THE DIGITAL LOOKING GLASS:

DISCOVERY, RETENTION and ADMISSIBILITY

of

ELECTRONIC EVIDENCE

An Overview

Presented to:

American Bar Association
Section of Litigation

Presented by:

Mark K. Slater[1/]
Sonnenschein Nath & Rosenthal
San Francisco, California

July 9, 2000
New York City

1/ The author wishes to thank Jonathan Hersey of Sonnenschein Nath & Rosenthal and the author's former colleagues at Sheppard, Mullin, Richter & Hampton LLP for their very valuable contribution in preparing these materials.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

MISCELLANEOUS

OUTLINE

I. WHY ELECTRONIC EVIDENCE?

1. 30% of company information never makes it to print. S. Silvernail, *Electronic Evidence: Discovery in the Computer Age*, 58 Ala. Law. 176, 177 (May, 1977).

2. What is Electronic Evidence?

   a. Unfiltered, Unabridged, Uncensored . . . E-Mail. E-mail can reflect the way people thought and communicated at the time, without coaching from counsel, or without thinking about ... anything.

   - *Siemens v. Atlantic*

   (E-mail from ARCO Solar Executive discovered in suit over sale of ARCO Solar to Siemens.) *See* H. McNeil and R. Kort, *Discovery of E-mail and Other Computerized Information*, Ariz. Att'y at 16 (April 31, 1995) citing *Siemens Solar Industries, Inc. v. Atlantic Richfield Co.*, U.S. Dist. LEXIS 3026 (S.D. N.Y. 1994).

   - the Company President

   (From president of defendant to its head of human resources; case settled.) See M. Lavelle, *Digital Information Boom Worries Corporate Counsel,* Nat'l L. J. at B1 (May 30, 1994).

   - Rodney King Trial

   (E-mail from defendant police officer Lawrence Powell, sent after beating of Rodney King.) See 415 PLI/Pat 277, 282 (1995).

   - Microsoft Trial — almost 3000 E-mail trial exhibits
   - Will people treat E-mail as they do other written correspondence?
   - San Francisco Chronicle Antitrust case – E-mail shows Hearst Corporation executives may have

known about editorial favors to S.F. mayor Willie Brown

b. Digitized pictures and audio — JPEG, MPEG, GIF files

c. Spreadsheet, database programs.

Spreadsheets and databases are often how the company measures the market, its competitors and itself. But the data may not be as understandable or compelling when not in its program format.

d. Drafts, versions.

A series of draft contracts and letters can show how a contract developed and what the parties intended. Internal memoranda and draft correspondence may exist only in electronic form. Backup tapes often hold electronic documents that have ceased to exist in other forms.

Voluminous records.

Financial and sales information, including payroll records, G&A ledgers, financial statements, etc. Discovery of the electronic data itself may not suffice. For companies with sophisticated custom accounting software, a copy of the software and the assistance of the company personnel responsible for administering or designing it may be required to fully access the information it contains.

e. Voice Mail — Too ephemeral to request?

f. Videotape.

g. Electronic Eavesdropping

(Sales manager fired for harassing statement while viewing web site photo of co-worker in bikini top at company picnic - whistle and comment secretly recorded by his own personal computer; $30,000,000 discrimination suit pending). See P. Somerson, PC Microphones Used to Record Employee Conversations, *PC/Computing* at 89 (April 1, 1999).

Virtually every computer made after March of 1996 has a concealed microphone. Voice-activated Speech Collection Port ("SCP") software installed by IT departments can record user conversations within 5 feet of a computer and send recordings to a remote server.

II. DISCOVERY OF ELECTRONIC PROGRAMS AND DATA

"If you give me six lines written by the most honest man, I will find something in them to hang him" — Cardinal Richelieu

A. Federal Rule.

1. It is "axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure . . . ." *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 461 (C.D. Utah 1985); *Manual For Complex Litigation, 3d*, § 21.446 (1995). Further, "a party requesting such information should be granted access to the electronic files themselves as long as sufficient safeguards are provided." Advisory Committee Note to Fed. R. Civ. P. 34(a)(1) (1970 Amendment) (discussing situations in which "the discovering party needs to check the electronic source itself"). *Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F.Supp. 1257, 1267 (E.D. Pa. 1980) aff'd in part and rev'd on other grounds, 723 F.2d 238 (3rd Cir. 1983), rev'd on other grounds 475 U.S. 574 (1986) (party entitled to computer data in form usable by adversary's computers).

2. Courts increasingly interpret Fed. R. Civ. P. 34 to require production of electronic data even where the propounding party could re-create the database or other electronic document from hard copy, guided by Fed. R. Civ. P. 1's mandate of a "just, speedy, and inexpensive determination of every action." *Id.* In *Williams v. E.I. du Pont de Nemours & Co.*, 119 F.R.D. 648 (W.D. Ky. 1987), the court ordered the plaintiff to produce its expert's database, which used information produced originally by the defendant. *Anti-Monopoly, Inc. v. Hasbro*, 1995 WL 649934 (S.D.N.Y. 1995).

B. California Rule. Evidence Code § 250 (defining "writing") is interpreted to include information stored electronically. *Aguimatang v. California State Lottery,* 234 Cal.App. 3d 769, 797 (1991).

C. Propounding and Responding To Electronic Discovery.

1. Cost, scope and reciprocity considerations in serving electronic discovery; defining the playing field.

Be careful of what you ask for....

2. Mechanics

a. Where does data reside? Networks, microcomputers, laptop/portable computers, file servers, application servers, workstations, minicomputers, mainframes, PDAs, home/remote computers, Internet/mail servers.

b. In house or outside computer experts can often extract "deleted" files from computers. They can tell you how to ask for, and help find, what you're looking for. They cost money.

- Your Information Technology Department may advise on drafting discovery.

- Ontrack Evidence - Reputable outside consultants (See Tab 1).

c. Why delete doesn't mean delete.

- a "delete" command simply causes the computer to rename files so that they are hidden. Files are not actually deleted until they are overwritten by other data.

3. Discovery Forms

a. Including electronic evidence in the definition of "document" (Document Requests, Tab 2).

b. Interrogatories directed to the electronic infrastructure (Interrogatories, Tab 3).

c. Deposing the adversary's IT persons (Deposition Outline, Tab 4).

d. Inspecting the computer system. (Inspection Request, Tab 5)

(1) Code Civ. Proc. § 2031
(2) Federal Rule Civil Procedure 34

e. Upon engagement, advise the client to preserve electronic evidence (form letter re retention of evidence, Tab 6).

f. Preservation letters – careful work or stones in glass houses? (form letter to opposing counsel, with stipulation, Tab 7).

g. Preservation stipulations and orders — Injunction under Code Civ. Proc. § 525 requiring parties to preserve and retain files relevant to the action.

h. Sample Motion To Compel (Tab 8)

i. Searching the Web — fast and free.

4. Hard Drive Copying - Must Create A Reliable "Mirror Image")

a. Use software designed to create reliable evidentiary copies. The software does not write to the drive being analyzed and creates an audit trail to document the creation of and later access to the evidentiary image copy. The mirror image copy process (also called a sector by sector copy) differs from that of a commercial software backup because it creates a copy of the entire disk, thereby copying all data, including data and software files and fragments thereof. This way, deleted files can be recovered.

b. The actual process is simple. A hard disk drive containing a removable disk such as a Jaz® drive is connected to the target computer. The computer then is booted up from the disk drive, which also executes the image capture software. No software is loaded onto the target computer. The evidentiary image copy is stored on the removable disk, which in turn is analyzed by a diagnostic computer for review. The evidentiary, tamper-proof disk copy can be sealed and held by a neutral party. Betty Ann Olmsted, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, 763 Def. Couns. J. 523 (October 1996) (discussing e-mail retention and discovery issues).

5. Requesting/Challenging the inspection.

a. Upon a showing that the electronic discovery is reasonably calculated to lead to admissible evidence, most courts will permit it. *Lawyers Title Ins. Corp. v. United States Fidelity & Guaranty Co.*, 122 F.R.D. 567, 570 (N.D. Cal. 1988).

b. *Inspection denied: Fennell v. First Step Designs,* 83 F.3d 526, 532-33 (1st Cir. 1996) (upholding trial court's determination that mirror image of defendant's hard drive not discoverable because plaintiff set forth no plausible basis for believing that specified facts exist).

c. *Inspection granted: Playboy Enterprises, Inc. v. Welles* 1999 WL 669114 (S.D. Cal. August 2, 1999.) Trademark action; where requested e-mails had been deleted, examination and image copying of hard drive permitted subject to showing that deleted e-mails could be recovered from hard drive. In this case, the defendant set up plaintiff's electronic evidence motion by filing a declaration that her practice was to read and delete email messages.

6. Cost of Compilation /Production (Who's Buying?).

a. Federal: Rule 34 provides for production of computerized information in "reasonably usable" form.

(1) *In re Brand Name Prescription Drug Antitrust Litigation*, 94-C-987, M.D.L. 997 (N.D. Ill. 1995) 1995 U.S. Dist. LEXIS 8281 at *6 (defendant bears cost of producing 30 million pages of e-mail messages because plaintiff has no control over defendant's record keeping scheme); *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 463-64 (C.D. Utah 1985) (disclosing party in best position to pay for information retrieval from own record-keeping system).

(2) Requesting party pays: *Anti-Monopoly Inc. v. Hasbro, Inc.*, 1995 W.L. 649934 (S.D. N.Y. 1995); *In re Air Crash Disaster at Detroit Metropolitan Airport*, 130 F.R.D. 634, 636 (E.D. Mich. 1989); *Williams v. E.I. du Pont de Nemours & Co.*, 119 F.R.D. 648 651 (W.D. Ky. 1987).

b. Data Compilation

(1) Where data must be compiled, rather than simply retrieved, and a party would make such a compilation prior to trial, the discovering party may share in the cost of production. However, simply making data available or producing it in "reasonably usable form," is a cost most often borne by the responding party. But see *PHE, Inc. v. Department of Justice*, 139 F.R.D. 249, 257 (D.D.C. 1991) (court overruled burden objection and ordered production of computerized files even though no program existed to access them).

(2) Courts broadly apply rule 34 in a way that allocates and equalizes cost, and which imposes requirements for translating the data in question. *Manual for Complex Litigation*, § 21.446 at 85 (1977). In *National Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F.Supp. 1257, 1263 (E.D. Pa. 1980), the court held that "while printout might be 'reasonably usable' within the meaning of Rule 34, the production of a party's data in a form is directly readable by the adverse party's computers is the preferred alternative." The defendant, the court noted, should not be forced to recreate a computer record from the paper printout supplied by plaintiff. *Id. See also, In re Air Crash Disaster*, 130 F.R.D. 634, 636 (E.D. Mich. 1989) (court required production of electronic data because re-creation of program from hard copy would involve unnecessary costs and delays); but see *Williams v. Owens-Illinois, Inc.*, 665 F.2d 918, 933 (9th Cir. 1982) (production of computer tapes is unnecessary because all information already produced in hard copy)

c. California: Typically, responding party storing must bear cost of search and retrieval; but *requesting* party will bear the cost of translating data compilations into "reasonably useable form." CCP § 2031(f)(1).

7. Discovery Responses - The Fundamental Rules Apply As Bytes Go By.

a. Protective Orders.

(1) Fed. R. Civ. P. 26(c).

(2) "For good cause . . . a court may make an order protecting a responding party from unwarranted annoyance, embarrassment, or oppression, or undue burden and expense..." Code Civ. Proc. §§ 2030, Subd. (e), 2031, Subd. (e), 2033, Subd. (e).

b. Trade Secret, Privacy, Work-product doctrine and Attorney-client privilege.

c. Privilege and waiver: *Genentech v. ITC* 122 F.3d 1409 (Fed. Cir. 1997) (privileged files produced among 12,000 pages of electronic documents: held, waiver).

d. Equally-available objection. *O'Meara v. Internal Revenue Service*, (N.D. Ill. 1997) 1997 WL 312054 (plaintiff charged with costs of retrieving data available in on-line database).

III. RETENTION OF ELECTRONIC DATA — FINDING THE BALANCE

A. The Client's Electronic Data Retention Policy.

1. What Policy?

Lack of policy may cause unanticipated destruction of favorable evidence, and may hurt client credibility in the eyes of court/jury.

2. How [not] to Create One.

a. Being [in]flexible after litigation is threatened or commenced.

b. What are the storage demands.

c. Some systems automatically delete/overwrite e-mail.

d. Lawyers and IT persons can work together.

e. System changeovers.

f. Audits

g. See sample document retention policies and guidelines (Tab 9). See also *Document Retention Programs For Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 Iowa J. Corp. L. 417 (Winter 1999).

3. Penalties: Where retention policy found inadequate (or worse) by court.

- *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 485-86 (S.D. Fla. 1984). Defendant destroyed documents years before to avoid production in anticipated litigation; sanctioned millions.

- *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D. Cal. 1987) (court imposed sanctions where agency altered and destroyed computer records in regular course of business).

- If the company has any reason to think that information will be pertinent to litigation, it should retain the data. *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988) (reasonableness of retention policy determined by, among other things, knowledge as to whether documents would become material at some future time).

4. California: *Willard v. Caterpillar, Inc.* 40 Cal.4th 892, 921 (1995). ("Good faith disposal pursuant to consistent, reasonable document retention policy could justify failure to produce documents in discovery.").

B. When Litigation is Commenced or Threatened.

1. Destruction must cease. *General Nutrition Corp v. Wm T. Thompson Co.*, 593 F.Supp. 1443 (C.D. Cal. 1984) (default entered for destruction of documents).

2. The duty to preserve evidence extends to both pre-litigation, regular business conduct and post-litigation activity.

3. The Specter of Spoliation — penalty ranges from monetary sanctions to default judgment.

- *Proctor & Gamble v. Haugen,* 179 F.R.D. 622 (D. Utah 1998) ($10,000 sanction for failure to preserve e-mail of persons identified by responding party as having knowledge).

- *Jankins v. TDC Management Corporation*, 21 F.3d 436, 444-445 (D.C. Cir. 1994) (defendant failed to turn over financial records, tax returns, and computer disks, resulting in court order excluding certain evidence and imposing sanctions for attorney's fees and expenses related to compelling discovery of $70,699.56 for failure to obey discovery orders).

- *Thompson Co. v. General Nutrition Corp., Inc.*, 593 F.Supp. 1443, 1455 (C.D. Cal. 1984).

- *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (appellate court upheld default judgment sanction against insurance company for failure to produce relevant electronic data in accordance with a former broker's general document requests).

- *Computer Assocs. Int'l v. American Fundware, Inc.*, 133 F.R.D. 166, 168-170 (D. Colo. 1990); copyright infringement case concerning source code; settlement discussions fail; litigation ensues. Defendant continued to revise (overwrite) the code prior to litigation, retaining only the most current version, per industry practice. Court entered sanction of default judgment against the defendant for failing to preserve evidence once it knew relevance of old source code to plaintiff's claims.

- *Skeete v. McKinsey & Co., Inc.* 1993 WL 256659 (S.D.N.Y. 1993) (pre-existing discovery order under F.R.C.P. 37 not prerequisite to sanctions).

- In *Linnen v. A.H. Robbins Co., Inc.*, 1999 WL 462015 (Mass.Super. 1999), a defendant purged back-up E-mail archive tapes after litigation began and after receiving discovery requests. The court denied monetary sanctions as inappropriate for a violation of its "short lived" *ex parte* Order to Preserve Evidence, although the court noted that the violation was nonetheless "serious." The court granted plaintiff's request for a jury instruction containing a "spoilation inference" against the defendant (jury may infer party who destroyed potentially relevant evidence did so "out of a realization that the evidence was unfavorable." *Id.* at 11. Court denied evidence preclusion sanctions as speculative because the plaintiff had no proof as to the content of the deleted files. The court did award fees and costs to the plaintiff, as well as fees and costs related to the additional discovery needed to investigate the deleted files. *Id.*

- *Lexis-Nexis v. Beer*, 41 F. Supp. 2d 950 (D. Minn. 1999). Lexis-Nexis brought suit and obtained a TRO against a former employee accused of misappropriating proprietary software and e-mails from Lexis-Nexis. After the TRO hearing, during which the Court ordered the former employee to delete all Lexis-Nexis material from the employee's new laptop computer, the parties engaged in expedited discovery. Lexis-Nexis had the new laptop analyzed by its own forensic computer expert. In checking to be certain that the former employee had deleted the files, the fornsic expert identified deleted files that the defendant had previously not admitted to have taken from Lexis-Nexis. In violation of the Court's order, other files were not deleted. Lexis-Nexis brought a motion for sanctions. The Court denied the motion as to Lexis-Nexis' spoliation claim that the former employee

had purposefully "destroyed" evidence and prejudiced Lexis-Nexis' case. On the other hand, the Court granted the motion based on its finding that the employee's actions "set off a high-tech wild goose chase that ... needlessly multiplied the time and expense of this litigation." *Id.* at 956.

IV. ADMISSIBILITY OF ELECTRONIC EVIDENCE

Let's [not] *Give Them Something To Talk About* — Bonnie Raitt

A. Electronic documents may be discoverable, but not admissible.

1. Whether e-mail satisfies the business records exception to the hearsay rule, or some other exception, will usually be a fact- intensive analysis involving the nature of the e-mail system used, the purpose of that system, the reason the particular e-mail at issue was sent, and the other circumstances surrounding the e-mail.

2. *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993) (Government e-mail is a record as defined by the Federal Records Act, and Government must provide access to electronic data in addition to hard copy printouts of e-mail messages).

B. Authentication in Federal Courts: Fed. R. Evid. 901.

1. "[S]atisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

a. Generally refers to the requirement that, prior to being admitted, authorship or other connection to a writing must be shown.

b. Process or system put into evidence must be authenticated through "describing . . . [the] system used to produce a result and showing that the process or system produces an accurate result." Fed.R. Evid. 901(b)(9)

2. Authentication of Electronic Evidence.

a. Output of Electronically-Stored Data: Fed. R. Evid. 901(b)(9).

(1) "[T]he accuracy of a result is dependant upon a process or system which produces it." As a consequence, Fed.R. Evid. 901(b)(9) requires showing of the reliability of the hardware and software used, the method of entering and storing the data, and the measures to ensure accuracy of the system.

(2) Courts are split in their approach to the level of proof necessary to meet this requirement.

(a) Some courts view computer technology as unique, and demand detailed information; but the overwhelming trend, as technology becomes more ubiquitous, is for courts to be much more easily satisfied with its accuracy.

(b) The proof necessary to meet this requirement will be more stringent depending upon the perceived reliability of the hardware and software. A custom-designed system probably requires more foundation than common equipment and software.

b. Solid Foundation — making (overcoming) objections.

(1) Experts must take particular care to "utilize the method which would yield the most complete and accurate results." *Gates Rubber Co. v. Bando Chemical Indus. Ltd.*, 167 F.R.D. 90, 112 (D. Colo. 1996) (court

criticized party expert for not making image copies of computer drive, which would more accurately reflect drive's contents, after expert extracted data pursuant to court site inspection order.) *Doe v. R.R. Donnelley & Sons Co.*, 42 F.3d 439 (7th Cir. 1994).

(2) Foundation testimony should include:

(a) equipment used is standard and reliable.

(b) program used is standard and reliable.

(c) any data entry is regularly checked for accuracy.

(d) data stored securely from loss or alteration.

(e) output fairly and accurately represents stored data.

(3) Sponsoring witness.

Personal knowledge not required. Can attest to the genuineness of the data and how it was prepared (entered, stored, manipulated, output).

3. Electronic Images.

a. Pictures traditionally authenticated through:

Sponsoring witness with personal knowledge.

b. Photographs inherently reliable;

But, altering photographs with relatively inexpensive computer equipment is now almost impossible to detect.

c. Document Imaging Systems:

(1) Digital computer storage and organization replaces mountains of paper;

(2) Reliability problems similar to other computer-based evidence (i.e., photographs);

(a) Scanned digital images can be easily altered.

(b) To assure genuineness, document imaging systems should include encryption and security features to preclude tampering.

(c) Procedures for scanning and cataloging may show accuracy.

C. "Best Evidence" Rule.

1. "To prove the content of a writing, recording, or photograph, the original writing, recording or photograph is required."

2. Under Fed. R. Evid. 1001(3), a printout of almost all computer-based information is considered an "original."

a. "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"

- It is unclear whether documents stored in imaging systems would be encompassed under this definition, or whether printouts of those documents would be considered a photocopy, and therefore inadmissible.

b. Computer-Based Summaries of Information: Fed. R. Evid. 1006.

(1) Some courts require that the underlying data summarized itself be admissible.

(2) Others find that the underlying data need only be provided to the opposing party.

D. Electronic evidence is usually hearsay.

1. Computer-Based Data and EDI.

a. The Business Records Exception: Fed. R. Evid 803(6). Fed. R. Evid. 803(6). Courts have overwhelmingly held that computer-based information is covered by this exception. *See, e.g. United States v. Miller*, 771 F.2d 1219 (9th Cir. 1985); *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984); *United States v. Scholle*, 553 F.2d 1109 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977). (*But see Monotype Corp. v. International Typeface Corp.*, 43 F.3d 443 (9th Cir. 1994) (e-mail not sufficiently routine in business to qualify for hearsay exception).

(1) Absence of Records: Fed. R. Evid. 803(7) "[e]vidence that a matter is not included" in records kept within requirements of 803(6) to be used "to prove the nonoccurrence or nonexistence of the matter."

(2) Business Record Admissibility: Records must be made in the normal course of business at or near the time of the event and must not "indicate lack of trustworthiness."

(3) Normal course of business could be a problem when the evidence for trial is printed or created by a program written specifically for the litigation.

(4) Timely recording.

(a) The argument that a printout is not made close enough to the time of the underlying transaction has been almost unanimously rejected by courts: "[i]t would restrict the admissibility of computerized records too severely to hold that the computer product, as well as the input upon which it is based, must be produced at or within a reasonable time after each act or transaction to which it relates."

(5) Courts have disagreed on the level of proof necessary to prove record is "trustworthy."

(a) Some commentators and courts believe the requirements should be rigorous, requiring a more strict foundation than typical business records to ensure that no mechanical or human errors have occurred.

(b) Most modern courts regard computer-based evidence as inherently more reliable, and requiring less of a foundation. In one case, a judge explained that the "computer evidence . . .[was] even more reliable than . . . average business record[s] because they are not even touched by the hands of man." *U.S. v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982).

i) Attitude: if computerized information is good enough for business, it should be good enough for the courts.

b. Public Records: Fed. R. Evid. 803(8).

(1) Provides another avenue to overcome a hearsay objection.

(a) Public records are self-authenticating under Fed. R. Evid. 902(4).

(b) *Armstrong v. Executive Office of the President*, 1 F.3d 1234 (D.C. Cir. 1993). 803(8) also proscribes from evidence data that is not trustworthy.

E. *California* admissibility — Presumptions favor admission.

1. Authentication. (It is what the proponent says it is.) Evid. Code § 1400, subd. (a).

2. Direct and Circumstantial Evidence (party creating or witnessing creation; admission by party against whom document offered) travel of message through intermediary. Evid. Code §§ 1411-1414.

3. *California's* Secondary Evidence Rule. Repeals the Best Evidence Rule (Former Evid. Code § 1500, *et seq.*)

4. Printouts are "originals" (Evid. Code § 255; *Aguimatang v. California State Lottery,* 234 Cal.App. 3d 769, 797 (1991) (interpreting Evid. Code § 1500).

5. As of January 1, 1999: "Proof of content of a writing" (Evid. Code § 1520). Writing may be proved by otherwise admissible secondary evidence unless a genuine dispute exists, or admission of secondary evidence "unfair."

a. Printed representations of computer information data are presumed accurate. (Evid. Code § 1552 subd. (a))

b. Printed representation of images on video or digital media presumed accurate. (Evid. Code § 1553)

6. Hearsay (Evid. Code § 1200, subd. (a))

a. Electronic documents, if offered for the truth of the matter stated, are hearsay.

(1) Electronic documents, if used to establish operative facts, not hearsay.

(2) Evidence from adversary's computer — admission of a party opponent. (Evid. Code § 1220)

(3) Business Record Exception (Evid. 1271, 1280, subd. (c))

b. *People v. Lugashi* (1988) 205 Cal.App.3d 632 (foundation for computer records; requirement for establishing system reliability/maintenance rejected). Sufficient that "person who generally understands system operation, possess knowledge and skill to use system and explain resulting data is 'qualified witness' required by Evidence Code Section 1271." *Aguimatang v. California State Lottery* (1991) 234 Cal.App. 3d 764, 797.

c. Garbage in, garbage out — not all electronic records are inadmissible. *People v. Hernandez* (1992) 55 Cal.App.4th 225, 261.