The Judge's Role in Electronic Discovery

Lessons from Case Law and Proposed Judicial Guidelines for the Discovery and Use of Electronic Evidence

by **Larry Johnson**
Director, Electronic Discovery Services
Fios

The business world's shift away from paper documents to exclusively electronic files has been dramatic and inexorable. This evolution is in great part due to the ubiquitous use of e-mail and the Internet.

The reality of our increasingly digital world poses both challenges and opportunities for the bench and bar as we struggle with unique discovery and evidentiary issues posed by electronically stored data.

Issues such as:

- Are there unique features of electronic data requiring changes in Local Rules or the Civil Rules of Civil Procedure to accommodate them?
- With electronic discovery extending to home computers, are privacy issues of a new kind raised?
- If electronic data are unusually difficult or expensive to locate or extract, does that require unique consideration to be given to "overly broad" and "burdensome" objections?
- What can judges do to take advantage of the potential inherent in digital data to streamline the pre-trial and trial processes?

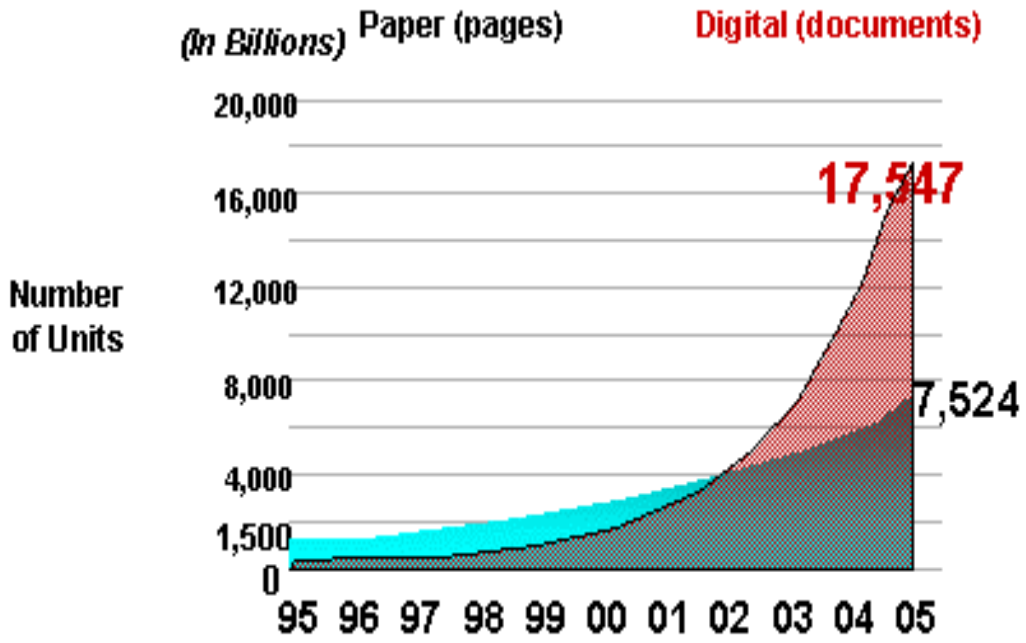
In short: What guidance can judges give the bar in formulating rules and protocols for the exchange and handling of electronic evidence?

These questions, as well as recommended answers, are addressed in this white paper.

The Tsunami Waves of Data

The ease with which electronic documents can be duplicated, transmitted and stored makes them as prolific as the ever-multiplying brooms of Walt Disney's Sorcerer's Apprentice in that classic movie, *Fantasia*.

The following chart, based on predictions made in 1998, shows that by 2005, electronic documents generated in commerce will outnumber paper printouts by almost 3-1.[1]



In today's digital world, it is impossible to conduct complete discovery of potential evidence in the custody of the opposing side if discovery is limited to paper documents only.[2] Too many

[1] Source: Xplor International Document Strategies Conference keynote address, February, 1998; *Documents, Technology and People: Designing a Document Strategy*. Craine, K, 1999 (book manuscript). More recent data suggest the crossover point has already been reached.

[2] It is black-letter law that electronic files are discoverable, even if paper "equivalents" have been produced, since electronic documents contain within them unique metadata in addition to content. *Public Citizen Inc. v. Carlin*, No. 96-2840 (PLF) (D.D.C. Oct. 22, 1997); *Tiniken Co. v. United States*. 659 F.Supp. 239 (CIT 1987); and *Armstrong v. Executive Office of the President*, 821 F. Supp. 761, 773 (D.D.C. 1993). FRCP 26 includes in its scope electronic documents. FRCP 26(B) refers to discoverable "data compilations," as does FRCP 34(a), which also encompasses "documents" that include such things as "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, or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served." Under these rules, discoverable material can include not only internal e-mail messages, word-processed documents and spreadsheets, but also databases, payroll records, telephone records, Internet

"documents" exist only as electronic files (e.g. e-mail, e-mail attachments, files downloaded from the Internet). It is conservatively estimated that at least 35% of all business documents are never printed out,[3] and lawyers who accept paper documents over the electronic files that created them miss out on a potential treasure trove of "metadata" contained within those files (see Fios White Paper *Rock, Scissors, Paper...Electrons! Why You Should Insist on Electronic Document Originals Instead of Printouts*).

As litigators "get the message" that electronic discovery is not only cost-effective and efficient, but also unique in the kinds of data it can uncover, courts will be challenged at every stage of the trial process with inevitable issues about how to handle electronic data.

Back to those questions facing trial judges as they make decisions in the realm of electronic evidence.

1. **Are there unique features of electronic data requiring changes in Local Rules or Rules of Civil Procedure in order to accommodate them?**

   Answer: We at Fios think so, at least as far as the following issues are concerned:

   a. Avoiding spoliation of electronic evidence.

      Electronic evidence, unlike paper, is invisible and volatile. But unlike paper, discarded ("deleted") computer files can often be recovered from a computer's hard disk, but often only if done quickly, before the data are overwritten with new data. More important, transient but often highly relevant data exist on hard drives in the form of "electronic garbage" created by software and operating systems, useful data that soon disappear within days of their creation.[4] Time is thus of the essence in preserving electronic evidence by making, as soon as possible, complete, bit-streamed "mirror" images of all storage media for computers that are potential targets of discovery. See the white paper at the Fios Web site: *How to Conduct On-Premises Discovery of Computer Records*, by Joe Kashi, ABA Law Practice Today.

---

communications, computer graphic images, digitized photo files and any "data compilation" stored on magnetic disks, optical disks, hard disks, back-up tapes and other electronic storage media

[3] Source: "What About 'Deleted' Files Still Subject to Discovery?" *The New Jersey Lawyer* (May 6, 1996).

[4] Much of what makes "computer forensics" possible relates to security holes inherent in Microsoft Windows and Microsoft Office applications. For example, a large chunk of a hard drive is typically reserved as pseudo-memory in what is known as the "swap" file. When you multitask with a number of programs running at the same time, space is made available for the currently chosen application by dropping portions of programs currently "on hold" out of RAM memory and onto this large scratch-pad "swap" file. Properly examined, your "swap" file can reveal passwords, e-mail you sent, revisions made to a Word document, and so on. Similarly, all kinds of files are generated by Windows when you go browsing the Internet, some of which may be known to you (histories, cookies), others not (the index.dat file that tracks where you've been, kept under Temporary Internet Files in the Windows directory and very difficult to eradicate).

But the Federal Rules of Civil Procedure, along with its state civil procedure cousins, are not set up to respond quickly to meet the need for early capture of electronic data, even with the relatively "short-fuse" provisions of FRCP 26(a).

Although there are changes coming soon in FRCP 26,[5] the amended rule will be largely ineffective in preventing the spoliation of electronic evidence.[6] Though Rule 26(a) will no longer be an option that the U.S. District Courts can choose not to adopt, the revised rule leaves open possibilities for significant delays. It requires of all federal litigants that they disclose to their opponents any evidence which a party will use in, or "may use to support" its case in chief "or in any manner for motion or further discovery practice." This includes "a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." Electronic evidence is clearly encompassed in this description of what is to be produced.

Assembling all evidence required by FRCP 26(a), both paper and electronic, has to be done no less than fourteen days before the Rule 16(f) scheduling conference. But the scheduling of that conference may come weeks or months after a lawsuit has been commenced, and absent extraordinary *ad hoc* efforts from the court or counsel, valuable electronic data will by then be irretrievably lost.

Nor do the items raised in FRCP 16(b) (1) through (6) speak specifically to the unique measures that should be taken to preserve electronic evidence.[7] Since it can be anticipated that electronic discovery will become increasingly the rule rather than the exception in civil cases, protocols should be established through local rule or further amendment of FRCP 16 and 26.

To sum up: Courts need to set and enforce consistent guidelines for the swift preservation of electronic data, such as set forth in attached Appendix A.

b. <u>The other side of the FRCP 26(a) coin: there's not enough time to assemble all the potentially discoverable electronic data</u>.

---

[5] The United States Supreme Court submitted prescribed changes in the Federal Rules of Civil Procedure (FRCP) to the House on April 17, 2000. The changes included significant changes to FRCP 26 restricting the scope of discovery, as well as to FRCP 30 and 37. If Congress takes no action, the Rules will become effective on December 1, 2000.

[7] Rule 16(b)(6) does provide for a court's response to "any other matters appropriate in the circumstances of the case," but we submit that electronic evidence discovery issues should not be treated on an *ad hoc* basis, but in accordance to guidelines (such as set forth in Appendix A) that present and future litigants can reliably use to prepare for (or avoid) litigation.

> Electronic files are also distinguishable from paper in that storing vast numbers of them does not take up physical space beyond the storage media they are kept on. It is also much easier to copy and distribute electronic files, so that one computer "document" can reside in dozens of work stations in a network, in untold numbers of computers of recipients of e-mail, and redundantly on numbers of floppy disks, and backup and archive tapes. While Rule 26(a) allows too much time to pass for the effective prevention of spoliation, on the other hand it does not provide enough time for a major enterprise litigant to locate, retrieve, isolate and analyze gigabytes or terabytes of data, much of which may have been preserved for decades without a single thought given to its content, relevance or cost of reconstruction (especially if the hardware or software needed to read it no longer exists!).

To illustrate just how long it can take to assemble some electronic data, take the often-encountered situation where archived "legacy" data have to be examined and produced. This is usually data kept for years on backup tapes, with no clues left current IT staff about how to restore them. That was the problem one party had in the case of *Sanders v. Levy,* 558 F.2d 636, 649 (2nd Cir. 1982). There the court required a new program to be created to extract the requested data and to translate them into usable form, all at the producing company's time and expense. The court explained:

> "Computers, which in general make information more readily available, may occasionally make information more difficult to discover. Even where a party adapts his computer software strictly in accordance with legitimate business purposes, complex electronic processes may be required to extract information which might have been obtainable through a minimum of effort had different systems been used. If the information demanded is such as the respondent might reasonably have expected to be required to make available for public examination or for use in the judicial process, it seems not unfair to require production of the information albeit necessitating special programming."

In other words: You created and kept the data, so you bear the risk of having to turn it over in intelligible form if it turns out to be useful to a party in litigation.[8]

---

[8] In accord is *Daewoo Electronics Co. v. United States,* 650 F.Supp. 1003, 1006-7 (CIT 1986). The case included claims which involved discovery of data sought from the United States Department of Commerce. The data proved to be in a format that was not readily decipherable by the requesting party. The Department of Commerce was ordered to provide data and information about how the data could be made accessible by a computer, as well as such cooperation and reasonable assistance as needed to enable the discovering party to process the computerized data, "including, but not necessarily limited to, conferring with ... counsel and an automated data processing ('ADP') expert."

At any rate, it is obvious Rule 26(a) cannot be satisfied in short order when problems with electronic data conversion present themselves. With paper one can always direct an adversary to a warehouse full of boxes; an equivalent option is not reasonably available with electronic data, since all the potentially relevant information on a hard drive cannot be physically segregated and parceled out.

2. With electronic discovery extending to home computers, are privacy issues of a new kind raised?

In *Northwest Airlines, Inc. v. Teamsters Local 2000, et al.,* 163 L.R.R.M. (BNA) 2460, (USDC Minn. 1999), the court ordered that the home computers of two Northwest Airlines employees be subjected to the copying of their hard drives for analysis and retrieval of potentially relevant evidence relating to an alleged illegal "sick-out" that the company believed was being orchestrated by members of the Teamsters union. Northwest filed a motion for discovery of materials that might prove that the local union had in fact encouraged such activity, and it requested searches of the hard drives of the office and home computers of union officials. Northwest also requested searches of the home computers of non-union employees, including Kevin Griffin and Frank Reeve, who for their part moved for a protective order denying or limiting access to "computer hardware and information and communications which may be contained on computer hard drives." They believed searches of their computers fell outside of the scope of the lawsuit, which focused on whether union officers had sanctioned the alleged illegal sick-out.

The case is unusual in that the court appointed Northwest Airlines' expert, Ernst & Young, to act as essentially *its* witness, even though it had been hired by Northwest to serve in the case as its expert. The magistrate ordered Ernst & Young to image-copy the hard drives and pick its own search terms in a search for relevant evidence; then, if it found any, it was to turn such evidence over to the defendants, who could then make privilege and work product claims in withholding some or all of the evidence Ernst & Young found. But under the protocol ordered by the magistrate,[9] both plaintiff and defendants were relegated to secondary, reactive roles in the electronic discovery process.

In their appeal of the magistrate's ruling, defendants Griffin and Reeve filed a Memorandum In Support of Appeal of Defendants Griffin and Reeve from Order Requiring Them to Submit to a Search of Their Personal Computer Equipment. It contains this recitation of what happened in the case and their objections to the protocol ordered by the magistrate:

> "…Defendants Griffin and Reeve argued that they had conducted their own search of their hard drives, and that, because the computers had been used mostly for private and not work-related purposes, they contained a vast array of personal material that should not be subject to inspection by strangers. The attached affidavits of Griffin, ¶¶ 3, 13, 14, and Reeve, ¶¶ 4, 8, provide details concerning the nature of these private contents. As a fallback position, Griffin and Reeve suggested that, if the Court accepted Northwest's

[9] The text of that protocol is attached as Appendix B to this white paper.

> demand for a global search of their computers, defendants should be allowed to pick their own computer professional to conduct such an examination, instead of being forced to turn over their entire hard drives to an entity selected by and responsible only to Northwest.
>
> Defendants forcefully argued that the normal course of discovery is to allow each party to search their own documents for relevant material, and not to turn all of their papers and electronic records over to a stranger to conduct the review for them. The only exception, defendants argued, is where evidence is presented, and the Court finds, that relevant documents have been deliberately withheld or destroyed, in which case it might be appropriate for a Court to order a third party computer search. However, defendants pointed out that there was no evidence of such destruction of relevant computer documents, and hence, they argued, the precedents required denial of Northwest's demand that its own agents be allowed to copy and search their computer hard drives and other equipment."

These are compelling arguments, but there was some justification for what the magistrate was trying to accomplish: to get as much data assembled as quickly as possible to determine whether a temporary restraining order should issue. To that end he ordered Ernst & Young to perform an impossible task: capture, retrieve and deliver all potentially relevant data from the hard-drives within 24 hours.

> "… noting that the airline's attorneys had just been hit with an avalanche of more than 6,000 documents from Ernst & Young, Northwest attorney Timothy Thornton pleaded for more time to review them. 'I think everybody was a little naive when we felt we could just dive into these computers and make it simple,' he said."

Michael J. McCarthy, *Privacy: Can your PC be subpoenaed?* Wall Street Journal, May 24, 2000, at A1,reprinted in ZDNet News, (http://www.zdnet.com/zdnn/stories/news/0,4586,2576340,00.html)

Practical considerations aside, however, not only did the magistrate in the Northwest Airlines case deprive the litigants of the opportunity to review their own documents and decide in good faith what to produce, he also put Ernst & Young in a position where it had a clear conflict of interest. Ernst & Young is Northwest's accounting firm, [10] and it was also retained by some of Northwest's lawyers to do their computer analysis of the data which Ernst & Young was supposed to cull as a neutral party. [11] The judicial system, ever vigilant to monitor conflicts of interest in the lawyers who serve it, failed to see in this instance the impropriety in the conflict of interest that was furthered by the magistrate. [12]

---

[10] *Privacy: Can your PC be subpoenaed?* id.
[11] *Privacy: Can your PC be subpoenaed?* id.
[12] The magistrate's protocol, Appendix B, is no less offensive because some, but not all, defendants agreed to it.

Also sobering are the privacy implications of the Northwest case and its chilling effect on free speech. The Berkman Center for Internet & Society at the Harvard School of Law reviewed the case (http://cyber.law.harvard.edu/digitaldiscovery/digdisc_library_1.html) and came up with these penetrating questions that give pause for thought:

> Do people have different expectations of privacy regarding e-mails and documents composed on home computers versus computer equipment used at work?
>
> Is it legitimate for an employee who expresses support for a sick-out or strike on a publicly accessible website not to expect to become the target of further investigation?
>
> Was Northwest's decision to cast such a broad discovery net tactical? What might be the advantages of including rank-and-file members in a discovery request?
>
> Given the privacy implications, should the ruling judge have considered whether all requested targets of discovery were relevant to Northwest's actual complaint? Would such differences in expectations of privacy be legitimate?
>
> How analogous is electronic file discovery to wiretapping? What are the important similarities? What are the important differences?

These questions become more compelling when it is the government itself that is the party seeking to find evidence on the home computers of individual citizens:

"As people commit an ever-growing pile of information to computers, their hard drives are becoming a digital mother lode for lawyers. The issue moved into the spotlight when Kenneth Starr's prosecutors scavenged Monica Lewinsky's computers and published what they found, including e-mail messages to friends and unsent drafts of letters."[13]

Thus, beyond the issues posed by the unique nature of electronic evidence, the very sources and means by which it can be extracted give rise to several fundamental public policy issues that will push the courts into adopting comprehensive, objective and, above all, fair protocols to deal with them.

3. **If some electronic data are unusually difficult or expensive to locate or extract, does that require unique consideration to be given "overly broad" and "burdensome" objections?**

   a. Burden

[13] *Privacy: Can your PC be subpoenaed?* id.

As noted *supra* in the commentary of the *Sanders v Levy* and *Daewoo* cases, burdens posed by large amounts of data or the difficulty in making them readable may be dismissed because those burdens come self-imposed in the absence of electronic retention policies that would potentially eliminate or reduce the size of such accumulated information. There may be inherent in this insouciance a recognition that thousands of pages of electronic documents can be stored on a hard drive no bigger than the size of a paperback book,[14] so that assembling, copying and transmitting electronic files is no appreciable *time* or *physical* burden. Whether there is a *financial* burden to consider, however, and who bears the cost of it, appear to turn on the facts of individual cases.[15]

b. Overbreadth

There is a tendency in electronic discovery for lawyers to engage in what we call the "false overbreadth objection" to image-copying of hard drives, where a process which normally only sets the *foundation* for *possible* future electronic discovery is confused with an attempt to discover everything contained in the imaged copy. It is not uncommon for judges and lawyers to misunderstand the purposes behind an imaged copy of a hard drive.

One such purpose we have already noted: the avoidance of spoliation. The other aspect to imaged copies is this: only with an imaged copy is "computer forensics" at all possible – all the techniques that can be employed to recover deleted files, hidden file fragments, and that "electronic garbage" of slack, swap files, and all the rest. Thus, clarity must

[14] Or even smaller. IBM will be selling its new "Microdrive" to the public, beginning September, 2000. The size of a quarter, for use in hand-held "Pocket PC's," it will be able to contain up to a gigabyte of data, enough, IBM claims, to store 1,000 high-resolution photographs, a thousand 200-page novels or nearly 18 hours of high-quality digital audio music.

[15] For example, see *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 98 S.Ct. 2380, 57 L.Ed.2d 253, Fed. Sec. L. Rep. P 96,470 (U.S.N.Y. Jun 19, 1978). "The fact that part of records necessary to identify class members was kept on computer tapes did not justify imposing on defendants, who had the right to control the tapes and who were ordered to make them available to plaintiffs, the resulting identification expense, especially absent an indication or contention that defendants acted in bad faith to conceal information; also, a defendant is not to be penalized for not maintaining his records in the form most convenient to some potential future litigants whose identity and perceived needs could not have been anticipated." The opinion goes on to say: "In some instances, however, the defendant may be able to perform a necessary task with less difficulty or expense than could the representative plaintiff. In such cases, we think that the district court properly may exercise its discretion under Rule 23(d) to order the defendant to perform the task in question. As the Nissan court recognized, in identifying the instances in which such an order may be appropriate, a rough analogy might usefully be drawn to practice under Rule 33(c) of the discovery rules. [footnote omitted] Under that Rule, when one party directs an interrogatory to another party which can be answered by examination of the responding party's business records, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to" examine and copy the records, if the burden of deriving the answer would be 'substantially the same' for either party. Not unlike Eisen IV, this provision is intended to place the 'burden of discovery upon its potential benefitee.'" At 356, 357 of 437 U.S.

reign on this point: the bit-by-bit, mirror-image copying of storage media such as hard drives is *only in preparation for possible discovery, and not discovery itself*.[16]

If lawyers intend to overreach and claim a discovery right to the other side's imaged copies of computer storage media, then an objection for overbreadth is obviously appropriate. The discovery rules were never meant to give a party free rein to ask for *everything* the other side has. But lawyers who intend to thwart the entire imaging process at the outset with overbreadth objections, especially when it is clear that the images are only meant to preserve evidence and provide a platform for limited discovery from there, cry with crocodile tears.

The bottom line: Imaged copies of hard drives must be made to avoid spoliation claims; months from the start of a lawsuit, data that might have been thought irrelevant at the beginning could suddenly become relevant as issues are narrowed, new parties enter the case, or new issues emerge. If an imaged copy is not kept somewhere, preserving the evidence in amber, the electronic evidence will quite likely be lost, at least in part, in the normal course of business. Second, at any point in a lawsuit, looking for clues or fraudulent behavior, or resurrecting evidence to prove a course of conduct (innocent or otherwise), may require computer forensics to "dig up" the evidence out of the imaged copies.

Other than to achieve those limited purposes, provision should be made to protect the privacy of litigants and keep discovery within the boundaries of the discovery rules, meaning that the imaged copies themselves are out of bounds for direct discovery (though always available for *in camera* inspections when a party is suspected of withholding evidence).

Judges can play an important role in providing uniformity and consistency to this process, as outlined in the suggested proposed guidelines, Appendix A.

4. What can judges do to take advantage of the potential inherent in digital data to streamline the pre-trial and trial processes?

This paper has focused primarily on the unique nature of electronic evidence, and how that has promoted unique if not always salutary approaches to digital discovery. Courts

---

[16] Failure to image-copy a drive could get a party to litigation into a lot of trouble. In *Gates Rubber Co. v. Bando Chemical Indus., Ltd*., 167 F.R.D. 90, 112 (D.Colo. 1996), the expert for Gates Rubber Voorhees "failed to capture important information because of an inadequate effort. In using Norton's Unerase, [the expert] unnecessarily copied this program onto the Denver computer first, and thereby overwrote 7 to 8 percent of the hard drive before commencing his efforts to copy the contents." Imaging Bando's hard drive would have prevented this destruction of evidence. "Gates had a duty to utilize the method which would yield the most complete and accurate results. .. In these circumstances, Gates failed to preserve evidence in the most appropriate manner." Accordingly, sanctions were imposed on Gates.

have the opportunity to become more creatively involved in *how* electronic evidence is discovered so that the end product – evidence to be used at trial – can be seamlessly produced from the tools litigants use to cull that evidence from the oceans of electronic data produced in discovery.

We at Fios, for example, have developed software that assigns a unique FENS™ number (Fios Electronic Number System) to each electronic document, so that when used in pre-trial submissions of a party's list of intended exhibits there is a quick and easy reference that the court and other litigants can use to identify the precise documents, rather than making a huge bundle of photocopies to accomplish the task.

Other software licensed to Fios can also identify duplicate digital documents that other parties may be submitting as proposed evidence as well. Unnecessary duplicates can be eliminated by comparing them with a highly reliable "MD5 hash comparison" which finds bit-by-bit, byte-by-byte identity between documents with a reliability factor of 2^{128}.

Further, Fios' proprietary software converts over 360 different file formats to standard HTML documents that are searchable and viewable on a secure Internet Web site. These documents are in turn linked to the "original" document which, when necessary, can be viewed in its native application environment. This means that during the trial of a case, all counsel and the court can have identical access to uniformly identified and retrievable trial exhibits. These exhibits can be readily projected through the monitor ports in laptops onto a courtroom screen where the judge and jury can see the exhibits comfortably when used at trial.

These are but a few of the advantages to digitized evidence harnessed by software (including paper documents that have been imaged and merged into databases containing the same kind of images generated by Fios software from electronic source files).

APPENDIX A

Proposed Judicial Guidelines

Whether through Special Master appointment per FRCP 53,[17] local rule, or a supplement to FRCP 26 and 34 and their state equivalents, we propose the following guidelines to be used by judges and magistrates when dealing with electronic discovery issues:

1. Absent a showing indicating a different course of action, the parties shall have image-copied (i.e. make bit-stream, mirror images) of the storage media of all computers which can be anticipated to be subject to discovery requests from other parties to the litigation, including hard drives, floppy disks and backup tapes.

2. These copies shall be made preferably prior to, but no later than concomitant with, the filing of the complaint in the lawsuit in the case of the plaintiff or plaintiffs, and upon receipt of service of process and the retainer of counsel in the case of all other parties.

3. Each party shall retain and keep in a safe and secure place all such image copies described above. [*Optional: Where the cost of duplicating such image copies is reasonable, such duplicate copies shall be filed with the registry of the court.*]

4. Where a party seeks to explore or copy the contents of the storage media used on the personal home computer of a person who also owns that computer (as opposed to its having been provided to him or her as a convenience to his or her employer), a hearing shall be had to determine whether the likelihood of potential evidence uniquely available on that computer outweighs the privacy expectations of that person. If not, that computer shall not be available for discovery purposes; otherwise, it is to be imaged with due dispatch, following the guidelines set forth herein.

5. The parties shall collaborate and, if necessary, make available for the court's use compatible software and hardware for the retrieval, analysis and organization of electronic data. Electronic data shall be processed in such a way that they can be readily and uniformly identified in all pleadings, including those portions of proposed pre-trial and trial orders that deal with the identification of exhibits. Further, electronic files will be processed in such a way that they can be printed or viewed on computer monitors and used in the presentation of evidence at trial, including, where appropriate, presentation or use of electronic documents within their native software applications.

---

[17] FRCP 53(b) appears to discourage the appointment of Special Masters for other than limited purposes: "A reference to a master shall be the exception and not the rule. In actions to be tried by a jury, a reference shall be made only when the issues are complicated; in actions to be tried without a jury, save in matters of account and of difficult computation of damages, a reference shall be made only upon a showing that some exceptional condition requires it. Upon the consent of the parties, a magistrate judge may be designated to serve as a special master without regard to the provisions of this subdivision."

Appendix B (verbatim from court file)

PROTOCOL FOR INSPECTION AND COPYING OF COMPUTER
AND COMMUNICATIONS EQUIPMENT
(attached to Court Order dated March 2,2000)

1. Place of Production. Any discovery requests and/or subpoenas issued by Northwest for equipment shall specify that the equipment will be produced at the offices of Ernst & Young nearest to the site of the equipment. Northwest will advise you further, if, at the request of any respondent, or by Order of the Court, alternative arrangements are to be made for you to review the equipment either at the site where it is located or at some other site.

2. Minimize Disruption or Interference. Consistent with the schedule of this litigation, you shall endeavor to conduct your inspection to the extent possible, in a manner which is least intrusive or disruptive of the normal activities or business operations of the person or organization producing the equipment.

3. Only Ernst & Young to Review. When any equipment is produced to you, the only persons authorized to inspect or otherwise handle such equipment shall be employees of Ernst & Young assigned to this project. No employee of Northwest Airlines, the International Brotherhood of Teamsters of Local 2000, or other named parties, or their respective counsel, will inspect or otherwise handle the equipment produced.

4. Receipts. Your personnel should provide a receipt for the equipment when it is delivered to you, including a description of the type of equipment, computer manufacturer, model number and serial number; hard drive manufacturer, model number, serial number, and MAC address wherever possible. Likewise, you should obtain a similar receipt when you return the equipment. Ernst & Young should document the chain of custody of the equipment and of any copies of information drawn from the equipment.

5. Limited Scope of Inspection. It is understood from your representations that the standard practice among experts in computer forensics is to make a “mirror image” of any disc drive, or other storage device and then to utilize search methodologies to locate responsive words, phrase [sic], data, documents, messages or fragments thereof {[sic]hereinafter “Data”) contained on the mirror image. The Court has limited discovery to the period between April 1, 1999, and February 8, 2000. In order to protect the privacy interest of the person producing the equipment, except to the extent necessary to search for responsive Data, you shall not read or review Data on the equipment which does not fall within the discovery period and does not relate to the persons or subject matter listed on Attachment A to these instructions. Ernst & Young shall retain custody of the mirror image until conclusion of this litigation, at which time you shall destroy the mirror image and shall issue written confirmation of that fact to the Court and to the person or organization who produced the equipment.

6. Produce Copies of Responsive Information. Whenever your inspection of equipment identifies Data that you deem to be responsive to Attachment A, you shall designate the item on a checklist/index. The listing form shall contain a line for each item of data followed by separate spaces/boxes which may be checked (by defendants only) to designate any objections based upon (1) privilege; (2) negotiation or strike strategy; (3) relevance; (4) other (specified). You shall make three paper copies of each such item, retaining one copy for your records and delivering one copy, along with the prepared checklist, to the attorney representing the party to whom the date [sic] belongs. Upon notification by defense counsel you shall release particularly identified documents to counsel for plaintiff Northwest. Copies of documents not released to Northwest shall be retained by counsel for safekeeping pending determination of discoverability. Upon request of the person producing the equipment, you may provide to that person a copy of any document you have copied for Northwest. You shall not otherwise copy, or disclose, the contents of the equipment.

7. Qualification of Personnel; Verification of Procedures. You shall be responsible for ensuring that all personnel assigned to this project are qualified and experienced in the field of computer forensic investigations and operate under the direction and control of one or more individuals qualified to serve as expert witnesses on the subject of computer forensic investigations. You shall also be responsible for confirming in writing, and testifying under oath, if necessary, that you have strictly followed the foregoing procedures.

8. No changes to these Procedures Without Written Notice. There shall be no change in the foregoing instructions without prior written notice to the parties. Please confirm such notice before accepting any propose [sic] changes to these procedures.

9. Acknowledgement and Agreement. Please confirm by an authorized signature below your receipt of and agreement to be bound by, the foregoing procedures.

Accepted and Agreed:

_____/s/_____
Mark Petersen
Partner

Ernst & Young

ATTACHMENT A

1) All data discussing, concerning or relating to Northwest flight attendants calling in sick, being unavailable for contact by crew scheduling, flying high time or not flying high time, or failing to report to work because they claimed they were sick or might claim they were sick between December 1, 1999 and February 8, 2000.

2) All Data discussing, concerning or relating to any component of a HAVOC campaign, featuring a planned or actual sick-out before release by the NMB by Local 2000, its subordinate units, or Northwest flight attendants, acting collectively, before expiration of the status quo period.

3) All Data discussing, concerning or related to sick calls or to any concerted sick-out, strike, slowdown, work-to-rule, or other job action by Northwest flight attendants before release by the NMB sent to or from or generated by:

a) The HAVOC Committee, by HAVOC Coordinators or volunteers, or by any other individuals acting on behalf of the HAVOC committee, or

b) The Contract Action Team, or by Contract Action Team officials or volunteers, or by any other individuals acting on behalf of the Contract Action Team, or

c) The Rank and File Action Team, or by Rank and File Action Team officials or volunteers, or by any other individuals acting on behalf of the Rank and File Action Team, or

d) Local 2000, its subordinate units, or any Northwest flight attendants, acting collectively, before expiration of the status quo period, or

e) Any off [sic] the following individuals or e-mail address [sic]:

[list of names with e-mail addresses, omitted here…ed.]