

Minnesota State Bar Association
Continuing Legal Education

The Litigator's Annual Short Course

New Developments in Electronic Discovery

George Socha

Halleland Lewis Nilan Sipkins & Johnson
220 S. Sixth Street, Suite 600
Minneapolis, MN 55402
612.204.4134
gsocha@halleland.com

© 2003 George Socha, all rights reserved

I.	How Electronic Discovery Issues Arise in Every Type of Case	1
A.	What Is Electronic Discovery? A Brief Introduction.....	1
B.	What Type of Cases Might Involve Electronic Discovery.....	1
II.	Obtaining Information on Your Opponent’s Computer	2
A.	Finding Help	2
1.	General Sources of Information	2
2.	Computer Forensics Service Providers.....	2
3.	Electronic Discovery Service Providers	3
4.	Automated Litigation Support Providers.....	3
5.	Accounting Firms and Security Firms	4
6.	Computer Forensics/Electronic Discovery Software Providers.....	4
7.	Automated Litigation Support Software Providers	4
8.	Specialized Search Tools	4
B.	Identifying and Preserving Electronic Information.....	5
C.	Requesting Electronic Information	5
D.	Exchanging Electronic Information	6
E.	Assessing Electronic Information	7
1.	Did You Get All the Data?.....	7
2.	Did the Data Come From the People You Thought It Would?.....	8
3.	Look for “Hidden” Data.....	8
4.	Test the Data	9
5.	Work the Data	10
III.	Cost as a Factor Affecting Electronic Discovery.....	10
A.	How Much Will This Cost?.....	10
B.	Containing Costs	11
C.	Determining and Controlling Who Pays.....	11

I. HOW ELECTRONIC DISCOVERY ISSUES ARISE IN EVERY TYPE OF CASE

A. What Is Electronic Discovery? A Brief Introduction

Electronic discovery is the process of gathering and working with electronic files during a lawsuit. The electronic files could come from your own client, from opposing parties, from expert witness, or from third parties. The process relies on all the traditional discovery mechanisms used for paper-based discovery – informal discovery, interrogatories, requests for production of documents, depositions, and the like. It differs, however, in its focus. For the most part, traditional discovery looked at information stored on paper or in the mind. Electronic discovery focuses on information that has been committed to some form of electronic storage medium.

A few years ago, electronic discovery was rare and for good reason. Most information was not stored in computers. Floppy disks were relatively new, CDs and DVDs unheard of. Information that was “born electronic” – created on a computer or similar device – or that had been converted from paper to electronic form was not regarded as reliable or useable in a courtroom; records retention personnel did not consider computer-based information as official records; archivists did not consider information stored in electronic form to part of the range of materials that should be preserved for posterity.

All that has changed. Almost all of use create information in electronic form daily with PCs, PDAs, cell phones, and a plethora of other electronic devices. According to a study published by the University of California at Berkeley in 2000, 93% of recorded information was being created in digital format and much of that was never being committed to paper.

At the same time that the volume of information in electronic form has increased greatly, the costs of gathering and working with electronic materials during discovery has dropped substantially. The number of vendors catering to this area had gone up, their skills have improved, and the tools they have at their disposal have gotten better.

B. What Type of Cases Might Involve Electronic Discovery

Electronic discovery can be an issue, a problem, and a potential boon in any case. Whether it is, depends more where information has been stored than on the type or size of case.

Whether a case warrants electronic discovery is a separate question, and one without a simple answer. Part of the answer depends on the size of the case and the amount of money at issue – no news there. A large part of the answer, however, hinges on how important the electronic information likely will be, how costly it will be to get and work with, and how effectively it can be presented to the ultimate decision makers.

II. OBTAINING INFORMATION ON YOUR OPPONENT'S COMPUTER

A. Finding Help

If this is your first foray into electronic discovery, you should get help from someone who already has some experience in the area. Even if you have dealt with electronic discovery in the past, you still may want outside assistance.

Following are lists of electronic discovery vendors to consider, arranged by the types of services offered. These lists are not at all comprehensive but they provide a solid starting point.

1. General Sources of Information

There are several sources general information about computer forensics and electronic discovery. One can search on Google using terms such as “electronic discovery,” but the results are likely to be overwhelming. Most of the sites listed in the following paragraphs provide useful information, but you should also consider the following:

- California Civil Discovery Law: Discovery of Electronic Data (californiadiscovery.findlaw.com/electronic_data_discovery.htm)
- Federal Guidelines for Searching and Seizing Computers (www.epic.org/security/computer_search_guidelines.txt)
- Harvard Law School Digital Discovery Project (cyber.law.harvard.edu/digitaldiscovery)
- www.kenwithers.com (www.kenwithers.com)

2. Computer Forensics Service Providers

These companies help identify potential sources of relevant computer files, make forensically appropriate copies of those files, and convert and filter the files before delivering them to you.

Minnesota Presence

- Computer Forensic Services (www.compforensics.com)
- Cyberensics, LLP (www.cyberensics.net)
- Kroll Ontrack (www.krollontrack.com)
- Merrill Corporation (<http://www.merrillcorp.com/dms>)
- RenewData (www.renewdata.com)

Outside of Minnesota

- Attenex (www.attenex.com)
- Computer Forensics Inc. (www.forensics.com)
- Cricket Technologies (www.crickettechnologies.com)

- Daticon, Inc. (www.daticon.com)
- Electronic Evidence Discovery, Inc. (www.eedinc.com)
- Fast Track Litigation Support (www.ftls.com)
- New Technologies, Inc. (www.forensics-intl.com)

3. **Electronic Discovery Service Providers**

These organizations take electronic files gathered by computer forensics services vendors, convert them to formats that can more readily be worked with by attorneys and their support staff, and offer tools to allow those folks to review, organize, annotate and produce the files. Some offer web-based review and analysis tools.

- Applied Discovery Inc. (www.applieddiscovery.com)
- Attenex (www.attenex.com)
- CaseCentral (www.casecentral.com)
- Cricket Technologies (www.crickettechnologies.com)
- Daticon, Inc. (www.daticon.com)
- DolphinSearch (www.dolphinsearch.com)
- Electronic Evidence Discovery, Inc. (www.eedinc.com)
- Fios, Inc. (www.fiosinc.com)
- Merrill Corporation (<http://www.merrillcorp.com/dms>)

4. **Automated Litigation Support Providers**

Over the past few years, automated litigation support companies have been trying to reposition themselves as electronic discovery vendors. They recognize computer forensics and electronic discovery as challenges to their traditional lines of work as well as potential growth areas. They want to be prepared for the day when electronic files demand at least as much attention as paper and are moving rapidly in that direction.

Minnesota Presence

- Merrill Corporation (<http://www.merrillcorp.com/dms>)
- Quorum (www.quorum.com)

Outside of Minnesota

- Daticon, Inc. (www.daticon.com)
- Fast Track Litigation Support (www.ftls.com)
- Techlaw Inc. (www.techlawinc.com)

5. Accounting Firms and Security Firms

The large accounting firms have worked to establish a presence in this arena. Security firms have noticed an opportunity, as witnessed by Kroll's purchase of Ontrack last year.

- Deloitte & Touche (<http://www.deloitte.com/vs/0,1616,sid%253D2018,00.html>)
- KPMG (<http://www.kpmg.com/services/content.asp?l1id=60&l2id=0>)
- PriceWaterhouseCoopers (<http://www.pwcglobal.com/extweb/service.nsf/docid/D579B1FCA2E5100E852568F7001D1ECB>)

6. Computer Forensics/Electronic Discovery Software Providers

Software options are limited for law firms and corporate legal departments that want to gather, organize, evaluate and produce digital discovery themselves.

- Cricket Technologies (www.crickettechnologies.com)
- Electronic Evidence Discovery, Inc. (www.eedinc.com)
- Guidance Software, Inc. (www.guidancesoftware.com)
- New Technologies, Inc. (www.forensics-intl.com)

7. Automated Litigation Support Software Providers

Most, if not all, of the major automated litigation support packages now supposedly can handle information gathered during digital discovery.

- Concordance from Dataflight Software, Inc. (www.dataflight.com)
- Ringtail (www.ringtail.com.au)
- Summation (www.summation.com)

8. Specialized Search Tools

The more ready availability of massive volumes of searchable full text offered through electronic discovery has opened the market to search tools designed to find the computer files that matter the most.

- Autonomy (www.autonomy.com)
- Cataphora (www.cataphora.com)
- DolphinSearch (www.dolphinsearch.com)
- Syngence (www.syngence.com)

B. Identifying and Preserving Electronic Information

Whether a trial lawyer is handling a routine “slip and fall” premises liability case or a multimillion-dollar product liability case, the ability to identify, discover, and analyze computer files and other electronic data can be crucial to the outcome. Federal Rule of Civil Procedure 26 (b) and its state counterparts permit discovery of any matter, not privileged, which is relevant to the subject matter of an action. Rule 26(a)(1)(C) specifically contemplates electronic data when it obligates parties to federal actions to provide opponents with copies or descriptions of documents, *data compilations*, and tangible things in the party’s possession, custody, or control. Rule 26(b) makes clear that information sought need not be admissible at trial; it is discoverable if it appears reasonably calculated to lead to the discovery of admissible evidence. Information about the organization and contents of an opponent’s electronic record-keeping system clearly meets this requirement.

Rather than wait for an opponent to provide this information, as soon as counsel suspects that discovering an opponent’s electronic data compilations might prove helpful to the case, the first step should be to issue a notice to preserve and retain the data. This can be done even before commencement of discovery, and may reduce any temptation to lose, hide, or destroy data.

Soon after discovery begins, counsel will gain at least a preliminary idea of the names and titles of people, offices, and departments that may have discoverable electronic data. It is a good practice to supplement the initial general notice to preserve with a more specific request.

C. Requesting Electronic Information

Federal Rule of Civil Procedure 34, and its counterparts in many states, permits a party to serve on another party a request to produce designated documents for inspection and copying. Rule 34 specifically mentions “data compilations” in its list of documents. This request must list the items to be inspected with “reasonable particularity.”

Requests for production of electronic media are routinely rejected as "overly broad" if they are drafted without specific knowledge of an opponent’s system.

In conjunction with requests for production, attorneys can often gain the most useful information by taking the deposition of the opposition’s custodian of *electronic* records, who is typically a middle manager in an information services department. Federal Rule of Civil Procedure 30(b)(6) and its state counterparts allow a party to name as the deponent a corporation, partnership, association, or government agency. The organization so named must designate one or more officers, directors, or agents to testify on its behalf.

D. Exchanging Electronic Information

If at all possible, talk with opposing counsel as early as you can about how the electronic information will be delivered to you. On one hand, you want to make sure that you actually can make use of the data sent to you. On the other hand, you want to do what you can to ensure that you get all the information you need, not just that part that the other side thought you should get or just those parts that were easy to send to you.

You need to get the data onto a medium you can use, if it is not already on one. Data can come on a variety of media, such as data tapes, Zip disks, DVDs, CD-ROM disks, 3.5 inch floppy disks, and 5.25 inch floppy disks.

If you receive electronic data on an 8-millimeter data tape, chances are that you will not have an 8-mm tape drive at your desk. Even if you have a drive, it may not be able to read that specific tape. You need to get the data onto a medium your computer can read, which these days generally means a 3.5 inch floppy or a CD disk. How do you do this? Usually you will need to turn to an outside vendor to copy the files from the tape onto a medium that you can use.

Zip disks are simpler. The cost of Iomega Zip drives (www.iomega.com) is low enough that you can keep one on hand just to copy data from Zip disks you receive (and to copy data to Zip disks when others request data from us on that medium).

CDs are even simpler, as CD drives have become commonplace on PCs. Similarly 3.5 inch disks generally pose no problem.

5.25 inch floppy disks have started to become problematic, as fewer and fewer PCs have the drives in them. Older sizes of floppies can be even more difficult; you almost certainly will have had to engage outside vendors to move the data over to media that you can work with.

Having data on a useable medium is useless unless it also is in a useable format. At times this is not an issue. If the data comes in a format that you already use, then you can begin to work with it as soon as you get it off the media. The formats most likely to be useable without conversion are word processing files (principally WordPerfect and Word files), spreadsheet files (principally Excel and Lotus) and presentation files (principally PowerPoint files).

Even if the data is in a format that appears to be one you already use, conversion may be necessary. The format may be too new. For example, you will not be able to open a Word XL file if you are using WordPerfect 5.1 or even Word 7. The problem is a basic one. When those programs were written, Word XL did not yet exist. As a result, they do not have in them the pieces of code needed to read Word XL files. You will need to find a machine with a word processing package capable of reading Word XL files. Alternatively, you will need to get a program

such as Word for Word that can recognize and work with many different files types.

In a similar vein, you may have to get the data converted if it comes to you in a format that is too old or runs on a different operating system such as Macintosh or UNIX.

You may encounter problems of the WordPerfect-versus-Word ilk. Although simpler files created with one company's software generally can be opened without problem using a competitor's comparable product, this often does not hold true for more complex files. Thus, Word documents formatted using "styles" or containing complex tables may not be fully readable by WordPerfect (the same holds true when going from WordPerfect to Word.)

Once again, it is best to try to work with opposing counsel as early as you can to resolve these issues.

You may get electronic data in a format that you cannot use "out of the box." When that happens, you have to convert the files to a format you can use – or find someone to do the conversion for you. Anyone who has undertaken this task can attest that it is potentially a difficult and painstaking process.

Any time you suspect that you will have to convert data, there are some steps you can take to facilitate the process. Initially, try to get as much information about how the files were created and maintained as you can. Whether you intend to try the conversion yourself or rely on outside resources to get the work done, the more you know about the files the better your chances of a successful conversion. For example, if you receive a ".txt" file that appears to contain information from a database file, try to find out, among other things, the make and model of computer the file came from, the name and version of the operating system the computer ran, the name and version of the database program used, the name of the database file, a list of all fields in the database, and descriptions of each field with the descriptions including the type, length and other characteristics of the field.

Further, get sample printouts if possible. If you get these, they may provide answers to some of the questions listed above. They may show how the data was laid out – and hence how it was used. They also may give clues about electronic data that you should have received, but did not.

E. Assessing Electronic Information

Once you are in a position to work with the electronic data you got from the other side, check to see that the data is what it ought to be.

1. Did You Get All the Data?

Check to see whether you received all the data you should have received. Prepare an inventory of what you received and compare it against what

you requested. This may be as simple as preparing and comparing lists of file names. More likely, however, it will require that you develop short descriptions of the data you received and then match the descriptions with your discovery requests. It may even mean that you will have to closely analyze the data to see whether gaps emerge that indicate some failure by the other side to produce all that it ought to have produced.

You also can search the electronic data for references to electronic files that should have been produced to you but were not. This can be done through a manual review. The manual review can be enhanced if the software you are using to review the data allows you to search for strings of characters. If it does, you can search for filename extensions that are typically associated with the types of files you want to find. Examples include .doc, .htm, .html, .htx, .rtf, .mcw, .txt, .wps and .wpd for word processing files; .csv, .dbf, .dif, .txt, .wk1, .wk3, .wk4, .wks, .wq1, .xls and .xlw for spreadsheet files; and .asc, .csv, .dbe, .dbf, .htm, .html, .mda, .mdb, .mde, .mdw, .tab, .txt and .xls for database files.

If you received spreadsheet or database files in their native format, you can scrutinize them for signs of links to files that were used in connection with the files you got but nonetheless were not produced to you. In a spreadsheet file such as an Excel file, this might mean searching the cells for extensions such as the ones listed above. It also can mean checking the “properties.” If you are asked whether you want to reestablish link when you open the file, that is a clear sign of potentially missing files; keep track of the file names and check to see whether you received them. In a database file such as an Access file, this means closely examining all tables, queries, forms, reports, macros and modules for references to other files.

2. Did the Data Come From the People You Thought It Would?

Files often contain indications of who created them, who worked on them, and who last saved them. If you go to **File | Properties**, you can sometimes find this information.

3. Look for “Hidden” Data

Electronic files often contain “hidden” data – i.e., information that does not show up on printouts of the file – which can potentially prove useful.

Go to **File | Properties** where you may be able to find a host of details about the file that the people sending it to you may not have known went with it. These details can include:

- when the file was created,
- when it was last modified,

- who created it,
- what comments have been added,
- what title was given to the file, whether intentionally or automatically,
- what subjects have been assigned to the file,
- who last saved the file, and
- how many revisions the file has gone through.

In word processing files, look for comments that display on the screen but do not automatically print out. If there are tables containing numbers, check them for formulae that calculate the figures displayed in the tables. If there are objects embedded in the word processing file, such as portions of spreadsheet files, try to ascertain the names of source files.

In spreadsheet files, look at the formulae; these show the true work being done by the spreadsheet file in a way that a printout never can. Check the formulae for references to other files. Look for hidden columns. If the column listing across the top goes “A B C E H,” that means that there are at least three hidden columns – D, F and G – that might contain information of greater value than anything shown. Watch for comments; in Excel 97 these may initially only show up as small red triangles at the upper right corners of cells. Beware of cells that appear to be empty but are not.

In database files, look for explanation of field names or contents; in Access you might find this by looking at the database tables in “design” mode. Look for links to files you did not receive; in Access this might be indicated by small arrows to the left of the table icons. Look for tables, queries, forms, reports, macros and modules that you did not know about. In tables, look for hidden fields.

4. Test the Data

Test the electronic data to determine how complete, how accurate, and how reliable it is. Test the data against itself, looking for inconsistencies.

When feasible, the electronic data can be compared to underlying documents, to determine the completeness, accuracy, and reliability of the data. This comparison can highlight coding errors made when creating the database, such as wrong numbers, wrong dates, and wrong names. It also can reveal categories of information that were not added to the electronic data, which if they had been added, would have affected the results one obtains by searching the data.

Just as electronic data can be compared to underlying documents, so too can it be compared to data in other electronic files, the contents of other documents, and information available through the Internet.

5. Work the Data

What can be done with the other side's electronic data is limited more by lack of imagination than by anything else. That said, two general suggestions can be offered:

Put the data into tools you can use. Spreadsheet programs allow one to perform calculations, prepare pivot tables that quickly summarize data across several dimensions, develop charts to graphically present trends in the data, and map information geographically. Database programs may permit searches or queries of databases in complex and subtle ways, perform calculations, and generate a broad range of reports.

Share the data you receive and the knowledge you glean from it with your client, your experts, and other colleagues, as appropriate. This can enable you to handle your case more effectively.

III. COST AS A FACTOR AFFECTING ELECTRONIC DISCOVERY

A. How Much Will This Cost?

Electronic discovery costs vary greatly. For an unusually frank discussion of electronic discovery costs, see Residential Funding Corp. v. DeGeorge Financial Corp., et al., 306 F.3d 99 (2nd Cir. 2002), which contains a section on the actual or projected costs of electronic discovery work for the various parties to the lawsuit.

At a recent conference on electronic discovery, one of the most-established electronic discovery vendors shared some approximate costs with the audience. They were:

- Cataloging backup tape contents: \$150/tape
- Restoring backup data to hard drives: \$150/tape
- Capturing the contents of a hard drive for evidentiary purposes: \$1,000/drive
- Restoring and analyzing data from the drive: \$2,800 (8 hours at \$350/hour)
- Searching text of drives and similar media: \$1,400 (4 hours at \$350/hour)
- Copying data to DVD, CD or hard drive: \$500 (4 hours at \$125/hour)
- Loading data to litigation support database: \$500 (2 hours at \$250/hour)

These numbers provide a rough guide, but only that. Prices may differ depending on how much work there is to be done and whether travel is required: more work may mean volume discounts, travel will push up costs. Also, in general expect that the more complicated work will be more costly.

B. Containing Costs

Computer forensics and electronic discovery costs can be difficult to contain. Several steps can be taken, however, to keep costs down. They include:

- Educate yourself
- Start early and plan ahead
- Get vendor recommendations from colleagues
- Get competitive bids from vendors
- Get information from the vendor in writing – what the vendor is going to do for you, what it will cost, when it will be delivered to you
- Work closely with the vendor
- Monitor vendor activity closely

C. Determining and Controlling Who Pays

There is not any single rule or set of rules to which one can turn to determine who will pay for the cost of electronic discovery. The most cogent decision to date come a Federal magistrate in the Southern District of New York, Rowe Entertainment, 205 F.R.D. 412 (SDNY 2002). In that case, the magistrate judge outlined eight factors that he considered to be important in determining whether the responding party should bear the costs of electronic discovery – the traditional approach – or whether those costs should be shifted to the demanding party. The factors were:

FACTOR	WHEN REQUESTING PARTY SHOULD PAY	WHEN RESPONDING PARTY SHOULD PAY
Specificity of request	Broad requests	Targeted requests
Likelihood of a successful search	Low likelihood	High likelihood
Availability from other sources	Available	Not available
Purposes behind retention of the materials	Retained only for emergency purposes or through oversight	Retained for current use
Benefits to responding party	Few, if any	Useful for other business reasons or for litigation
Total costs	Substantial	Low
Who can best control	The requesting party	The responding party

FACTOR	WHEN REQUESTING PARTY SHOULD PAY	WHEN RESPONDING PARTY SHOULD PAY
costs		
Who can most easily pay the costs	The requesting party	The responding party

These factors should be viewed only as guidelines. The list is not comprehensive, and in a given case not all of the factors may come into play. The court did not attempt to weight the factors, nor should it have done so.