THE ELECTRONIC COURTROOM

A Collection of Articles

E-Filing in North Carolina, page 2
Attorney's Instructions for E-filing in the appellate level courts of North Carolina

Plugged into E-Filing, page 10
Where it's been, where it's going and how it affects legal assistants.
By Susan Jennen Larson

What Every New Attorney Needs To Know…, page 18
About E-Discovery
By: Rhea Frederick, J.D

Electronic Discovery, page 26
A Brave New World
By Michael P. Zweig and Mark J. Goldberg

ATTORNEY'S INSTRUCTIONS FOR ELECTRONIC FILING OF DOCUMENTS IN THE SUPREME COURT AND COURT OF APPEALS OF NORTH CAROLINA

Electronic Filing allows attorneys to submit their documents to be filed, such as petitions, briefs, and responses, through an electronic medium, rather than a paper medium. This reduces costs to all parties involved, including the taxpayers and the attorneys. We hope this instructional web page is helpful to you. Please feel free to contact either the Supreme Court or the Court of Appeals Clerk's Office with any questions or suggestions.

I'm an attorney and I want to submit my document electronically to the Supreme Court of North Carolina or Court of Appeals. What do I do?

Equipment required:

1. Personal Computer

2. Internet Access

3. Adobe Acrobat-Version 6.0 Full Version. For more information about Adobe Acrobat, go to their website at www.adobe.com. Other pdf writer software include Wordperfect 10 and above, and PDF Creator.

4. Scanner with automatic feeder only if appendix needs to be added to the document.

Internet address: ***www.ncappellatecourts.org*** (You may wish to bookmark this address.)

STEPS

How to submit electronically:

1. Log onto Internet address and click on **Register** in order to register to submit your document. You will receive an email from the Clerk's Office when you are enabled. Once you register and are accepted, you are free to submit numerous documents at any time you would like to both the Court of Appeals and Supreme Court. **Note:** Remember your password and exactly how you submitted your name. The system is case and punctuation sensitive.

2. Next you must **Prepare your Document** to be sent electronically. This involves converting the document to a PDF file using your Adobe Acrobat PDF Writer and scanning in appendix pages to attach to the PDF file.

3. When your document is ready to **Submit**, you can go back to the Internet address and fill out the form on the web by clicking on submit and entering your registered user name and password. Fill out the required information and then upload your file.

If you need **Help**, please call or email the support line at 919-733-6973 or *efiling@sc.state.nc.us.*

REGISTER

ATTORNEY'S REQUEST FOR SUBMISSION

In order to verify that you really are who you say you are, we need you to register, get a password, and be approved to e-file documents with us.

On the Internet, go to the address www.ncappellatecourts.org. Our web page for the Electronic Filing and Document Library will be

displayed on the screen. From this site you can register, submit, browse briefs that have been filed, and do keyword searches.

At the left side, under **User**, click on **Register**. The User Registration screen will appear at the right. Choose whether you want to:

Request a new account or

Login to update your existing account.

If you have never registered, click on **Request a new account.**

Fill in the blanks on the screen. The password suggested on screen may be used, or you may choose one that is more easily remembered. **Note:** You must remember your own password, because the Clerk's Office will not have access to it. Also remember the exact way you filled out your name. The system is case sensitive and punctuation sensitive.

Click on **Submit Request.**

You will be contacted by telephone to verify your identity or we will verify your NC Bar status. After that, you will be notified by e-mail that your request for registration is approved. If you need to expedite your request or have problems with your confirmation, please call us at 919/733-6973. You will usually be approved within the same day as submission, unless your request was received after business hours (8:00am-5:00pm eastern Standard time) or on weekends or holidays.

PREPARE THE DOCUMENT

Now that I'm approved, how do I submit my document?

ATTORNEY'S SUBMISSION

After receiving email that your application has been approved, you may then submit the document to be filed. The completed document must first be processed through Adobe Acrobat v. 5 or 6 to convert it

to a PDF (Portable Document Format) file. Why PDF? This is very important to successful electronic filing because a PDF document can be viewed and printed by anyone even though they do not have the same word processing software that you have. Also, unlike word processor files, a PDF document is very difficult to alter, which increases your document's integrity. The software to view a PDF file is free and readily available via the Internet from www.adobe.com.

Converting the WordPerfect or other Document to be Submitted to PDF Format:

To save the document as a PDF file:

Open the document you want to convert from the word processing application being used (ie. WordPerfect 9 and below, Notepad, MS Word, etc.).

Click on File, Print, in the main menu.

Click on Printer (at the top of print box) and select "Acrobat PDF Writer" from the list of available printers. Note that this process converts and does not actually print. The document will now have ".PDF" extension after the file name.

Click on Print.

"Save As" comes up on the screen. Enter the name of the file and specify the folder or subdirectory where you want to save the file. Then click on "Save."

Close the document and either close or minimize your word processor.

Do you have pages of transcript or additional pages to append to your document? If Yes, read on; if No, then skip down to "When you are finished with the PDF file."

If additional pages are required for the document, such as pages of transcript, orders, Court of Appeals opinion, etc., they will need to be

scanned and inserted or appended to the document.

Place the document or page(s) to be scanned into feeder according to scanner instructions.

Open Adobe Acrobat.

On the toolbar, go to File then click on "Import" and then "Scan."

Accept the default settings and Click on "Scan."

Click on "Select parts of page or View page first" to deselect (it is defaulted on).

Click on "Scan Speed" and choose "faster scan speed" and then "best quality text." Click "OK."

Click on "Scan" and wait while each page is pulled through the scanner and processed.

When the computer says "next page" and "front sheet 2", continue with prompts until finished scanning all pages, and then click "Done."

Wait for the computer to display the document scanned.

Inserting the PDF Document into the Scanned Pages:

While still in Adobe Acrobat, with the scanned pages or document on screen, on the toolbar, click on "Document" and then "Insert Pages."

Click on the arrow at the top to specify the location of the already converted brief or document to be filed (filename.PDF) and click on "Open."

If the scanned pages are to serve as an appendix, change the location to "Before" to specify that the document should precede the scanned pages ("after last page" is the default). Click on "OK."

Moving pages after inserting:

If the scanned pages are to appear at various places throughout the document, they can be moved individually or as a group.

On the toolbar, click on "Window" then click on "Show Thumbnails."

If there are too many thumbnails to be shown at once, opposite click in the thumbnail area and select "Small Thumbnails."

Double click on pages to check the order (double clicking shows the page you double click on).

Click once on the page you want to move. This should highlight the page in blue on the thumbnails. Hold the "Ctrl" button down while you highlight in order to move multiple pages.

Click and drag the page to the position desired.

When you are finished with the PDF file:

On the toolbar, go to "File" and then "Save As" (not "Save"). You use "Save As" because it compresses the document to the smallest size possible.

Name the file and click on "Save."

Be sure to close your document before attaching it in the instructions below.

SUBMIT

OK, my document is ready. What's next?

Filling out the Form on the Web:

When the you are ready to transmit the document, please return to the web address to complete the final step:

http://www.ncappellatecourts.org

Under the **Library** heading, click on **Submit**.

Enter the **User Name** and **Password**. The E-Court Docket Submission screen appears.

Select Supreme Court or Court of Appeals.

Indicate whether a document is to be **filed on an existing case** by entering the case number or whether the **filing is for a new docket** for which there is no number yet.

Click on "**Let's Go**" and fill in the required information to be submitted with your document. Note: If this is an existing case, the data won't have to be re-entered again.

Uploading the File:

At the end of the data-fill section is a **File Upload** section where you must "Select the file you wish to upload." Click on the **Browse** button to go to the directory or folder where you have saved your document and **double click on the file you want to submit** for docketing. The filename will appear in the blank to the left of the Browse button.

Then Click on the **Upload** button to submit your file plus all the accompanying data you have entered.

If you receive a window about security, select the option to continue. Since court documents are public information, the unsecured transmission is acceptable.

To print a copy of the data you have submitted, **click File and Print** in the main menu.

- Your document will be considered filed by the Clerk's Office when it is received. Within the next day or so you will receive an e-mail message giving the exact time and date docketed in our

database.

OK, that involves a few steps, but it's really pretty easy. What do I do if I have questions?

HELP

For additional help with Electronic Filing, feel free to call anyone at the North Carolina Supreme Court Clerk's Office at **919-733-3723** or the Court of Appeals Clerk's Office at **919-733-3561** from 8 a.m. to 5 p.m., Monday through Friday. But remember, you may electronically file at any time of day or night, every day!

If you have comments or suggestions as to how we may improve this process, please e-mail them to **efiling@sc.state.nc.us**, and someone will respond to you and also run your ideas by the staff.

Plugged into E-Filing

Where it's been, where it's going and how it affects legal assistants.

By Susan Jennen Larson

Every court electronic filing project at some point faces a critical question — will attorneys use it? At the December 2003 E-Court Conference in Las Vegas, members of the American Bar Association's electronic filing committee met with vendors and courts to hear their concerns and issues regarding e-filing. The most frequently asked question was: Why won't attorneys use electronic filing systems, and what can we do to get them to e-file? I suspect the decision whether to use electronic filing really lies with legal assistants in many firms. Consequently, I think the question should be rephrased: Why won't legal assistants use electronic filing systems, and what can we do to get them to e-file?

The first step is for all legal assistants to understand where court e-filing has been and where it's going. This article discusses some of the critical issues surrounding e-filing today, and highlights some of the future features that will make the e-filing system much better to use.

In the Beginning

Even though e-filing has been going on in some courts for several years, the technology and concept have not yet matured. The low percentage of courts that have implemented e-filing systems to date have applied limited features and offered e-filing for limited case types. No U.S. courts have implemented all the features e-filing promises for the future, and no U.S. courts have introduced e-filing for all types of filings and exhibits.

In the early years, courts turned to e-filing for class action cases. With large numbers of plaintiffs and endless exhibits, e-filing offered a streamlined way to file and view documents. Parties were given passwords and access rights so they could view all filings online. Documents were hosted on the vendor's system, allowing for quick setup and use for any given court. Fees were charged on a per-document or per-filing basis to cover the technology and hosting costs. LexisNexis was one of the first vendors to develop and host e-filing for class action cases, and continues to offer this type of service today for class action, as well as other types of cases.

Later, another e-filing model emerged allowing courts to install e-filing software on their own hardware. In many respects this has become

the preferable approach because it allows courts to store its e-filed documents in-house and retain control over them. It also allows for easier integration with existing court case management systems and better control over technology development costs. With this model, courts collect their own filing fees, and sometimes add an “e-filing” fee on top of existing fees to help cover the cost of the e-filing technology.

This model also allows courts to integrate their e-filing systems with existing court case management systems. This is an important goal for most courts. As paper documents are filed in court, clerks enter data into case management systems to track things such as filing dates, document names, parties and attorneys. As electronic documents are filed in court, the ideal scenario is to automatically import this data from the e-filing system to the case management system, and any other systems that need the data. Otherwise, clerks will be reviewing e-filed documents and entering the same data into their case management system.

As courts move forward with both of these models, a significant concern is that if courts don’t implement e-filing systems with some uniformity or standards, the end result will be law firms having difficulty adapting their e-filing processes for each court. Large firms filing in multiple courts will have to learn the details of each court’s e-filing system, adding a layer of complexity to firm processes and additional costs for clients.

Standardization Efforts

A number of national efforts are underway to help address the issue of standards and uniformity for court electronic filing systems and processes. The following groups are working together to define and set standards to help courts and vendors move forward with e-filing projects: the Conference of Chief Justices, the Conference of State Court Administrators, the National Association for Court Management, the National Consortium for State Court Automation, Organization for the Advancement of Structured Information Standards and the Global Justice Information Network Advisory Committee.

The “Standards for Electronic Filing Processes” is a document that recently emerged to identify policy standards, functional standards and a conceptual model of the e-filing process. Even though parts of these standards are somewhat technical in nature, they are worth reading for anyone interested in e-filing systems. Readers will find discussions

about e-filing policy, technology and business process issues. For example, the policy standards address:

- the official court record
- technical requirements (Web browsers and XML)
- identification of the sender
- integrity of transmitted and filed documents and data
- court control over documents
- service of filings on opposing parties
- when a document is considered filed
- available hours for e-filing
- remedies when e-filing fails
- maintaining supplementary scanning capability for paper filed documents
- eliminating unnecessary paper processes
- archiving electronic documents

The functional standards address:

- document integrity
- system security
- signatures and authentication
- case/document confidentiality
- acceptance and rejection of filings
- user and service registration
- court payments
- submission of all filings
- case opening filings and subsequent case filings
- service and notice
- judicial consideration of drafts
- clerk review
- court initiated filings
- requests for and responses to requests for case information
- integration with document and case management systems

Another model of e-filing software also is emerging that might help provide a uniform user interface across all court e-filing systems. This model uses a “middleman” service that will accept filings from attorneys and then turn around and package them properly to e-file with any court. This will take the headache away from legal assistants as they try to remember and package e-filed documents differently for different courts. However, it will come with a fee, and that fee will surely have to be passed on to clients.

Important Features of E-filing Systems

Of all the issues addressed by the "Standards for Electronic Filing Processes," a few emerge that are critical to law firms and the courts.

Signatures. How does a law firm or a client sign court documents filed electronically? Of course, they can sign a paper copy and then scan it to "take a snapshot" of the document and signature. Many e-filing systems in existence today rely on this snapshot method, as they allow attorneys to scan documents and submit them in the commonly used Portable Document Format (PDF).

Another well-known approach is the user ID and password. Courts assign a user ID and password to an attorney. Then all documents filed under this user ID and password are trusted to be filed and "signed" by that attorney. This is considered an "electronic" signature, as it provides a completely electronic means for identifying the sender and attaching the sender's identity to the filed documents.

Future e-filing systems will do better than either of these two approaches. They will incorporate a more sophisticated way of signing, commonly referred to as a "digital signature." The concept behind "digital signatures" is complicated, and also commonly referred to as "digital certificates." It involves many parties working together to assign, use and recognize digital signatures across many environments — not just court e-filing.

The first step is for an authoritative body to assign a digital certificate, which involves a pair of codes called a "key-pair." One of the keys is private, and one is public and published in a registry for public use. Using the appropriate software, an individual can use the private key to "sign" a document prior to sending. The originating software, such as Adobe Acrobat and Microsoft Word, uses the private key and a mathematical formula called a "hashing algorithm" to produce a "hash" number, which is attached to the document. The document also can be encrypted at this time, if desired. The private key isn't sent or visible on the document. However, an image of the sender's signature can be automatically "stamped" on a document when the sender enters the private key.

Later, when a court or other individual receives a signed document, a "look-up" is performed against the public key registry to find the sender's public key. The public key also can be stored within a court database so a look-up isn't required every time a document is

received. Once obtained, the public key is applied to the hashing algorithm and another "hash" number is calculated. If it matches the first "hash," then it can be determined that the document was sent and "signed" by the person who claims to have sent it.

To put such a system in place is no small matter, however. A single authority for issuing signatures must be established, and software applications must be programmed to use these types of signatures. Attorneys must initially sign up to receive a digital certificate, and then must not disclose the private key.

This raises an interesting question for legal assistants — should they know an attorney's private key if they are responsible for preparing papers for that attorney? It would certainly be inconvenient to have to ask attorneys to come over to the preparer's computer and enter the private key. It would be more convenient for the preparer to present the papers for final review and then enter the attorney's private key. However, in the paper world, legal assistants don't forge signatures and the entering of another's private key would be the same as signing for the attorney on paper. Clearly, if looked at this way, there is no question that attorneys should not disclose their private keys, even to their paralegals.

Public Access. As courts offer e-filing, they must make some decisions regarding public access to electronically filed documents. Most paper court documents are public and available in person at the courthouse, but only a few court documents are available in electronic form on the Internet. Part of the reason is courts don't have electronic images of all the paper-filed documents. However, as they receive electronic filings, they obtain electronic copies. The most logical step then, is to make the documents available on the Internet.

Courts have not had an easy time, however, making the decision to put electronic documents on the Internet, even if they were electronically filed. For the past 10 years, courts have debated whether or not public documents should be available in their entirety on the Internet. Some argue the personal information contained in some court filings would be embarrassing and perhaps harmful if more readily available through the click of a mouse. Others argue public means public, including the Internet.

A recent development in this area is a document published in October 2002, by the Conference of Chief Justices and the Conference of State Court Administrators that set forth "Guidelines for Public Access to

Court Records (Guidelines)" These "Guidelines" are not mandates but provide a suggested course of action for state courts wrestling with Internet access issues. In a nutshell, they suggest some court documents and data from court documents should not be available on the Internet. They encourage state courts to identify a list of items that should be kept from the Internet, even though the information is available in paper files. For example, Section 4.50 of the "Guidelines" advocates the following information only be available in person at the courthouse:

- address, phone and other contact information for victims and witnesses in criminal, domestic violence, stalking, sexual assault and civil protection order cases/proceedings
- Social Security numbers
- account numbers of specific assets, liabilities, accounts, credit cards and PINs
- medical records
- family law proceedings, including dissolution, child support, custody, visitation, adoption, domestic violence and paternity, except final judgments and orders
- photographs of involuntary nudity and of victims and witnesses involved in certain kinds of actions
- obscene photographs and other materials
- termination of parental rights proceedings
- abuse and neglect proceedings
- names of minor children in certain types of actions

This approach of restricting access to specific data elements across all case types places a burden on court clerks to identify and redact these data elements from otherwise public court documents before placing the documents on the Internet.

For example, a person's Social Security number might be included within the text of pleadings or exhibits, making redaction difficult for clerks. However, technology can provide an answer with data tagging, which is the topic of the next section of this article.

Attorneys also voice another concern about court documents on the Internet — they don't want their work product so readily available to other attorneys. Some also claim copyright infringement and demand courts not post their documents. This is an issue that will be interesting to watch as it more fully develops.

Data Tagging & XML. As courts attempt to redact certain data elements from documents placed on the Internet, and as they work to integrate electronic filing systems with case management systems, they look to data tagging as a solution. Data tagging is the concept of identifying certain data elements when they appear in the text, heading, footer or any other part of a document. If, upon creation of a document, certain data can be electronically "tagged," then other systems can recognize and process the data according to defined business rules.

In the future, I expect court rules will include detailed lists of data items to be "tagged" upon creation of court documents. Under each type of court rule and in connection with the various types of filings, the rules or an exhibit to the rules will require certain data be tagged or used only in certain documents. This will be an additional burden for legal assistants, and will be an important part of the filing process. Courts might even impose sanctions for noncompliance.

So how will legal assistants tag the required data? Luckily, software will help. If you have not yet heard the buzz about XML, you will in the near future. XML is an acronym that stands for Extensible Markup Language. It's a language that allows data to be defined and easily "tagged" within forms. Future e-filing software for law firms will use XML and ultimately be programmed to help legal assistants comply with court rule data lists. After a court receives a document with data tags, it will pull certain data directly into its case management system automatically and redact the data elements not to be publicly accessible or available on the Internet.

Future e-filing software using XML actually will submit documents in XML and include an "envelope" concept. An electronic "envelope" will collect all the documents, exhibits, filing data and signature information to make a complete e-filing package.

Round the Clock Filing. One of the most desired future features of court e-filing systems might be the capability to file court documents 24 hours a day, seven days a week. No more rushing to meet a 4:30 p.m. closing deadline — courts will accept filings round-the-clock. Of course, date stamping will remain important to comply with statutes of limitation, but it's just on the horizon that filings might occur as late as 11:59 p.m.

While this might be desirable to many, some attorneys have expressed concern that allowing later filings will cause attorneys and their staff to

work later hours to perfect their filings. Or perhaps they will just procrastinate a little more. Either scenario will surely result in more late hours at the office.

A humorous example of late-night filing is found in an order recently issued by the United Stated District Court of the Western District of Wisconsin. In the case of Hyperphrase v. Microsoft, Order # 02-C-647-C allows a summary judgment motion filed electronically by Microsoft at 12:04:27 a.m. (four minutes and 27 seconds after the midnight deadline), along with supporting documents that trickled in as late as 1:11:15 a.m. The judge remarked in his order, "I don't know this personally because I was home sleeping, but that's what the court's computer docketing program says, so I'll accept it as true." He went on to conclude, "Wounded though this court may be by Microsoft's four minute and 27 second dereliction of duty, it will transcend the affront and forgive the tardiness. Indeed, to demonstrate the even-handedness of its magnanimity, the court will allow Hyperphrase on some future occasion in this case to e-file a motion four minutes and 30 seconds late, with supporting documents to follow up to 72 minutes later." The plaintiff's motion to strike Microsoft's summary judgment motion due to its untimeliness was therefore denied.

The Next Step

So now, how can you, the legal assistant, start using e-filing? I think the answer is easy. If e-filing is available where you are, learn all you can about it and dive right in. If it's not available to you yet, you still need to educate yourself and become prepared for when it does arrive. As for what the future holds for e-filing, all legal assistants should keep their eyes and ears open so when the technology is mature and systems make filing easier rather than harder — or when courts mandate e-filing — legal assistants will be ready to meet the challenge.

What Every New Attorney Needs To Know About E-Discovery

By: Rhea Frederick, J.D

After graduating from law school, surviving the bar exam, racking up a small fortune in law school loans, and finally landing a job, a new lawyer quickly discovers that one's legal education only begins on his or her first day of work. For example, despite the fact that over 93% of all information is created electronically, electronic data and discovery is one topic that is only briefly mentioned – if referenced at all – in most law school courses. As a result, a new attorney served with a discovery request involving electronic data may not know where to turn first. And because so much information is created electronically, the likelihood of being involved in an electronic discovery project is quite high.

Fortunately, a myriad of solutions exist to help new attorneys get up to speed quickly on the topic, manage electronic information, and control costs associated with electronic document productions. What is the optimal method for pursuing electronic document discovery? What will the court and opposing parties expect from you and your clients?

How can technology assist you and your client? This article will give tips and ideas for attorneys, new to electronic evidence, on effectively managing the electronic discovery process.

Step 1:Defining Electronic Discovery

Initially, counsel must understand and identify the information being sought. In the case of electronic discovery, this means pinpointing relevant and discoverable data existing in electronic form – such as information created on an individual's computer using a word processor or stored and shared with others on the company's "file server." Digital data is located in a variety of places, including individual desktops and laptops, network hard disks, removable media (i.e. floppy disks, tapes, USB drives, and CDs), cell phones, and personal digital assistants (i.e. PalmPilots, Blackberries).

With the increasing popularity of mobile devices, this list will continue to expand. In addition to these locations, e-data can exist in a myriad of different forms and places that may not be readily apparent – a company's old, forgotten archive tapes, an executive's handheld electronic organizer and mobile phone, or memory in a fax machine that stores received data if it cannot be printed immediately(such as

when it runs out of paper). Third parties, like Internet service providers and other peripherally involved entities, may also possess important information.

Minn. R. Civ. P. 34 specifically requires the disclosure of "data, compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form," which includes all forms of electronic data such as electronic files, databases and e-mails. This imposes a duty on attorneys to determine if electronic data might be a legitimate part of the case, thus the need to implement a strategic electronic discovery plan including identifying, locating, retrieving, preserving, and authenticating electronic evidence. Counsel is also responsible for developing, implementing and ensuring compliance with data preservation plans and for producing responsive documents to the opposing party, court or agency.

Groundbreaking E-Discovery Cases

Electronic Evidence is Discoverable: "The law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced…[T]oday it is black letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. 1995). *See also Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003), *McPeek v. Ashcroft*, 202F.R.D. 31 (D.D.C.2001); *Linnen v .A. H. Robins Co.,* 1999 WL 462015 (Mass. Super. 1999).

Deleted Data can be Discoverable: Deleted electronic evidence is fully discoverable. *Dodge, Warren, & Peters Ins. Servs. v. Riley,* 2003 WL 245586 (Cal. Ct. App. 2003); *Simon Property Group v.mySimon, Inc.,* 194 F.R.D. 639 (S.D. Ind. 2000).

Step2:Data Collection

After identifying and locating relevant data, counsel must collect the data for review and production. The modern era has revolutionized the amount of relevant electronic evidence in an average case, and, in most cases, millions of documents exist. Opening and printing such a large volume of documents is simply not feasible. In fact, such conduct can even result in evidence spoliation if any of the document's content or valuable metadata – "the data about the data" or information about a document – is altered.

When faced with an electronic data collection, counsel should form a data collection "plan of attack." The components of a solid plan should incorporate the relevant information sought, potential data locations and key players, internal and external contact information, procedural guidelines, documented chain of custody instructions, an inventory of forensic tools, and a summary of anticipated business continuity issues. Clearly defining the collection scope and priority of key players will avoid creating unnecessary delays and increased costs down the road. In addition, by collecting and processing the highest priority individuals first, crucial case-altering evidence – either helpful or detrimental – may be discovered, changing the litigation team's positions and strategies.

When organizations operate in multiple locations, utilize differing types of technologies, or have employees with disparate access to these technologies, it can be difficult to ascertain where electronic evidence is held. It is incredibly important to consider all potential data locations, including geographical locations as well as storage locations such as file shares, e-mail devices, archival tapes, hosted e-mail, and attachments.

Because IT may not always understand how to best handle data subject to legal discovery, counsel may need to engage the help of an electronic discovery expert for the collection. Attorneys should seek the help of an expert if the IT staff lacks the requisite equipment, time, training and experience to perform a best practices collection. An expert may also be necessary if calling an IT person as a witness at trial is undesirable or if a conflict of interest might hurt the case.

Step 3: Data Filtering

In most cases, it makes sense to keep electronic data in an electronic format. The benefits include quicker and more efficient searching, Bates number branding, redacting, annotating, and the ability to catalogue and reorganize for production, depositions or trial. Electronic discovery experts, the firm's litigation support department, or the client's IT department can create copies of the collected data, without making any alterations, and place it in a central storage location.

Obviously, not every electronic document found within the files retrieved from a document custodian or on backup tapes is responsive or relevant to a discovery request. Electronic discovery filtering engines can be used to scan the data, separating and eliminating the "jokes, recipes and spam" from potentially responsive files and e-mails. For smaller or simple projects, the firm's litigation support

department or the client's IT staff can use some basic commercially available e-discovery filtering engines.

However, large amounts of data or complicated data types are best left to an electronic discovery expert's proprietary filtering technology. Such proprietary technology can narrow the universe of data down to a smaller, more manage able set by providing enhanced options to better define a more complex but precise filtering process, such as limiting the universe of data to certain custodians or to documents with specified file attributes (i.e. keywords, certain document types, created or last accessed within a specified date range). Attorneys using all of the filtering techniques described below typically experience a 75% reduction in the number of documents they need to review for production.

• Custodian filtering – segregating the key custodians who may be relevant to the case and isolating the files associated with those specific individuals;
• Time and date filtering – targeting discrete periods of times, which are particularly relevant to a case or which are required to be produced in accordance with a pending court order;
• File Size Filtering – capturing files between a certain size range in order to isolate mid-sized files from exorbitantly large files;
• De-duplication – identifying documents that are duplicates of one another and eliminating these duplicate documents from the review and production set of documents.
• Keyword searching – applying a set of keywords and terms to segregate potentially responsive information for further review and scrutiny; and,

Step 4: Review Options

After data has been gathered and culled using filtering technologies, counsel must determine the data format for the internal review and contemplate the next step – production to the court, governmental agency and/or opposing party.

In most cases, two options are available for review; paper and electronic.

If a paper review is chosen, the electronic documents are printed. While paper review may seem straight-forward and "tried and true," it poses several disadvantages. First, an electronic document's metadata could potentially be lost since this information may not print out on the face of the document when the "print" button is pushed. Further, when

electronic documents are reduced to paper, the review team loses its ability to search these documents, without using scanning, coding, and optical character recognition technology at some point down the road. If the opposing party is demanding the production in an electronic format, first relegating the documents to a paper format only adds expense, time-delay, and the chance of data loss.

An electronic review is another option for reviewing documents for responsiveness or privilege. Using an electronic review option is becoming standard for litigators faced with electronic document productions since it typically provides greater flexibility, efficiency and cost-effectiveness over paper. Electronic review generally occurs one of three ways: (1) reviewing documents in their "native" format, (2) using a local database (like Summation or Concor dance) or (3) using an online document review repository – a web-based database into which the data files have been loaded in either a standard file format (such as tiff images) or the native file format for viewing, categorization, redaction, and searching.

Electronic document online repositories represent the most modern document management and review tools and are gaining momentum in the legal community. With such software programs, reviewers remotely access their documents via a secure Internet connection and review each document file by file. The files must be converted to a standard file format or undergo some sort of text extraction in order for the documents to be placed into a web-based tool with searching capabilities. Each page of a document is placed into a database after being converted into two separate components (1) a graphic image (such as a tiff, PDF or jpg) that is able to be viewed in a standard browser, along with (2) an accompanying file that contains the text and metadata for each page.

Consider the following when selecting an electronic online review repository:

• *Speed.* Look for a software package that provides for speedy document viewing. How many seconds does it take to log on to the system? How many seconds does it take to navigate between documents in the system?

• *Security.* The data review repository should handle all security issues. How are the documents protected against interception by someone else on the World Wide Web?

• *Ease of Use.* What does the program's GUI look like? The software's graphical user interface ("GUI") should be easy to use. The layout should be familiar (i.e., similar to a common word processing or e-mail system such as Microsoft Office) and simple to navigate to the commonly used functionalities. How many hours of training are necessary before the review team can begin looking at documents?

• *All-inclusive software.* Can standard software be used, such as Microsoft's Internet Explorer? Must any additional software or licenses be purchased before the review begins? Are there any hidden costs associated with the review?

• *Robust Functionality.* These systems are constantly changing, offering the customer more advanced features and functionality. Does the repository offer note-taking? Highlighting? Redactions? Redaction coding? Privilege log creation?

• *Searching.* Being able to search the database of documents is one main advantage of keeping documents in an electronic format. How does the repository's searching work? Can the metadata be searched? Are notes and comments searchable? Is advanced searching (conceptual searching or fuzzy searching) available?

• *Duplicate Handling and Family Cascading.* If the data is kept in an electronic format, relationships between duplicate documents and parent and children documents can be identified and maintained in the database. Using this feature, reviewers can handle related documents together and categorize them simultaneously; reducing time spent reviewing the same documents several times.

• *Mass Categorization.* With mass categorization, reviewers can categorize several documents at once based on search results. This feature gives reviewers the power to quickly review clearly responsive, non-responsive or privileged documents in the document set.

• *Native File Review*. Cutting-edge online document repositories are giving litigation teams the best of both worlds, typically allowing for native and tiff viewing in one unique database. While such tools have only emerged recently in the legal arena, without such a solution, litigation teams are forced to deal with the disadvantages of raw native files or tiff images when reviewing documents. Instead, depending on the features and functionality built into the tool, counsel can leverage the advantages of native file review and tiff image review, without

incurring any of the drawbacks of either review format in its individual setting.

• *Paper and Electronic Integration.* Traditionally, law firms have split outsourced discovery work between different paper and electronic discovery experts. If a law firm selects a single, specialized expert offering both electronic paper discovery services, the law firm and its client will likely realize many administrative advantages and be able to develop the most solid theory for the case by having all of the documentary evidence in a single location at one point in time.

Step 5: Production Options

Once the review is complete and all documents have been identified as responsive, non-responsive or privileged, counsel must focus on producing the responsive documents to the opposing party, court or government. Counsel must ask: What format will the documents need to be produced in and will the court, opposing party, or government accept documents in an electronic format? These questions are best addressed by counsel long before the document review ever begins, typically at some of the first discovery planning conferences with the opposing party or court.

While production in the past was generally in paper, production in electronic format is becoming a clear trend. Given the fact that an overwhelming majority of corporate documents appear in electronic form, production in electronic format should not come as a surprise to counsel. The requesting party must make a strategic decision when determining production format, especially in light of its ability to conduct an effective review of the evidence received.

As online review tools and repositories increase in popularity and become more sophisticated, attorneys are also finding it easier and more cost-effective to produce electronic documents in an online repository. The litigation team can categorize, redact, and annotate the documents in the review tool, and when complete, have the relevant and non-privileged documents copied to a separate production database for the opposing party, court, or government agency to complete its review. Expect to see increased use of online repositories for producing and managing volumes of both paper and electronic documents.

In today's high-tech corporate world, courts, counsel and organizations have clearly acknowledged that technology has a significant role in litigation. With this ever-growing recognition of modern technology

trends, newly-practicing attorneys representing today's organizations need to know more than simply where electronic evidence resides.

They also have a duty to know if that data is accessible and how much it will cost to restore, search and produce the data should litigation or a regulatory investigation ensue. A comprehensive understanding of the electronic discovery process – coupled with strategies to manage electronic discovery costs – will allow new attorneys to gain recognition as their law firms' electronic discovery authority and deliver a successful, case-winning discovery plan of attack.

Electronic Discovery:

A Brave New World

By Michael P. Zweig and Mark J. Goldberg

In May of 2003, Judge Shira Scheindlin of the U.S. District Court for the Southern District of New York issued what is sure to become a seminal opinion on one of today's hottest legal topics: the discovery of electronic data. Judge Scheindlin began her opinion in *Zubulake v. UBS Warburg LLC*[1] with the observation that the world [is] a different place. Indeed, estimates are that ninety-three percent of all business records now created are stored electronically.[2] Seventy percent of these records are never printed out,[3] and, in 2001, businesses in North America generated approximately 2.5 trillion e-mail messages.[4]

Indeed, the world is a very different place than it was five years ago when, often out of ignorance, many litigators disregarded the existence of much electronic data in discovery, producing only that which was reduced to hard copy or which an adversary specifically requested by name. Today, newspapers are peppered with headlines of explosive and smoking gun e-mails, such as Nancy Temples e-mail in the Arthur Anderson/Enron debacle, Frank Quatrones e-mail reminder of Credit Suisse First Boston's document destruction policy, and Jack Grubmans e-mail suggesting that he published overly optimistic research reports in an effort to inspire Citigroup Inc.'s CEO, Sanford Weill, to help get Grubmans children into a competitive Manhattan nursery school.

Thanks to these smoking gun e-mails, attorneys are now focused on the discovery of electronic data. It is quite clear that the quaint era of dont-ask-dont-tell with respect to the existence of electronic data has come to a crashing halt. Lawyers now realize that electronic data actually drives today's discovery and litigation process, and that the existence or non-existence of such data can be critical to the outcome of many litigations.

Given this increased attention to electronic discovery, companies, their attorneys, and the courts are now, for the first time, grappling with a number of related issues. This article addresses four:

Is electronic data discoverable?

What are the obligations of counsel regarding electronic discovery?

What is the form and scope of electronic discovery?

Who pays for electronic discovery?

The Discoverability of Electronic Data

In the area of electronic discovery, courts are not writing on a blank slate. Rules 26 through 37 of the Federal Rules of Civil Procedure have regulated discovery for over 30 years under the guiding principle that full and complete discovery is presumed as to any document or issue that is relevant to a claim or defense or is likely to lead to the discovery of relevant evidence. These rules make clear that electronic data is discoverable. Rule 26(a)(1)(b) requires that all parties produce as part of their initial litigation disclosure *data compilations* that may be used to support their claims and defenses. Rule 34(a) similarly requires that documents, including writings . . . and other *data compilations*, be produced. The 1970 Advisory Committee Notes to Rule 34, as well as case law construing the rule, emphasize that Rule 34 applies to electronic data.[5] Likewise, Local Civil Rule 26.3 for the U.S. District Courts for the Southern and Eastern Districts of New York expressly defines documents to include *all electronic or computerized data compilations*.

Obligations of Counsel in Electronic Discovery

Not only is electronic data discoverable, but the courts have made clear that attorneys have considerable obligations in conducting electronic discovery. Before responding to a discovery request, an attorney must gain a firm understanding of the clients electronic data capabilities and supervise the search of electronic data to see if such data is responsive to one or more discovery requests. In doing so, an attorney should ask the client to designate a technologically knowledgeable point-person at the client to coordinate with counsel and to assist with the collection and management of relevant electronic data. If necessary either due to the complexity of a clients information systems or the lack of in-house expertise an attorney should consider retaining an expert computer consultant.

It is prudent for an attorney to take these steps because the failure to conduct an inventory of a clients electronic capabilities or to search for or produce electronic data can result in sanctions to the client and/or the attorney. For example, in *GTFM v. Wal-Mart Stores, Inc.*, the Southern District of New York recently granted the plaintiffs motion for sanctions in the form of reimbursement of certain expenses and legal fees because the defendants misrepresentation about its computer capacity caused the plaintiffs to expend[] extensive time and money attempting to retrieve the information in other ways. [6] Similarly, in January of this year, the same court, in *Metropolitan Opera Assoc., Inc. v. Local 100*, found that counsel for the defendants had failed to comply with discovery rules by, among other things, (1) failing to give adequate instructions to their clients about the clients overall discovery obligations; (2) knowing that their clients had no document retention or filing system and failing to implement a systematic procedure for producing and retaining documents, including electronic documents; and (3) delegating document production to a layperson who did not understand that a document included computer files and e-mails. In light of counsels wholesale failure to comply with their discovery obligations, the court granted the severest of sanctions, finding liability on the part of the defendants and ordering the defendants to pay the plaintiffs attorneys fees necessitated by the discovery abuse.[7]

What should you be looking for?

Gaining a comprehensive understanding of what types of relevant electronic data may be available and where such data may be located can seem like a daunting task to attorneys who are not technologically inclined. For most companies, there generally are four key areas of electronic evidence subject to discovery:

1. Electronic correspondence (*e.g.*, e-mail messages, voicemail messages, and instant messaging dialogs);

2. Electronically created and stored business documents (*e.g.*, word processing documents, spreadsheets, personal and shared calendars, and company policies and procedures);

3. Computer databases (*e.g.*, financial and human resources databases); and

4. System information (*i.e.*, detailed logs automatically created by a computer detailing who is doing what and when on the computer).

Notably, even where such electronic evidence also exists in paper form, the electronic version is often more useful because it contains information known as metadata or embedded data. This information, which may not be apparent in a print-out, may include the date the document was created, the identity of the author, the identity of subsequent editors, the distribution route for the document, or the history of editorial changes.[8]

Where can you find it?

In determining where relevant electronic data is located, an attorney should consider the following places where electronic data is routinely stored. However, as further discussed below, just because relevant data may exist in one or more of these locations does not mean that a party must *automatically* preserve and/or produce such data during discovery.

- **Online storage media**. This type of storage media is connected at all times to a computer, makes data immediately available, and is typically used for data that is accessed on a regular basis. Common examples are the hard drives in PCs and network storage devices, as well as the memory chips in personal digital assistants (like Palm Pilots) and Blackberries.
- **Near-line storage media.** This type of storage media is connected to a computer and makes data available, generally within minutes. Examples are disk and tape libraries using robotic arms to access individual disks or tapes, which are similar to (but often larger than) the CD changers that many people have in their cars.
- **Offline storage devices.** These storage devices are not connected to a computer and require a person to make such a connection. Examples include floppy disks or CDs. Businesses often use offline storage devices to make disaster copies of records or for records that are unlikely to be used often. Depending on where an offline storage device is located, accessing the data on it can take minutes, hours, or even days.
- **Back-up tapes.** These tapes contain copies of the information stored on a computers hard disk and are usually kept for disaster recovery purposes. This information is not easily accessible. To understand why, it is necessary to understand how a computer stores information. When storing a file on a hard drive, a computer does not necessarily put all the data in one spot. Often, because various parts of the hard drive have already been used, no one block of free space is large enough

for the new file. Therefore, the computer saves the new file in fragments stored in multiple free spaces on the hard drive and keeps an index or directory of where it put the fragments. When the file is subsequently accessed, the computer uses the directory to reassemble the file fragments. This is done quickly, since a computer can directly access different parts of its hard drive.

When a backup tape is used, information is saved in the random order in which it appears on the hard drive, often using data compression technology. Because, unlike a hard drive, different spots on a magnetic tape cannot be directly accessed, the information stored thereon cannot be easily accessed without first putting it back onto a hard drive in a potentially time consuming and costly process called restoring the data.

- **Residual data.** This data is typically created when information is marked for deletion or is damaged. When a computer deletes a file, it does not actually erase the contents of the file from the computers hard drive. Instead, it simply changes the files entry on the hard drives directory to not used, thereby allowing the computer to overwrite the file fragments on the hard disk in which the file was stored. However, before all the file fragments have been overwritten, it is still possible to access them using computer forensics technology.
- **Replicant files.** These files, also called temporary files or file clones, are copies of files that are automatically created by a computer (usually on its hard drive) to prevent the loss of data in the event of a computer malfunction. For example, word processing programs often automatically save a document every few minutes so that if the computer freezes or experiences some other problem, the only work lost will be changes made since the last time the document was automatically saved.

When does the duty to preserve electronic evidence arise?

In addition to knowing where to look for data, an attorney must also confirm that clients preserve relevant electronic data (as well as other types of relevant evidence) in connection with an actual or potential claim.[9] A number of issues arise in connection with this obligation. An initial question is when does this duty to preserve arise. It is clear that a client has the duty to preserve *all* documents when a civil claim or proceeding commences, is likely to occur, or is reasonably foreseeable. The same duty also arises when a subpoena is served or

threatened or when a regulatory or criminal proceeding, litigation, or arbitration is commenced.[10] A more difficult instance, and one that is case-dependant, is whether the duty to preserve evidence arises even at the pre-dispute stage when the principals are engaged in settlement discussions.

Even in the absence of an actual or potential claim, a client may be obligated to preserve documents, including electronically stored data. For example, in the securities industry, Rule 17a-4 under the Securities and Exchange Act requires broker-dealers to preserve business-related documents, including interoffice e-mails and electronic correspondence with clients, for specified periods of time. Indeed, in November 2002, five major investment banks consented to findings that they had violated Rule 17a-4s record retention requirement with respect to business-related e-mails and agreed to pay fines totaling $8.25 million. In addition to the requirements of Rule 17a-4, employers, in general, are required to preserve various employment-related documents, often for a period of one to three years.[11]

Once the duty to preserve evidence arises, courts have held that the obligation to preserve evidence runs first to counsel, who then has a duty to advise and explain to the client its obligations to retain pertinent documents that may be relevant to the litigation.[12] Thus, counsel should institute an early warning system within their clients so that counsel are alerted as soon as the duty to preserve documents and information is triggered. Such an early warning system allows counsel, in conjunction with the clients MIS or IT department, to insure that relevant documents are preserved and not destroyed.

The reason for paranoia on this subject is obvious. The specter of documents that have been destroyed can poison a case, even if the documents had they been preserved and produced would have been relatively harmless. Accordingly, counsel should establish a litigation-oriented protocol to preserve relevant and discoverable material already created, or to be created in the future. That protocol should include:

- An intelligent review of the clients document destruction policies to confirm that any relevant data that may be destroyed or over-written is preserved, potentially by using mirror imaging technology, which copies hard drives at a given point in time; and

- The more traditional measure of sending document preservation letters to all employees, as well as agents of the company, who may have potentially relevant data.

Another related issue is what types of electronic evidence must a party *automatically* preserve and produce during the course of discovery. It is clear that a party must automatically preserve and produce electronic data that is easily accessed, such as online, near-line, and some offline data. However, the answer is less clear with respect to electronic data that is not easily accessed, such as information on backup tapes and residual data. While there is little question that such data is discoverable,[13] most courts and commentators that have addressed this issue have taken the position that a party need not *automatically* produce such hard-to-access data unless the requesting party demonstrates that the need and the relevance of the data outweigh the cost, burden and disruption of retrieving, processing and producing it.[14] As a matter of prudence, a party and its counsel should nevertheless take steps to preserve any backup tapes and residual data reasonably believed to contain relevant electronic data.

What are the risks?

Failure of a party or its counsel to fulfill this obligation to preserve electronic and other evidence which is known as spoliation of evidence can result in civil and, possibly, criminal sanctions. At least in the Second Circuit, a client need not be found to have acted intentionally in order to be sanctioned; mere negligence may be sufficient. In *Residential Funding Corp. v. DeGeorge Financial Corp.*,[15] where the plaintiff corporation had won a $96.4 million jury verdict, the Second Circuit criticized the trial courts denial of a defense motion for sanctions to redress the plaintiffs failure to produce voluminous e-mails until after the trial had begun. Notably, the court remanded the case with instructions that the district court should vacate the verdict if the defendant is able to establish that the plaintiff acted with the requisite culpable state of mind which included negligence in failing to produce the e-mails *and* the defendant was prejudiced as a result.

Civil sanctions that have been awarded for spoliation of evidence include (1) monetary damages, as in *In re Prudential Ins. Co. Sales Practices Litig.*,[16] where the court levied a $1 million sanction against a company for destruction of electronic evidence; (2) the possibility of an adverse inference jury instruction, as in *Residential Funding*;[17] and even (3) an adverse decision in a case, as in the recent Second Circuit decision of *Metropolitan Opera*,[18] where the

court held that a defendants failure to, among other things, preserve electronic data warranted an adverse finding of liability. Additionally, the intentional destruction of electronic documents likely to be sought in a civil action might constitute a criminal violation for obstruction of justice under 18 U.S.C. 1503.[19]

The Form and Scope of Electronic Discovery

Electronic discovery raises a number of unique issues regarding the form and scope of the contemplated discovery, including:

- Whether the discovery will be limited to active files, or include back-up material, archival and/or residual data;
- Whether the automatic document destruction procedures, including the overwriting of back-up tapes, should be suspended;
- Whether the search for relevant electronic data is to extend beyond those documents kept in the ordinary course of business;
- Whether such a search will be limited to data created or stored by certain employees and, if so, which ones;
- Whether to give the opposing party access to your computer system; and
- Whether the production will be in electronic or paper form and, if electronic, in what format the media will be produced and whether special access software be provided.

In many cases in which electronic discovery is sought, the parties will have a mutual interest in learning about the others electronic data systems and practices and in avoiding costly motion practice regarding electronic discovery. In such instances, the parties should confer at the outset of an action in an attempt to reach agreement on the scope of each party's rights and responsibilities regarding electronic discovery. Even if the parties do not agree on all the issues, any partial agreement is one matter less that needs to be addressed with the court. An opportune time to hold a discussion regarding electronic discovery issues is during the parties discovery conference as required in many federal jurisdictions by Fed. R. Civ. P. 26(f).[20] Indeed, this is required by some local court rules.[21] In appropriate circumstances, the parties should also consider involving either their own or a mutually agreed upon computer expert in these discussions.

Where parties have not been able to resolve electronic discovery issues themselves, they may seek resolution from the courts either by

moving for a protective order (under Fed. R. Civ. P. 26(c)) or by seeking an order to compel discovery (under Fed. R. Civ. P. 37). The parties also may raise such issues during a Rule 16(a) pretrial conference.

How can burdensome discovery be limited?

In deciding electronic discovery issues, courts often exercise their discretion under Fed. R. Civ. P. 26 to limit discovery if the burden or expense of the proposed discovery outweighs its likely benefit. For example, in *In re General Instrument Corp. Sec. Litig.*, the court denied the plaintiffs motion to compel the production of e-mail and other computer generated evidence, finding that the burden of the requested discovery outweighed its likely benefit because: (1) the defendants had already produced 110,000 pages of documents, including thousands of pages of e-mail; (2) the plaintiffs have not identified any specific factual issue for which [this] additional discovery would help them prove their case; and (3) given that the volume of e-mail at issue was potentially significant, the burden of reviewing the requested documents would be heavy. [22] A popular method by which courts attempt to determine the likely benefit (e.g., the extent and nature of relevant evidence likely to be had) from proposed electronic discovery is data sampling, which involves reviewing a limited, representative sample of the requested electronic data.[23]

Many courts also have used their discretion to limit burdensome discovery under Fed. R. Civ. P. 26 to fashion a computer-based discovery protocol similar to the one adopted by the Southern District of New York in *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*[24] In *Rowe*, the following procedure was ordered by the court:

1. The parties will agree on an expert responsible for extracting the relevant data and preparing it for the parties review;

2. The expert will create a mirror image of the computer data to be discovered;

3. The parties will agree upon a search procedure for the data;

4. The expert will execute the agreed upon search procedure;

5. The receiving party will review the results of the search and turn over to the producing party those documents that it considers material to the litigation; and

6. The producing party will review the selected documents for privilege.

The court also gave the producing party the option of reviewing the results of the experts search prior to any review by the receiving party for the purpose of identifying and withholding privileged documents. If the producing party chose such an option, it was required to produce a privilege log, identifying all withheld documents.[25]

Should production be in electronic or paper form?

Another issue courts have been asked to decide is whether electronic documents must be produced in electronic form. Electronic versions of documents have a number of advantages: they contain metadata, are more easily searchable, take up less space, and more clearly indicate what attachments go with which e-mails. Therefore, they are preferred over paper copies.

Most courts addressing the issue have held that electronic documents must be produced in electronic form.[26] However, in a 1982 decision, the Ninth Circuit held that a party could not be compelled to produce data in electronic form if it had supplied the same data in hard copy. The court specifically noted that, [w]hile using the [hard copies] may be more time consuming, difficult and expensive, these reasons, of themselves, do not show that the trial judge abused his discretion in denying [plaintiffs] the tapes.[27] Today, nearly 20 years later, the courts cost/benefit analysis might be different as it is now well-recognized that electronic versions of documents contain information, such as metadata, that is often not available on hard copies.

What about arbitration?

Issues relating to electronic discovery are not confined to litigation in the courts; it is predictable that the discovery of electronic evidence in arbitration proceedings will follow a similar route, lest the arbitration process be seen as a forum substantively unfavorable to claimants. Claimants attorneys in arbitration proceedings likely will push to have the same level of electronic discovery, and similar production protocols, as might be required in the courts.

The NASD has published a Discovery Guide for customer cases, which specifies the types of documents that presumptively should be produced in certain instances.[28] The Guide also requires a statement from the responding party if there are no responsive documents, and

calls for sanctions for non-production in the event documents actually did exist. Since many of the documents the Discovery Guide calls for are likely to be stored in electronic form (for example, all correspondence with customers and all notes about a customers account), it is likely that claimants attorneys will push for as much electronic data as possible.

Who Bears the Cost - "Cost Sharing"

The production of electronic documents can be very expensive if one needs to restore backup tapes, utilize forensic technology to access requested data, and review what is often a vast number of documents. As a result, one of today's hottest topics involving electronic discovery is who will pay for it. The general rule in civil discovery is that each party pays its own document production costs.[29] However, as the Supreme Court has recognized, a party may invoke the district courts discretion under Rule 26(c) to grant orders protecting him from undue burden and expense in [complying with discovery requests], including orders conditioning discovery on the requesting party's payment of the costs of discovery.[30]

Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved.[31] However, in *Zubulake*, Judge Scheindlin argues that this makes no sense . . . because [unlike paper documents, electronic evidence] can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.[32] According to Judge Scheindlin, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an *accessible* or *inaccessible* format.[33] As described above, electronic data that is in inaccessible formats, like backup tapes or residual data, will often be expensive to produce because it requires a party to restore the data and/or use computer forensic technology to access it.

In *Zubulake*, the plaintiff, who was suing her former employer, UBS Warburg, for gender discrimination and illegal retaliation, propounded a document request for all internal UBS communications, including e-mails, relating to her. The parties agreed that e-mail was an important means of communication at UBS, that e-mail would unquestionably yield relevant information, and that UBS would produce responsive e-mails from the accounts of certain of its employees. UBS maintained e-mail files in three different forms: active user e-mail files, archived e-mails on optical disks, and backup data stored on tapes. While UBS

produced responsive e-mails from its active user files and optical disks, it refused to produce the e-mails on its backup tapes on the ground that restoring and producing such e-mails would cost approximately $300,000. The plaintiff moved to compel the production of the e-mails on the backup tapes, and, while UBS opposed the motion, it also argued that, if any production was required, the plaintiff (not it) should be required to pay the costs.

Judge Scheindlin ordered UBS to produce only a small portion of the e-mails on the backup tapes requested and then applied a three-step analysis to the cost-shifting issue. Under Judge Scheindlins first step, a court should determine in what medium any relevant electronic data is stored. For data in an accessible format, the responding party should pay for the production. For data in an inaccessible format, a court should use the rest of the analysis to consider shifting the costs. Under the second step, a court should determine what information is likely to be contained in the inaccessible data and the cost to access it. This can be done by conducting a limited sampling of the backup tapes. For the third step, based on the results of the data sampling, the court can conduct a cost-shifting analysis utilizing a multi-factored balancing test. While this three-step analysis is certainly appropriate where data sampling is necessary to determine the likely contents of the inaccessible data at issue, it is more appropriate to go directly to step three (the cost-shifting analysis) where the likely content of the inaccessible data can already be determined.

Applying her three-step analysis, Judge Scheindlin ordered UBS to produce responsive e-mails from a sampling of backup tapes and to submit an affidavit detailing the results of the production, as well as the time and costs involved. Judge Scheindlin said that she would use that information to conduct a cost-shifting analysis based on her modification of certain aspects of the multi-factored balancing test first set forth in January 2002 in *Rowe Entertainment*.[34] In that case, the court ordered the plaintiffs to pay for the costs of restoring e-mails they had requested and which were stored on backup tapes. In determining to shift the costs of this electronic discovery to plaintiffs, the court utilized a balancing test with the following eight factors:

1. The specificity of the discovery request;

2. The likelihood of discovering critical information;

3. The availability of information from other sources;

4. The reasons why the responding party maintains the data;

5. The relative benefits of obtaining the data;

6. The total costs of production;

7. The relative abilities of the parties to control costs; and

8. The resources available to each party.

As Judge Scheindlin acknowledged in *Zubulake*, [i]n the year since *Rowe* was decided, its eight factor test has unquestionably become the gold standard for courts resolving electronic discovery disputes.[35]

Judge Scheindlin, however, argued that the *Rowe* test inappropriately favored cost shifting and did not take into account certain factors expressly required to be considered by Fed. R. Civ. P. 26. Therefore, building on *Rowe,* Judge Scheindlin revised the eight-factor test into a seven-factor one, utilizing the following factors to be weighted in the following order:

1. The extent to which the request is specifically tailored to discover relevant information;

2. The availability of such information from other sources;

3. The total cost of production, compared to the amount in controversy;

4. The total cost of production, compared to the resources available to each party;

5. The relative ability to each party to control costs and its incentive to do so;

6. The importance of the issues at stake in the litigation; and

7. The relative benefits to the parties of obtaining the information.[36]

Since it has been only a short period of time since *Zubulake* was decided, it is not clear yet whether this test will replace *Rowe*s as the gold standard or, indeed, how it will affect the allocation of expenses in the *Zubulake* case.

Conclusion

There are many new issues just now being raised and litigated in the brave new world of electronic discovery. Hard and fast rules are hard to come by; many rules are just first being crafted and others are being refined. As the smoke clears and the rules sort themselves out, the best advice is to be diligent about discovery obligations and proactive with respect to raising limitations and disputes about the scope of electronic discovery early on in the process.

---

* Michael P. Zweig (mzweig@loeb.com) is a litigation partner, and Mark J. Goldberg (mgoldberg@loeb.com) is a Senior Counsel, in the New York office of Loeb and Loeb LLP.

[1] No. 02 Civ. 1243 (SAS), 2003 WL 21087884 (S.D.N.Y. May 13, 2003).

[2] Mark Ballard, Digital headache, E-discovery costs soar into the millions, and litigants seek guidance, The Natl L. J. (Feb. 10, 2003), *available at* <www.nlj.com/business/021003bizlede.shtml>;.

[3] *Id.*

[4] Elizabeth Weinstein, Help! Im Drowning in E-Mail, WALL ST. J., Jan. 10, 2002, at B1.

[5] *See* Fed. R. Civ. P. 34 advisory committees note (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[.]); *see also* Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *1 (S.D.N.Y. Nov. 3, 1995) (The law is clear that data in computerized form is discoverable even if paper hard copies of the information have been produced); Santiago v. Miles, 121 F.R.D. 636, 639-640 (W.D.N.Y. 1988) (A request for raw *information* in computer banks is proper and the information is obtainable under the discovery rules.).

[6] No. 98 Civ. 7724, 2000 WL 335558, at *2 (S.D.N.Y. Mar. 30, 2000).

[7] 212 F.R.D. 178, 231 (S.D.N.Y. 2003).

[8] *See* James P. Flynn & Sheldon M. Finkelstein, A Primer on E-vide-n.c.e., 28 Litigation 34, 36-7 (Winter 2002) (*quoting* N.Y. State Bar Assn, Does Discovery of Electronic Information Require Amendments to the Federal Rules of Civil Procedure? (Feb. 22, 2001)).

[9] *See* Shamis v. Ambassador Factors Corp., 34 F. Supp. 2d 879, 888-89 (S.D.N.Y. 1999); Wm. T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984); Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472, 485-86 (S.D. Fla. 1984).

[10] *See, e.g.,* Hirsch v. General Motors Corp., 628 A.2d 1108 (N.J. 1993).

[11] For example, the Fair Labor Standards Act and the New York Labor Law require that employee payroll records(including an employees name, social security number,date of birth, gender, occupation, regular hourly rate or salary, hours worked, amount of overtime worked, and amount of wages paid) be kept for three years. Additionally, fair employment practice laws (*e.g.*, Title VII of the Civil Rights Act of 1964, the American with Disabilities Act, the Equal Pay Act) require employers to keep records relating to hiring, promotion, demotion, transfer, layoff or termination, rates of pay, selection for training, and physical examinations for one year from making the record or taking the personnel action, whichever is later.

[12] Telecom Intl Am., Ltd. v. AT&T Corp., 189 F.R.D. 76, 81 (S.D.N.Y. 1999); *see also* Mosel Vitelic Corp. v. Micron Tech., Inc., 162 F. Supp. 2d 307, 311 (D. Del. 2000) (quoting *Telecom*).

[13] Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) ([I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable.); Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) ([C]omputer records, including records that have been deleted, are documents discoverable under Fed. R. Civ. P. 34.); Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (Plaintiff needs to access the hard drive of Defendants computer only

because Defendants action in deleting those e-mails made it currently impossible to produce the information as a document.).

[14] *See, e.g.,* McPeek v. Ashcroft, 202 F.R.D. 31, 33-35 (D.D.C. 2001) (rejecting notion that there is an absolute obligation to pursue potentially relevant data on backup tapes); The Sedona Conference, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, March 2003, *available at* <www.thesedonaconference.org/publications_html>; (Principle No. 8: The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval, and resort to disaster recover backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.); ABA Section of Litigation Council, Civil Discovery Standard 29.a.iii (Aug. 1999), *available at* <www.abanet.org/litigation/public/standards.html>; (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.).

[15] 306 F.3d 99 (2d Cir. 2002).

[16] 169 F.R.D. 598, 617 (D.N.J. 1997).

[17] 306 F.3d at 113; *see also* Liafail, Inc. v. Learning 2000, Inc., Nos. CA 01-599 & 01-678, 2002 WL 31954396 *3-4 (D. Del. Dec. 23, 2002).

[18] 212 F.R.D. at 231.

[19] *See* United States v. Lundwall, 1 F. Supp. 2d 249, 250 (S.D.N.Y. 1998).

[20] *See* In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437 (D.N.J. 2002) (noting importance of discussing electronic evidence at Rule 26(f) conference); Kleiner v. Burns, 48 Fed. R. Serv. 644 (D. Kan. 2000) (holding that Rule 26 requires disclosure of the nature and

location of relevant electronic documents); Danis v. USN Commun., Inc., 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 23, 2000) (court criticized the parties for failure to communicate or gain complete mastery of what types of documents were generated [by defendant] in the ordinary course of business, how they were used, or their significance.).

[21] *See* U.S. Dist. Ct. Ark. L. R. 26.1 (The Fed. R. Civ. P. 26(f) report filed with the court must contain the parties views and proposals regarding . . . [w]hether any party will likely be requested to disclose or produce information from electronic or computer based media. If so, the report must also include a variety of details on electronic discovery as specified by the rule.); U.S. Dist. Ct. Wyo. L. R. 26.1(d)(3)(a) (The parties shall meet and confer regarding the following matters during the Fed. R. Civ. P. 26(f) conference: (i) Computer-based information (in general) . . . (ii) E-mail information . . . (iii) Deleted information . . . and (iv) Back-up data.).

[22] No. 96 C. 1129, 1999 U.S. Dist. LEXIS 18182, at *17-19 (N.D. Ill. Nov. 15, 1999).

[23] *See, e.g.,* Zubulake, 2003 WL 21087884, at *13 (ordering e-mails from just five backup tapes to be restored, after which the court said it would conduct a cost-shifting analysis); Tulip Computers Intl v. Dell Computer Corp., No. Civ. 00-981, 2002 WL 818061, at *7 (D.Del. Apr. 30, 2002) (endorsing plaintiffs proposal that defendant search hard drives of a small number of key executives for documents containing a list of mutually agreed upon search terms).

[24] 205 F.R.D. 421, 433 (S.D.N.Y. 2002), *affd*, 2002 U.S. Dist. LEXIS 8308 (S.D.N.Y. May 8, 2002).

[25] *See also* Playboy Enters*.,* 60 F. Supp. 2d at 1054-55; Simon Prop., 194 F.R.D. at 640.

[26] Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995) (production of information in hard copy documentary form does not preclude a party from receiving that same information in computerized/electronic form.); In re Air Crash Disaster at Detroit Metro. Airport, 130 F.R.D. 634, 636 (E.D. Mich. 1989) (compelling McDonnell Douglas to produce computer tape of a flight simulation program and data, even though such information had already been produced in hard copy); National Union Electric Corp. v. Matsushita Electronic Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980)

(ordering plaintiff to produce computer tape even though defendants already had a printout of the data contained therein).

[27] Williams v. Owens-Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982).

[28] NASDs Discovery Guide is available at <www.nasdadr.com/pdf-text/discovery_guide.pdf>;.

[29] Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978) (Under [the discovery] rules, the presumption is that the responding party must bear the expense of complying with discovery requests).

[30] *Id*.

[31] *Zubulake*, 2003 WL 21087884, at *7.

[32] *Id.*

[33] *Id.* (emphasis in original).

[34] 205 F.R.D. 421.

[35] 2003 WL 21087884, at *9.

[36] 2003 WL 21087884, at *13.

This article was first published in the July 2003 issue of *Wall Street Lawyer*.