitioner's Overview of Digital Discovery*, 33 Gonz. L. Rev. 347 (1997-98).
15. Andrew Johnson-Laird, *Smoking Guns And Spinning Disks*, The Computer Lawyer, August, 1994.
16. Joseph L. Kashi, *How To Conduct On-Premises Discovery of Computer Records*, 24 Law Prac. Mgmt. 26 (1998).
17. Ralph T. King, Jr., *Mysteries Of The "Dark Files"*, Reprinted From The Wall Street Journal, 1999 Dow Jones & Co., July 15, 1999.
18. Mark D. Robbins, *Computers And The Discovery Of Evidence - A New Dimension To Civil Procedure*, 17 J. Marshall J. Computer & Info. L. 411 (1999).
19. Joseph S. Solovy and Robert L. Byman, *Digital Discovery*, Nat'l L. J., Dec. 27, 1999, at A16.
20. Ralph A. Taylor, *Lawyers May Send Client Confidences By E-mail*, 23 Litig. News 5 (1998).