A Practical Introduction to Electronic Discovery

aka e-data discovery; digital discovery; computer discovery

How to discover what you cannot see

David Nuffer
U.S. Magistrate Judge

Utah State Bar
March 2004
St. George, Utah

Hazards of electronic discovery

Danis v. USN Communications, 2000 WL 1694325 (N. D. Ill.). An exhaustive opinion scorches counsel for both parties engaged in a major discovery dispute:

> Sorting out what happened here has been a challenging task not only due the complexity of some of the issues presented, but -- regrettably -- due to assertions of counsel that often have confused [rather] than clarified the issues. On a number of occasions, plaintiffs have asserted that certain documents were not produced, when in fact it later turned out that the documents long ago had been produced. Conversely, defendants have on occasion informed the Court that they have produced certain documents, when in fact it turned out that they had not. Moreover, throughout these proceedings, the submissions by the lawyers too often have offered overblown rhetoric rather than accurate information and careful reasoning. In the Court's judgment, there are several reasons why-- despite the high level of experience and quality of the attorneys -- this has occurred.
> [***]
> As a result, both sides were the losers. They lavished huge sums of time and money on an issue that did not remotely justify the expenditure, and which would have been more profitably spent focusing on the merits of this case.
> [***]
> 5. The Court recommends that no attorneys' fees and costs be assessed in connection with the prosecution or defense of this motion. Plaintiffs claim that their fees and costs on the sanctions issue total $757,559.61, and (not to be outdone) the individual defendants assess their fees and costs at $767,202.42. Viewed separately, not to mention collectively, these statements of fees and costs are nothing short of shocking: they are wholly disproportionate to what the evidence has disclosed. Because the conduct of each side has contributed to an excessive expenditure of fees and costs, the Court considers the fees and costs incurred to be a self-inflicted wound by each side, and that neither side should be forced to pay the costs and fees of the other side.

Gates Rubber v. Bando Chemical Industries, 167 F.R.D. 90 (D. Colo. 1996). A bitter trade secret case morphed into a data discovery disaster:

> The sanctions hearing itself consumed a total of six weeks of evidence and testimony, and the hearing was conducted in several sections over a period of a year. I viewed countless hours of segments of video deposition testimony, covering approximately 20 witnesses; I listened to testimony from 20 witnesses who were called to court to testify live; and I received thousands of pages of pleadings, exhibits, documents and deposition excerpts. These materials were presented to me in 3-ring binder notebooks, and by the conclusion of the sanctions hearing I had received 50 of them. As of the time of the writing of this order, there are over 1,500 docket entries in the clerk's office, the vast majority of the entries relating to the sanctions proceedings.
> [***]
> The lawyers for Gates have delayed this case for the better part of three and one-half years over an exaggerated concern with minutiae. They had little idea what they were looking for during the site inspection. They copied very little of the type of materials which they now complain were destroyed by the defendants. They admit that they have not examined any of the large quantity of boxes of documents which they did copy and preserve. In fact, the lawyers for Gates have argued vociferously that they have not yet even started discovery on the merits of this controversy. Harm from the alleged destruction of documents must be measured in light of what is produced, as well as what is not produced. Capellupo v. FMC Corp., 126 F.R.D. at 553. Gates has no idea what has been produced.

GTFM v. Wal-Mart Stores, 2000 WL 335558 (S.D. N.Y.). Defendant’s counsel provided inaccurate information to the plaintiffs about computer records early in discovery, and discoverable computer records were later destroyed.

> Therefore, defendant is ordered to pay all plaintiffs' expenses and legal fees unnecessarily expended due to defendant's failure to make an accurate disclosure of its computer capabilities in December 1998. Plaintiffs

shall, within thirty days of the entry of this Opinion and Order, make application for such expenses and legal fees, with defendant to file any opposition to such fee application within fifteen days thereafter.

In re the Prudential Insurance Company Of America Sales Practices Litigation, 169 F.R.D. 598, 36 Fed.R.Serv.3d 767 (D. N.J. 1997). Prudential failed to coordinate an existing document destruction policy with a court order to preserve documents.

> While there is no proof that Prudential, through its employees, engaged in conduct intended to thwart discovery through the purposeful destruction of documents, its haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute. Because the destroyed records in Cambridge are permanently lost, the Court will draw the inference that the destroyed materials are relevant and if available would lead to the proof of a claim.
> [***]
> When the September 15, 1995 Court Order to preserve documents was entered, it became the obligation of senior management to initiate a comprehensive document preservation plan and to distribute it to all employees.
> [***]
> The Court finds that the document destruction, particularly in the Cambridge, Massachusetts office, caused harm to party opponents. Over 9,000 files were cleansed.
> [***]
> Within ten (10) days after the issuance of this Opinion, Prudential shall pay to the Clerk of the United States District Court for the District of New Jersey, the sum of One Million Dollars ($1,000,000).

169 F.R.D. at 615-617

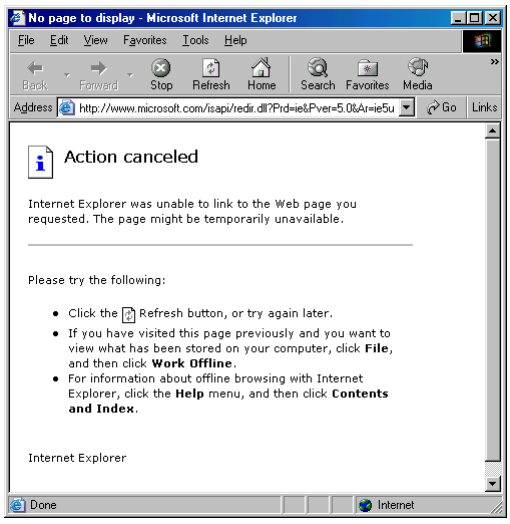
Invisible data can be seen

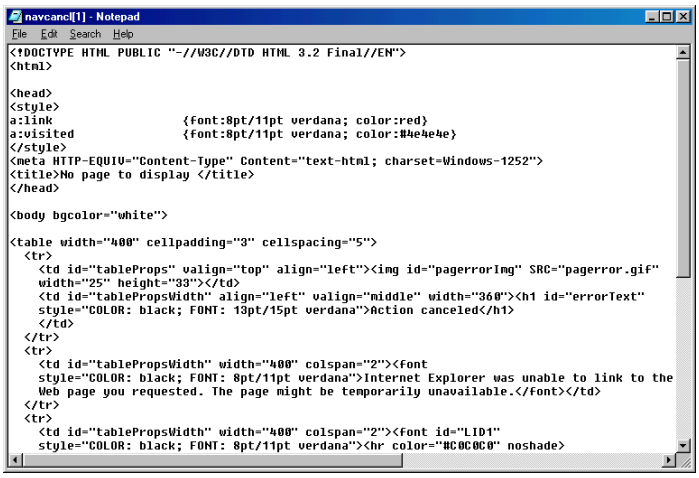
Paper is visible, tangible, tactile. We can see what is in it and when we copy it, we get it all.

Humans need to use a *viewer* to see electronic data . When we say ‘we saw the video’ we don’t mean we looked at the tape cartridge. We mean we put it in a VCR, connected to a TV. We cannot tell if a CD is ‘a good CD’ until we put it in a CD player. And we cannot tell what is on a computer disk without a computer *and* software to view the disk contents.

Viewer Examples:

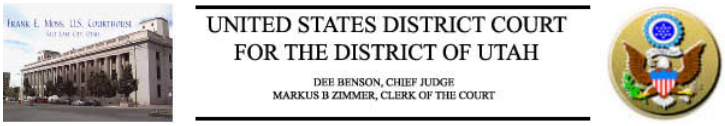
> A web page may look like this on a screen in a “web browser” viewer, but if we look at the HTML code that makes up the page, we see something entirely different, including things we do not see when looking at the page in a browser.



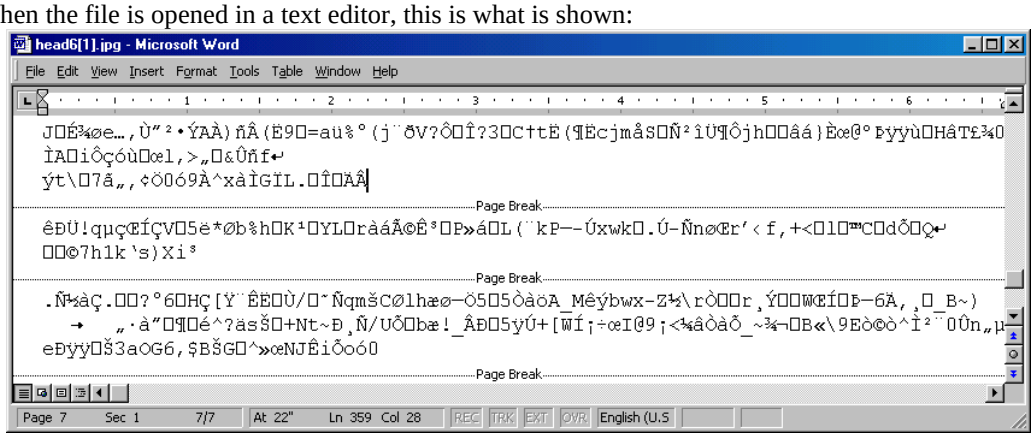


The bits and bytes of an image file appear differently in a text viewer than an image viewer.

This is the image:

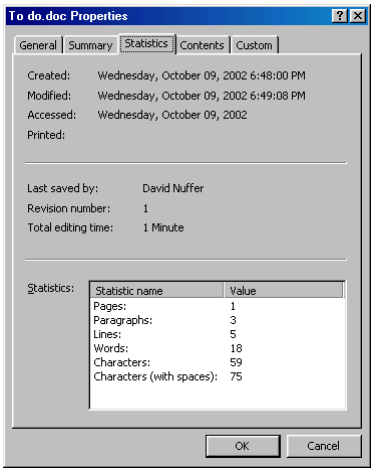


When the file is opened in a text editor, this is what is shown:

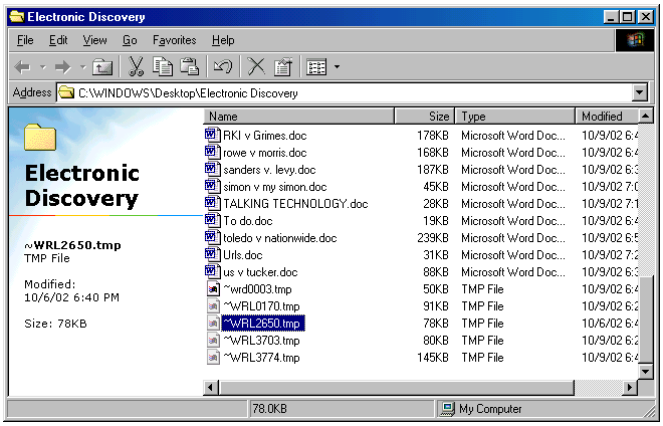


If the right viewer is used, invisible data that you normally do not see can be seen.

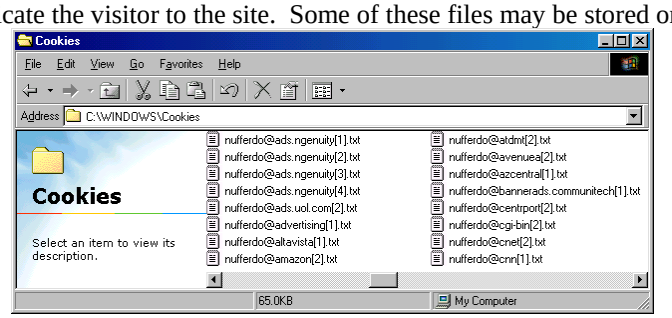
Meta data is data *about* the data being used. Meta data is stored with the data we usually see – but is usually invisible. For example, all word processors store many details about the documents they create. We can see some of it if we call it up.

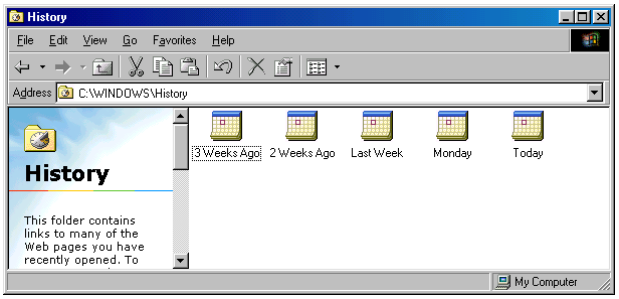


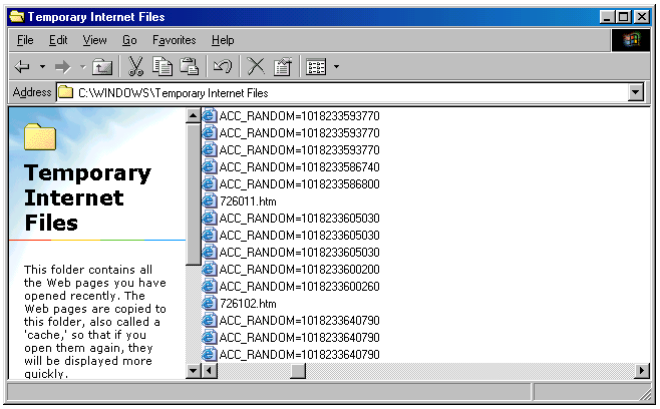
Most programs also create entirely separate files from the files we think we work with. These "temp files" are created without our knowledge or intervention, and may remain on a computer for long periods of time. They are often working files for the program. Some give the program a chance to recover data in the event of a crash.

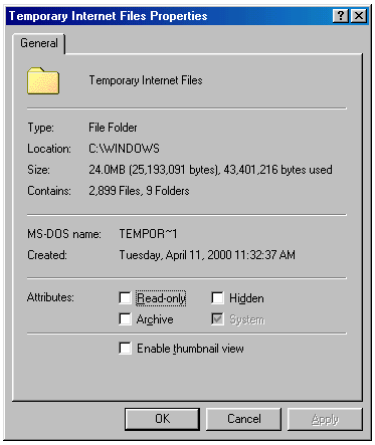


Web browsing creates files that may include every component of every page viewed and a separate list of those pages; and browsing may create a file to send to the web site every time the site is visited – to authenticate the visitor to the site. Some of these files may be stored on the computer *and* on the web site.









Other types of data files that a computer may create invisibly include:

Version files – other versions of a document.

Tracking files – data paths showing the entire history of edits made to a document.

"Shared"files – files sent via e mail or disk to others exist in two or more places.

Local copy of server stored documents, or server stored copies of local data – a computer system may safeguard data by storing multiple copies, using one as the "preferred" file and the other as a backup. Or one file may be a "working" file, while another is permanent.

Deleted files – files which are "deleted" by a computer user may be in the Recycle Bin and -- even if emptied from the trash or deleted -- are usually still present on disk. Deleting a file only removes the *address*. Only when another piece of data lands on that spot on the hard disk is the original file replaced with other data.

Swap files – Windows often uses part of the hard disk space as temporary memory, storing and tracking everything done on the computer.

Backup files – files may be stored periodically for emergency recovery.

Archive files – files may be stored permanently as a record of a point in time.

Putting it into perspective:

What we see on our screen is the tip of the data iceberg. Each viewer is optimized for the purposes of the moment, and does not necessarily reveal all data that is present.

Software reveals, conceals, organizes and locates electronic data for its own purposes. Different software may reveal, conceal, organize and locate the same data for other purposes.

In its natural state, electronic data is chaotic and unintelligible. Software makes it usable.

Storing and deleting data:

While paper records are often destroyed or discarded, electronic data is more often inadvertently retained than intentionally discarded, because the cost of storage is so small. It is hard to sort, filter and evaluate old data. Usually, it just goes out of date or out of mind, but remains alive.

Electronic data may be inadvertently erased as a computer is used. The operations of a computer will modify invisible data, particularly deleted data. Each time a file is accessed and stored, it may erase its own prior version.

Ken Withers -- "Nature abhors a vacuum, so your computer hard drive fills itself with data. You may not know it is there, but it is."

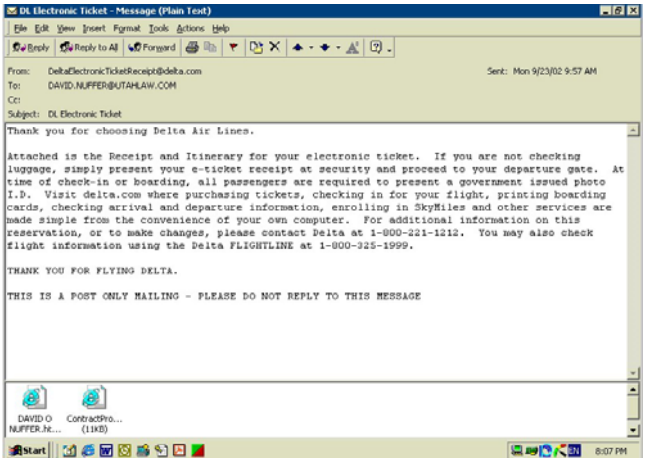
Ken Withers -- "Just like the yellowed newspapers used for packing in an old box, stray data may be more interesting than the object meant to be stored."

How do we find e-data?

Ask these questions:

What are the business processes? Which are conducted with electronic assistance? What records might exist? How does the business use– create – retrieve data?

- E Mail
- Word processing
- Spreadsheet
- Calendar
- Database
- Contacts
- Transactional/Workflow software



What e data is created? Intentionally? Inadvertently? Collaterally?

How does the business purposely and inadvertently retain data?

What sorts of media are in use?

- Tape
- CD (compact disc)
- DVD (digital vídeo disc)
- Hard disk (in almost all computers)
- Floppy disks
- Zip disks (removable large capacity disks)
- Memory Sticks (removable memory chips)

What data types are available?

- Current use - versions
- Archival use – permanent file (evidence at a point in time)
- Backup use – emergency restore

What is the geographic location of data?

- Workstation
- Server
- Replica Servers
- Co workstation
- Home computer
- Laptops
- PDA
- Phones
- Internet sites

The duty to preserve invisible data

New York National Organization for Women v. Cuomo, 1998 WL 395320 (S.D. N.Y.). Counsel has a duty to advise the client to take reasonable steps to preserve records subject to discovery.

> Service of a complaint puts the receiving party on notice that it is required to preserve evidence that may be relevant to the claims asserted. *See Turner v. Hudson Transit Lines, Inc.,* 142 F.R.D. 68, 73 (S.D.N.Y. 1991); *Computer Associates International, Inc. v. American Fundware, Inc.*, 133 F.R.D. 166, 169 (D. Colo.1990).

Danis v. USN Communications, 2000 WL 1694325 (N. D. Ill.). The failure to take reasonable steps to preserve data at the outset of discovery resulted in a personal fine levied against the defendant's CEO.

> [F]undamental to the duty of production of information is the threshold duty to preserve documents and other information that may be relevant in a case.
> [***]
> . . . when a charge is made that relevant information has been destroyed, and especially when a charge is made of intentional destruction, it is a charge that strikes at the core of our civil litigation system. The motion presently before this Court presents just such a charge.
> [***]
> Immediately upon the filing of the *Glotzer* lawsuit, USN was required to preserve for possible production in the lawsuit documents (whether in hard copy or electronic form) that might be discoverable. That duty flowed both from the Private Securities Litigation Reform Act of 1995 [citation omitted] and from a common law duty not to spoil documents that might be discoverable in the litigation. [citation omitted]
> [***]
> The duty to preserve documents in the face of pending litigation is not a passive obligation. Rather, it must be discharged actively:
>
> > [i]t was incumbent on senior management to advise its employees of the pending litigation ..., to provide them with a copy of the Court's order, and to acquaint its

> employees with the potential sanctions ... that could issue for noncompliance with [the] Court's Order.
> When senior management fails to establish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of field office actions. The obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers.
> [citations omitted]
> [***]
> The scope of the duty to preserve is a broad one, commensurate with the breadth of discovery permissible under Fed.R.Civ.P. 26.
> [***]
> Moreover, the case law establishes that a discovery request is not necessary to trigger this duty. "A party clearly is on notice of [t]he relevance of evidence once it receives a discovery request. However, the complaint itself may also alert a party that certain information is relevant and likely to be sought in discovery." [citations omitted]

In re Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437, 444, 51 Fed.R.Serv.3d 1212 (D. N.J. 2002).

> [C]ounsel should take advantage of the required Rule 26(f) meeting to discuss issues associated with electronic discovery. As the eve of electronic case filing (ECF) is upon us, in this and most other Districts, the production of electronic information should be at the forefront of any discussion of issues involving discovery and trial, including the fair and economical allocation of costs. Of course, in some instances, paper, rather than electronic, production may still be the preferable method of discovery.

ABA Civil Discovery Standards 10 & 29 (1999) Note these standards are under revision, with addition of many electronic discovery related standards. http://www.abanet.org/litigation/taskforces/electronic/amendments.doc

> IV. DOCUMENT PRODUCTION
>
> > 10. The Preservation of Documents. When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents and of the possible consequences of failing to do so.
>
> VIII. TECHNOLOGY
>
> > 29. Preserving and Producing Electronic Information.
> >
> > a. Duty to Preserve Electronic Information.
> >
> > i. A party's duty to take reasonable steps to preserve potentially relevant documents, described in Standard 10 above, also applies to information contained or stored in an electronic medium or format, including a computer word-processing document, storage medium, spreadsheet, database and electronic mail.
> >
> > ii. Unless otherwise stated in a request, a request for "documents" should be construed as also asking for information contained or stored in an electronic medium or format.
> >
> > iii. Unless the requesting party can demonstrate a substantial need for it, a party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory.

2001 Records Management Survey:

Businesses which have records management programs:

56% do not include electronic records in their program.
70% actually follow the records retention schedule. (30% do not.)
67% have a formal procedure to "hold" records needed for a special purpose, like litigation.
41% include electronic records in their hold procedure.

Records Managers:

94% believe the outcome of future litigation will be affected by the way they manage electronic records.
28% are confident they can defend their electronic records management in court.

To fulfill the duty to preserve:

Understand
Formulate
Write
Communicate
Delegate to competent people
Follow up

Should e-discovery be permitted?

Rule 34, F.R.Civ.P.

> Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form) . . .

F.R.Civ.P. 34(a) advisory committee's notes, 1970.

> The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data. The burden thus placed on respondent will vary from case to case, and the courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs. Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.

Anti-Monopoly v. Hasbro, 1995 WL 649934 (S.D. N.Y.).

> It is black letter law that computerized data is discoverable.
>
> Thus, the rule is clear: production of information in "hard copy" documentary form does not preclude a party from receiving that same information in computerized/electronic form.

Simon Property Group, L.P. v. mySimon, Inc.,194 F.R.D. 639, 47 Fed.R.Serv.3d 247 (S.D. Ind. 2000)

> [C]omputer records, including records that have been "deleted," are documents discoverable under Fed.R.Civ.P. 34.

Considerations vary with every case:

- Interference with business operations
- Invasion of privacy
- Software license issues
- Cost
- Complexity
- Diversion from main issues in case
- Likelihood of usefulness
- Availability in other forms
- Protection of privilege
- Work product
- Discretion of trial court

How to acquire and deliver e-data

Four major issues:

- Preserve – how do you preserve electronic data? (In your hands or the hands of an opponent.)
- Select – how is the data responsive to the request selected and by whom?
- Privilege – how can a meaningful opportunity be given to preserve privilege – and knowledge of privileged communication and how can inadvertent waiver be prevented?
- Transfer – how will the data be delivered to the requesting party?

Recommended procedures:

- "Image" – use specialized software and hardware to make an "image" or "mirror" copy of the data source.
- Use a qualified expert.

Gates Rubber v. Bando Chemical Industries, 167 F.R.D. 90 (D. Colo. 1996). When allowed direct access to the respondent's computer system for the purposes of discovery, the requesting party's computer discovery "expert" destroyed 7-8% of discoverable records and compromised the evidentiary integrity of the rest.

Simon Property Group, L.P. v. mySimon, Inc., 194 F.R.D. 639, 47 Fed.R.Serv.3d 247 (S.D. Ind. 2000)

> On June 7, 2000, the court . . . outlined a protocol for allowing [discovery of "deleted" files and documents in computer memories.] In general, the plan is to have plaintiff select and pay an expert in recovery of such information, and to have that expert serve as an officer of the court and turn over the recovered information to defendant's counsel for appropriate review to supplement defendant's discovery responses. [***]
>
> In essence, plaintiff shall select and pay an expert who will inspect the computers in question to create a "mirror image" or "snapshot" of the hard drives. Cf. *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, 167 F.R.D. 90, 111-13 (D.Colo.1996) (describing problems that arose when one party's effort to preserve and recover files resulted in overwriting of 7 to 8 percent of hard drive contents). Defendant shall have a chance to object to the selection of the expert. The court will appoint the expert to carry out the inspection and copying as an officer of the court.
>
> The expert shall then use his or her expertise to recover from the "mirror image" of the hard drive of each computer, and to provide in a reasonably convenient form to defendant's counsel, all available word-processing documents, electronic mail messages, powerpoint or similar presentations, spreadsheets, and similar files. The court intends that files making up operating systems and higher level programs in the computer not be duplicated, and that the copying be limited to the types of files reasonably likely to contain

material potentially relevant to this case. Cf. *Adobe Systems, Inc. v. South Sun Products, Inc.*, 187 F.R.D. 636, 642-43 (S.D.Cal.1999) (noting that Microsoft Office 97 occupies more than 200 megabytes on hard drive of a personal computer). To the extent possible, the expert shall also provide to defendant's counsel: (a) the available information showing when any recovered "deleted" file was deleted, and (b) the available information about the deletion and contents of any deleted file that cannot be recovered.

After receiving these records from the expert, defendant's counsel shall then have to review these records for privilege and responsiveness to plaintiff's discovery requests, and shall then supplement defendant's responses to discovery requests, as appropriate.

The expert shall sign the protective order in the case and shall retain until the end of this litigation the "mirror image" copies of the hard drives and a copy of all files provided to defendant's counsel. At the end of this litigation, the expert shall then destroy the records and confirm such destruction to the satisfaction of defendant. The expert shall not disclose the contents of any files or documents to plaintiff or its counsel or other persons. Because the expert will serve as an officer of the court, disclosure of a communication to the expert shall not be deemed a waiver of the attorney- client privilege or any other privilege.

Murphy Oil, Inc., v. Fluor Daniel, Inc., 2002 WL 246439, 52 Fed.R.Serv.3d 168 (E.D. La. 2002). After ordering the requesting party to pay the cost of restoring and printing e mail backup tapes, the Court concluded that since these backup tapes were retained in contravention of a disposal/recycling policy, they were not needed by the producing party – and could just be delivered to the requesting party. A privilege review protocol was established in alternative forms, depending on whether privilege review occurred after selection of responsive e mails by requesting party or after the producing party selected responsive e mails. The court ordered that if the requesting party culled e mails before the producing party made its privilege review, the requesting party's review of the emails would not waive the privilege – but obviously, counsel for the requesting party still knows what the e mails said!

First Technology Safety Systems, Inc., v. Depinet, 11 F.3d 641, 62 USLW 2390, 1994 Copr.L.Dec. P 27,187, 27 Fed.R.Serv.3d 947, 29 U.S.P.Q.2d 1269 (6th Cir. 1993). *Ex parte* order to enter and seize computer data reversed. The material seized -- and copies -- were ordered returned. *Ex parte* action requires a "showing that the adverse party has a history of disposing of evidence or violating court orders or that persons similar to the adverse party have such a history."

A party's business technology policy does not establish a litigation standard

Some assume that a business records retention policy will protect the business and counsel from preservation of electronic data, and that the responding party's lack of a "business purpose" for a mode of requested production of electronic data will automatically shift the cost of production of electronic data to the requesting party. This is not necessarily true. Businesses should formulate policies and information systems with a view to possible accountability, and may not restrict their considerations to maximum business efficiency.

. . . as to data retention and preservation:

Reimgold v. Wet 'N Wild Nevada Inc., 944 P.2d 800 (Nev. 1997) A jury verdict for the defendant was reversed for failure to instruct on adverse inference from failure to produce first aid records to show notice of prior accidents. Defendant's policy to destroy records at end of each season prior to running of statute of limitations; "following the company's normal records retention policy" may be willful suppression.

> [A] document retention/destruction policy that results in the systematic destruction of probable evidence will not provide protection from spoliation charges.

Computer Assoc. Intn'l. v American Fundware Inc., 133 F.R.D. 166 (D. Colo. 1990). Defendant's common practice was to only retain current source code and it continued destruction even after a discovery request. Default judgment was entered against defendant in this copyright case.

Lewy v. Remington Arms, 836 F. 2d 1104 (8th Cir. 1988). This pre-computer case held routine records management procedures should be designed to preserve records which the defendant may reasonably anticipate will be subject to discovery.

> This instruction was requested by the Lewys because Remington was unable to produce several documents that were destroyed pursuant to Remington's "record retention policy." Remington argues that destroying records pursuant to routine procedures does not provide an inference adverse to the party that destroyed the documents. Smith v. Uniroyal, Inc., 420 F.2d 438, 442-43 (7th Cir. 1970).
> [***]
> First, the court should determine whether Remington's record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents. For example, the court should determine whether a three year retention policy is reasonable given the particular document. A three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints. Second, in making this determination the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints.
> Finally, the court should determine whether the document retention policy was instituted in bad faith. Gumbs v. International Harvester, Inc., 718 F.2d 88, 96 (3rd Cir. 1983) ("no unfavorable inference arises when the circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where the failure to produce it is otherwise properly accounted for."); Boyd v. Ozark Air Lines, Inc., 568 F.2d 50, 53 (8th Cir. 1977) ("We recognize, however, that the destruction of business records may be sufficient to raise an unfavorable inference."). In cases where a document retention policy is instituted in order to limit damaging evidence available to potential plaintiffs, it may be proper to give an instruction similar to the one requested by the Lewys. Similarly, even if the court finds the policy to be reasonable given the nature of the documents subject to the policy, the court may find that under the particular circumstances certain documents should have been retained notwithstanding the policy. For example, 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. Gumbs, 718 F.2d at 96 ("Such a presumption or inference arises, however, only when the spoilation 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." (quoting 29 Am.Jur.2d Evidence ß 177 (1967)).

. . . as to data retrieval:

In re Brand Name Prescription Drugs Litigation, 1995 WL 360526 (N.D. Ill. 1995). When a defendant chooses a computer-based business system, the cost of retrieving information is an ordinary and foreseeable risk. Citing *Daewoo Electronics Co. v. United States*, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986), the court stated:

> It would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation. The use of excessive technical distinctions is inconsistent with the guiding principle that information which is stored, used, or transmitted in new forms should be available through discovery with the same openness as traditional forms.
> [* * *]
> The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship.

Linnen v. A.H. Robins, 1999 WL 462015 (Mass. Sup. Ct.). Counsel failed to adequately investigate the client's computer records and holdings, and thereby failed to preserve relevant computer records. In the face of repeated representations before the court that no relevant records existed, a spoliation inference would be a reasonable sanction.

The *Linnen* court also held that the responding party would bear the cost of restoring backup tapes to its computer system to facilitate discovery:

> While the court certainly recognizes the significant cost associated with restoring and producing responsive communications from these tapes, it agrees with the District Court for the Northern District of Illinois *In re: Brand Name Prescription Drugs Antitrust Litigation* that this is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world. 1995 WL 360526 (N.D.Ill.). To permit a corporation such as Wyeth to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.

Toledo Fair Housing Center v. Nationwide Insurance Company, 703 N.E.2d 340, 94 Ohio Misc.2d 17 (Ohio Ct. Common Pleas 1996)

> With regard to the discoverability of the computerized data, I find that the information sought in request numbers 25, 26, 29, and 30 is highly relevant to the plaintiffs' case and is, therefore, discoverable. Nationwide shall bear the cost of retrieving this information and making it available to the plaintiffs in a format readable by a layperson. Nationwide strenuously argues that the cost of producing the requested discovery is overly burdensome, and the record confirms that the cost is potentially great. However, inconvenience and expense, by themselves, do not justify denying discovery. See *Isaac v. Shell Oil Co.* (E.D.Mich.1979), 83 F.R.D. 428, 431 (discovery denied). Furthermore, a party cannot avoid discovery when its own recordkeeping system makes discovery burdensome. If a party chooses to store information in a manner that tends to conceal rather than reveal, that party bears the burden of putting the information in a format useable by others. See *id.; Kozlowski v. Sears, Roebuck & Co.* (D.Mass.1976), 73 F.R.D. 73, 76. See, also, *Dunn v. Midwestern Indemn.* (S.D.Ohio 1980), 88 F.R.D. 191, 198 (applying *Kozlowski* to computer-generated discovery in an insurance redlining case).

Kozlowski v. Sears, Roebuck, 73 F.R.D. 73 (D. Mass. 1976).

> In the instant case, the requested documents are clearly within the scope of Rule 26(b), Fed. R. Civ. P., the plaintiff has a demonstrable need for the documents, the defendant undisputedly has possession of them, and the plaintiff has no other access to them. Thus, the defendant has a duty pursuant to Rule 34, Fed. R. Civ. P., to produce its records of similar suits. The defendant seeks to absolve itself of this responsibility by alleging the herculean effort which would be necessary to locate the documents. The defendant may not excuse itself from compliance with Rule 34, Fed. R. Civ. P., by utilizing a system of record-keeping which conceals rather than discloses relevant records, or makes it unduly difficult to identify or locate them, thus rendering the production of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules. See *Hickman v. Taylor*, 329 U.S. 495, 500, 67 S.Ct. 385, 91 L.Ed. 451 (1947); Holtzoff, Instruments of Discovery Under Federal Rules of Civil Procedure, 41 Mich.L.Rev. 205, 224 (1942).
> [***]
> Finally, the defendant makes a confusing offer to finance the transportation to Chicago, Illinois (where the records are kept), by the plaintiff's attorney so that he may either attempt to locate the desired documents among the defendant's massive files, or else verify for himself the impossibility of such a task. The defendant has in essence told the plaintiff that, if he wishes, he may hunt through all its documents and find the information for himself. "This amounts to nothing more than a gigantic 'do it yourself' kit." See *Harlem River Consumers Cooperative, Inc. v. Associated Grocers of Harlem, Inc.*, 64 F.R.D. 459 (S.D.N.Y. 1974), quoting *Life Music, Inc. v. Broadcast Music, Inc.*, 41 F.R.D. 16 (S.D.N.Y. 1966). This Court will not shift the financial burden of discovery onto the discovering party, in this case an indigent plaintiff, where the

> costliness of the discovery procedure involved is entirely a product of the defendant's self- serving indexing scheme over which the plaintiff has no control.

See also Rhone-Poulenc Rorer, Inc. v. The Home Indemnity et. al. 1991 WL 111040, 1991 WL 111040 (E.D.Pa. 1991)

Who bears the cost of e-data discovery?

Rule 26(c), F.R.Civ.P.

> [T]he court in which the action is pending . . . may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense . . .

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003)
http://www.nysd.uscourts.gov/rulings/02cv01243_072403.pdf
The court shifted one-fourth of estimated $166,000 cost of restoring and searching 77 backup tapes to the plaintiff, a female former employee. She had requested archived e-mails off from backup tapes. The suit against her former employer alleged gender discrimination.
When a discovery request seeks accessible data--for example, active on-line or near-line data--it is typically inappropriate to consider cost-shifting. Although the presumption is that the responding party must bear the expense of complying with discovery requests, requests that run afoul of the Rule 26(b)(2) proportionality test may subject the requesting party to protective orders under Rule 26(c), "including orders conditioning discovery on the requesting party's payment of the costs of discovery. The responding party has the burden of proof on a motion for cost-shifting.
To determine whether shifting costs of discovery to requesting party is appropriate for discovery of inaccessible data, court should consider, weighted more-or-less in following order:

(1) extent to which request is specifically tailored to discover relevant information,
(2) availability of information from other sources,
(3) total cost of production, compared to amount in controversy,
(4) total cost of production, compared to resources available to each party,
(5) relative ability of each party to control costs and its incentive to do so,
(6) importance of issues at stake in litigation, and
(7) relative benefits to parties of obtaining information.

The first two factors together comprise the "marginal utility test" The second group of factors (3, 4 and 5) addresses cost issues: 'How expensive will this production be?' and, 'Who can handle that expense?' A list of factors is not merely a matter of counting and adding; it is only a guide. The precise allocation is a matter of judgment and fairness rather than a mathematical consequence of the seven factors discussed above. As a general rule, where cost-shifting is appropriate, only the costs of restoration and searching should be shifted. The responding party should *always* bear the cost of reviewing and producing electronic data once it has been converted to an accessible form.
In order to obtain a factual basis to support the cost-shifting analysis, the judge ordered Defendant UBS to restore and produce e-mails from five of ninety-four backup tapes. Plaintiff Zubulake was permitted to select the five tapes to be restored. The total number of *unique* e-mails restored was 6,203. A search for e-mails containing (in either the e-mail's text or its header information, such as the "subject" line) the terms "Laura", "Zubulake", or "LZ" yielded 1075 emails. Approximately 600 were responsive to Zubulake's document request and were produced.
Thus, the total cost of restoration and search was $11,524.63. In addition, UBS incurred $4,633 in attorney time for the document review and $2,845.80 in paralegal time. In addition, $432.60 in photocopying costs were paid by Plaintiff. The total cost of restoration and production from the five backup tapes was thus $19,003.43.
Extrapolated to the entire set of tapes, the total cost figure includes $165,954.67 to restore and search the tapes and $107,694.72 in attorney and paralegal review costs.
See also Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003)
http://www.nysd.uscourts.gov/rulings/02cv1243_051803.pdf

Rowe Entertainment, Inc. v. The William Morris Agency, Inc., 2002 WL 63190 (S.D.N.Y. Jan. 16, 2002), (Plaintiff's Motion to Reverse Magistrate Judge denied at 2002 WL 975713 (S.D.N.Y.), 2002-1 Trade Cases P 73,677).

> [C]ourts have adopted a balancing approach taking into consideration such factors as:
> (1) the specificity of the discovery requests;
> (2) the likelihood of discovering critical information;
> (3) the availability of such information from other sources;
> (4) the purposes for which the responding party maintains the requested data;
> (5) the relative benefit to the parties of obtaining the information;
> (6) the total cost associated with production;
> (7) the relative ability of each party to control costs and its incentive to do so; and
> (8) the resources available to each party.
> Each of these factors is relevant in determining whether discovery costs should be shifted in this case.

Murphy Oil, Inc., v. Fluor Daniel, Inc., 2002 WL 246439, 52 Fed.R.Serv.3d 168 (E.D. La. 2002). Restoring backup tapes of e mail to the system for printing would cost $6.2 million – by producing party's estimate – and requesting party failed to offer contrary proof. Using *Rowe* criteria, the court shifted the cost to requesting party. But with a deft twist, the Court concluded that these backup tapes were actually retained in contravention of a disposal/recycling policy and were not really needed by the producing party – and could just be delivered to the requesting party. A privilege review protocol for e-mail was established in alternative forms, depending on whether privilege review occurred before selection by requesting party or after.

In re Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437, 51 Fed.R.Serv.3d 1212 (D. N.J. 2002). Plaintiffs requested paper copies after defendants' Rule 26(a)(1) disclosures failed to reveal the existence of existing electronic versions of some of the documents. As to documents in electronic form at the time of the 26(a)(1) disclosures, plaintiffs were excused from paying copying or printing costs, and defendants were ordered to deliver CDs of those items for the nominal cost of copying a CD. After the 26(a)(1) disclosures, defendants scanned other documents into electronic form. Defendants were not required at the time of the 26(a)(1) disclosures to declare their intention to later scan these other documents, but since paper copies were produced for plaintiffs by printing rather than copying, plaintiffs were only required to pay the 8¢ per page *printing cost*, not the 10¢ per page copying cost. Since defendants made the decision to incur the scanning expense, independent of the request for production from plaintiffs, plaintiffs were entitled to copies of the CDs of these items also, for the nominal cost of copying.

Practice tips

Alert your client to preservation duties.
Alert opposing counsel to preservation duties.
Engage an expert.
Meet and confer regarding electronic discovery.
Include electronic discovery considerations in the discovery plan.
Obtain a preservation order (by stipulation).
Meet with your client's MIS director.
Take a 30(b)(6) deposition of your opponent's MIS director.
Ask every witness about electronic data.
Keep the chain of custody clean.
Maintain perspective.

Utah e-data cases

Bills v. Kennecott, 108 F.R.D. 459, 40 Fair Empl.Prac.Cas. (BNA) 1182, 42 Empl. Prac. Dec. P 36,732 (D. Utah 1985) (Greene) "Computers have become so commonplace that most court battles now involve discovery of some type of computer-stored information." Defendant employer's motion that plaintiffs pay $5,411.25 cost of printing e mail was denied, considering that the amount of money involved was not excessive or inordinate; the relative expense and burden in obtaining the data would have been substantially greater for plaintiffs as compared with defendant; the amount of money required to obtain the data as set forth by defendant would have been a substantial burden to plaintiffs; and the defendant was benefited to some degree by producing the data. Judge Greene acknowledges that cost-shifting to the requesting party has occurred in paper discovery by forcing the requesting party to make its own copies of produced material, but declined to cost-shift in this case.

Procter & Gamble v. Haugen, 179 F.R.D. 622, 1998-2 Trade Cases P 72,283 (D. Utah 1998) (Kimball) While "the duty to preserve evidence exists independently of court order, a court order would have delineated the scope of P & G's duties, provided clear evidence that P & G was on notice of the relevance of the e-mail communications, and furnished a standard by which this court could judge the adequacy of P & G's production efforts." Therefore, P&G's destruction of e mails it felt irrelevant *after* keyword searching was not penalized. But P&G's had destroyed e mails of five employees P&G had previously identified as pertinent. This justified a $10,000 sanction. The opinion also refines a court-approved list of keywords to be searched in Amway's electronic databases.

U.S. v. Tucker, 150 F.Supp.2d 1263 (D. Utah 2001), *aff'd* 305 F.3d 1193 (10th Cir. 2002). (Campbell). An image copy of defendant's hard drive revealed that he had visited child pornography web sites. As he viewed photos, the computer temporarily stored them in cache files. He purposely deleted these files, but intentionally stored some. "Possession" supported the conviction.

If you are aware of other Utah U.S. District Court decisions on e-data, please notify me at utmj_nuffer@utd.uscourts.gov

Resources

http://www.kenwithers.com/ Ken has it all.
http://www.fjc.gov/newweb/jnetweb.nsf/pages/196 Federal Judicial Center materials.

http://californiadiscovery.findlaw.com/electronic_data_discovery.htm California Commissioner Richard Best's exhaustive site on Electronic Discovery, part of his larger Discovery web site. Not especially pretty but if there is a case on point you will find it cited here.

http://cyber.law.harvard.edu/digitaldiscovery/ "A project to explore, develop, and educate on discovery in the digital sphere."

Many electronic discovery service providers have resources on their web sites:

- http://www.krollontrack.com/LawLibrary/ Articles; case law digest; offers a free e mail news letter.
- http://www.forensics.com/html/resource_center.html Articles, case law and **forms**.
- http://www.applieddiscovery.com/lawLibrary/default.asp
- http://www.legaltechnologygroup.com/WhitePapers.htm
- http://www.corefacts.net/electronicdiscovery/electronicdiscovery_main.htm
- http://forensic.to/links/pages/Forensic_Sciences/Field_of_expertise/Computer_Investigation/ Highly technical site exhaustively indexing resources on computer investigation.

Rev. 3/1/04