RECORD RETENTION AND DESTRUCTION
CURRENT BEST PRACTICES

RECORD RETENTION AND DESTRUCTION
CURRENT BEST PRACTICES

August 8, 2003

TABLE OF CONTENTS

PAGE

RECORDS RETENTION - AN ESSENTIAL PART OF CORPORATE COMPLIANCE

By R. Thomas Howell, Jr. and Rae N. Cogar[1]

It is impossible for an organization to achieve acceptable legal compliance without an appropriate and functioning records retention program, for two distinct but important reasons:

1. Records retention is an important substantive component of many of the laws with which most corporations must comply; and

2. Retained records are often the vehicle by which compliance is established.

As stated in "Documents, What Documents?" by Michael E. Arruda, Margaret Prinzing and Shruti Rana, January/February 2003 issue of Business Law Today at page 23, a good policy typically has two principal elements: (1) "a schedule identifying the retention periods (minimum and maximum) for all documents covered by the policy," and (2) a "framework for the administration of the policy…"

Determination of the schedule of appropriate legal retention periods involves consideration of both federal and state regulatory requirements, contractual obligations, intellectual property requirements and statutes of limitations. These various legal requirements must then be harmonized with business considerations, which may extend the legal retention periods. The records retention program must also deal with the demands of litigation, investigations and audits. Care must be taken not to violate regulatory or company privacy requirements, and a system must be in place to halt regular record destruction in the face of certain investigations and litigation.

Finally, as the Andersen/Enron situation so dramatically demonstrated, careful implementation of a document retention/destruction policy when "under fire" is critical. Failure to do so exposes an organization to multiple risks, including sanctions, considerable costs and adverse inferences.

---

[1] R. Thomas Howell Jr. is of counsel with Seyfarth Shaw in Chicago, IL. Rae N. Cogar is Senior Consultant with Cohasset Associates, Inc., Hamburg, N. Y.

Developing the appropriate substantive records retention policy may be easier than appropriately and consistently implementing it. Implementation involves training and education, capability assessment, assigning and monitoring responsibility and updating the policy to ensure that it reflects current legal requirements and business needs.

WHAT IS A BUSINESS RECORD?

Every company should define what constitutes a business record. Having a definition will make operational recordkeeping decisions easier. Records are created for a variety of reasons, including: complying with government regulatory or statutory reporting requirements, documenting daily business activities, documenting research and development methods for possible patent applications, as well preserving the legal rights of the business. For whatever reason a record is created, there is a useful life of that record -- a period of time when the record is important for business decisions.

Although the balance of this paper will deal with those items that are determined to be records, consideration should also be given to everything else. Every organization's files, hard drives and other repositories contain a great deal of material that will not be designated a "record," for business purposes, and subject to the record retention policy. The retention policy should also identify this information and provide guidance on what to do with this material. Such material might be drafts, records retained only for informational purposes or personal material. For the most part and for several obvious reasons, such material should be purged pursuant to a consistently followed program or policy at regular, frequent intervals. It should be noted that computer systems create records and systems that back them up on a regular basis and those records would be considered a business record for Information Technology departments as they provide information on the functioning of the computers.

There must be a well-defined method for managing material defined as records – retaining what is needed and eliminating what is not. While a standardized methodology has been developed for creating records retention programs, there is no off-the-shelf program that can be installed one day and in use the next. Each retention policy is created to the specifics of the individual business. Although there are many records management software programs available, the results of these programs rely on information contained in the company's records retention policies and procedures. Developing that information is a significant undertaking.

BEGINNING THE PROCESS

Inventory

The place to start is the development of a records retention schedule. This is done by identifying what records a business has through a records inventory. The inventory includes records created by all departments and users, in all media formats, and found in all locations. Once the inventory has been completed, how long each record is to be retained must be determined. Records that are created to comply with federal or state regulatory and reporting requirements will have the same retention requirements for most businesses. However, accounting records created by Company A may not have the same retention requirement as similar records created by Company B due to the difference in the internal use of those records. Typically, specific legal requirements apply to less than 25% of a business' records.

Index

To find records in a timely manner, quality indexes must be maintained of all record holdings. This includes not only the active and inactive records, but documentation pertaining to the destruction of records. Only with these types of records, and the proper authentication thereof, can the bona fides of a good record retention policy be established.

RETENTION CRITERIA

Legal Factors

One important factor to understand is that retention periods stated for any regulatory or statutory purpose are considered minimum retention periods – the shortest period of time a record must be held. Legally compliant retention schedules should be viewed as the time when disposing of a record can first be considered, rather than when you must dispose of a record. Decisions are frequently made to retain records longer than their prescribed minimum due to other factors; an on-going business use, internal audit requirements or historical value. Whenever retention periods are lengthened, a determination must be made identifying the potential risks and costs to the company. It is also desirable to review pertinent statutes of limitations when determining records retentions. Statutes of limitations define the time period an organization can sue or be sued on a matter, or the time period in which a government agency can conduct an investigation or audit. While statutes of limitations in themselves are not required retention periods, they should be a factor in determining risk for a company when deciding how long to retain records. A decision can also be made to eliminate

records before the prescribed minimum retention period has run. Such a decision will have its own set of risks that should be carefully considered. All decisions relating to extending or shortening prescribed retention periods should be documented and retained. This documentation will help others to understand why such decisions were made, which may be pertinent in subsequent litigation to support the reasonableness of the records policies, as the cases discussed below demonstrate.

Business Factors

By understanding how a record is used within a company, better decisions can be made about the retention of that record. The best method to determine a record's retention is using the team approach -- a team that includes the records manager, legal counsel, business manager, technology manager and a representative from the area or department that creates or uses the record. The collective knowledge of this team will enable informed records retention decisions.

Implementation

Once retention periods have been determined, agreed upon and signed off by management, the next step is to develop the policies and procedures that will govern the implementation of the schedules. One of the most important policies relates to the suspension of records destruction in the event of imminent or current litigation, receipt of subpoenas, government inquiries, audits, or any other type of event that might warrant such action. When the records may be needed beyond the defined retention period, a methodology should be in place which *immediately* notifies all appropriate persons of these actions. These persons might include legal counsel, the records manager, a departmental manager and the IT manager, especially to preserve electronic records. Depending on the matter, such notification may include everyone in the company.

ELECTRONIC RECORDS

Is There a Difference?

Electronic records compound the issues involved in the overall management of records because there are frequently multiple copies in multiple locations. A business decision must be made to identify who is the responsible party for retaining electronic records – is it the creator or the user of the document, is it the sender or the recipient of e-mail? A widely applied rule is that the creator of the document, either an e-mail or other electronic record, has the responsibility for retaining that document in the "official" electronic file cabinet. As many companies do not utilize record keeping software, there should be space on the

company network aligned to the hard copy filing schema that permits saving the documents for long-term use, which would include transferring pertinent e-mail records -- received or sent -- from the e-mail system into the electronic filing cabinet. Ask the question -- if the document were in paper format, what would be done? If it would be filed in the official file, then the electronic version deserves the same respect and should be placed in the official electronic file. If the paper version would be thrown away, the electronic version should be deleted from the in-box. Recipients of outside e-mail which has legitimate business content should file those e-mails in the same manner.

Rogue Copies

Even when a policy is followed conscientiously for filing or deleting the official electronic record, there may still be rogue copies – copies being held in other work stations within the company and copies that were sent outside the company. Is it possible to effectively destroy all copies of an electronic document when its retention period expires? In most instances the answer is -- no. A reasonable attempt should be made to remove unnecessary electronic records, per the retention schedule in all identified electronic repositories. Employee education, together with approved policies and procedures, will help reduce the number of copies being saved individually. The key is to have approved policies and procedures in place, employees trained in their responsibilities, and program audits conducted on a regular basis to ensure full compliance with the policies in the regular course of business.

Obsolescence

Another critically important factor to be considered for electronic records is the inevitability of hardware, software and media obsolescence. These records must either be migrated to new versions or the old hardware and software must be retained in order to read the records. Migrating may also cause the records to change or lose their format, so good quality control procedures must be in place when migrating to ensure all information retains its original content, context and structure. The language in the laws that directly impact electronic records should also be reviewed when determining the retention method for electronic records. The Uniform Electronic Transactions Act (UETA) requires two elements for the retention of electronic records (See Section 12)

"(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference."

If a document does not accurately reflect the information as originally created and cannot be accessed for later reference, does that record then meet the requirement of the Act? Can it be considered a record for evidentiary purposes?

RECORDS DESTRUCTION

Follow the Policy

The destruction of records should always be done in accordance with the official records management policy. Such a policy will delineate the methods to be used to destroy records regardless of a record's location or storage media. Destroying records in accordance with an official policy in the regular course of business is always preferable to selective or arbitrary destruction, which is usually what occurs when there is no official policy. The caveat is that the disposition policy must utilize retention schedules – ones that are up-to-date, reviewed regularly and revised. Having a five-year old policy that has never been reviewed and is not consistently followed is no better than having no policy. In fact, a court may determine there is no policy if it finds a lack of consistency in its application.

As long as records are retained, they are legally discoverable, regardless whether their retention period has expired. If the records are in the possession of the company, they are discoverable. Searching for documents responsive to a discovery request when every record ever created is retained will be time-consuming, expensive and labor intensive. If records are no longer of use in the business context and there are no statutory, regulatory or investigative reasons to retain them, then it is in the company's best interest to dispose of them.

Destruction of Electronic Records

What about the destruction of electronic records? What level of "destruction" is necessary to comply with a retention program and yet not be required to perform extraordinary methods to recreate records in the event of future litigation - such as requiring forensics investigators to recreate deleted data? Once records are deleted from the electronic system per the retention schedule, should that be enough to stop a review of electronic data for future litigation or investigation? Although there is limited guidance on this topic, the appropriate standard should again be reasonableness. Is it reasonable to just delete the electronic pointers

from the system and allow the system to overwrite the material in the regular course of business or should other methods of destruction be used? The industry standard seems to indicate that an overwrite of seven (7) times with random zeros (0) and ones (1) will adequately obliterate the data from most recovery attempts. Is it necessary to use that level on all material?

The media type must be considered, such as optical disk, write once read many (WORM) technology, or electronic/magnetic tapes. Different media require different disposition instructions to assure that the data has been effectively deleted.

RECORDS MANAGEMENT CASES

Below are four cases that provide some insight into what courts may be looking for when making decisions regarding inappropriate destruction of records and company record retention policies. These cases touch on different aspects of records management: the Carlucci court decision deals with the use of a document destruction policy, rather than a document retention policy; the Lewy court addresses unreasonably short time periods assigned to certain record types within a record retention program, allowing for their premature destruction; the Prudential court focuses on the responsibility of senior management in notifying employees of on-going litigation and their duty to preserve documents, and Zubulake offers a current, coherent approach to the thorny task of how to handle the voluminous electronic material that litigants are finding to be physically available for discovery.

In Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472 (S.D. Fla. 1984), Piper consistently ignored the requests for production of documents by the Plaintiff, requested extensions to produce the documents which were granted numerous times by the court, and finally was sanctioned by the court for showing an "obstructionist attitude toward production of the materials." According to testimony by Piper employees, "the stated purpose of the destruction of records was the elimination of documents that might be detrimental to Piper in a law suit…" Thereafter, the destruction of all potentially harmful documents was an ongoing process.

Piper further admitted that it had destroyed documents despite a court order requiring their protection. The court found "Piper has utterly failed to demonstrate that its document retention policy is actually implemented in any consistent manner. … Piper's absolute failure to provide any evidence on this issue must be construed as a tacit admission that the policy is a sham." Id. at 485. The Plaintiff had moved for default judgment against Piper, which was granted.

On the other hand, the court did state it was "not holding that the good faith disposal of documents pursuant to a bona fide, consistent and reasonable document retention policy can not be a valid justification for a failure to produce documents in discovery."

In In re Lewy v. Remington Arms Co., Inc., 836 F2d 1104 (8th Cir. 1988), the court had given instructions to the jury that because Remington had failed to produce documents, they could infer that those documents could have been harmful to Remington's case (a so-called "adverse inference"). Remington argued that the documents had been destroyed pursuant to its records retention policy. The records in question were customer complaints and gun examination reports. Under the retention policy, these records were "required to be retained for a period of three years and if no action regarding a particular record was taken in that period it was destroyed."

On appeal, Remington objected to the instructions, arguing that "destroying records pursuant to routine procedures does not provide an inference adverse to the party that destroyed the documents." The Appeals Court did not decide the issue but remanded the case to the trial court for retrial. The court did, however, instruct the trial court what to consider:

> "First, the court should determine whether Remington's record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents. For example, the court should determine whether a three year retention policy is reasonable given the particular document. A three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints. Second, in making this determination the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints. Finally, the court should determine whether the document retention policy was instituted in bad faith." Id. at 1112.

It went on to state: "if the corporation knew or should have known that the documents would become material at some point in the future then such documents should have been preserved. Thus, a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."

In In re Prudential Inc. Co. of America Sales Litig., 169 F.R.D. 598 (D.N.J. 1997), the court issued sanctions based in part on the failure of senior management to properly manage the discovery process and to prevent document destruction. The court found, after reviewing the facts, that, "It [Prudential] has no comprehensive document retention policy with informative guidelines and lacks a protocol that promptly notifies senior management of document destruction. These systematic failures impede the litigation process and merit the imposition of sanctions". Id. at 617. Under this order, Prudential was fined $1 million, and was required to take other constructive actions throughout the time of the lawsuit which included notification of the action to all employees.

During the discovery process in this case, a class action lawsuit alleging Prudential used deceptive sales practices in the selling of life insurance, Prudential was ordered to "preserve all documents and other records containing information potentially relevant to the subject matter of this litigation." Prudential had relied on its e-mail system as a method to caution employees against document destruction, but had failed to mention the class action litigation which was pending. During employee depositions it was discovered that many employees did not have e-mail access and those employees who had received the notices did not distribute them to employees without access, and some notices were not sent to all divisions. The court also found that using the e-mail system as a method of notice to employees to preserve documents and prevent destruction was ineffective and a failure to implement the Court's preservation order.

It went on to say: "When senior management fails to establish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of field office actions. The obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers. …" Id. at 615.

In Zubulake v. UBS Warbug, 2003 WL 21087884 (S.D.N.Y. May 13, 2003), the Plaintiff, in a gender discrimination suit against her former employer, requested that Defendant produce all documents "concerning any communication by or between UBS employees concerning Plaintiff." Defendant produced approximately 350 pages, including 100 pages of email. Plaintiff claimed to know that there were some records that had not been produced, because she had copies of relevant documents that had not been produced. She therefore asked for production of archived documents, which Defendant resisted on the grounds of expense.

In this context, Judge Scheindlin set forth a seven part test, with the factors listed in the order they are to be weighted:

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

2. The availability of such information from other sources;

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

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

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

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

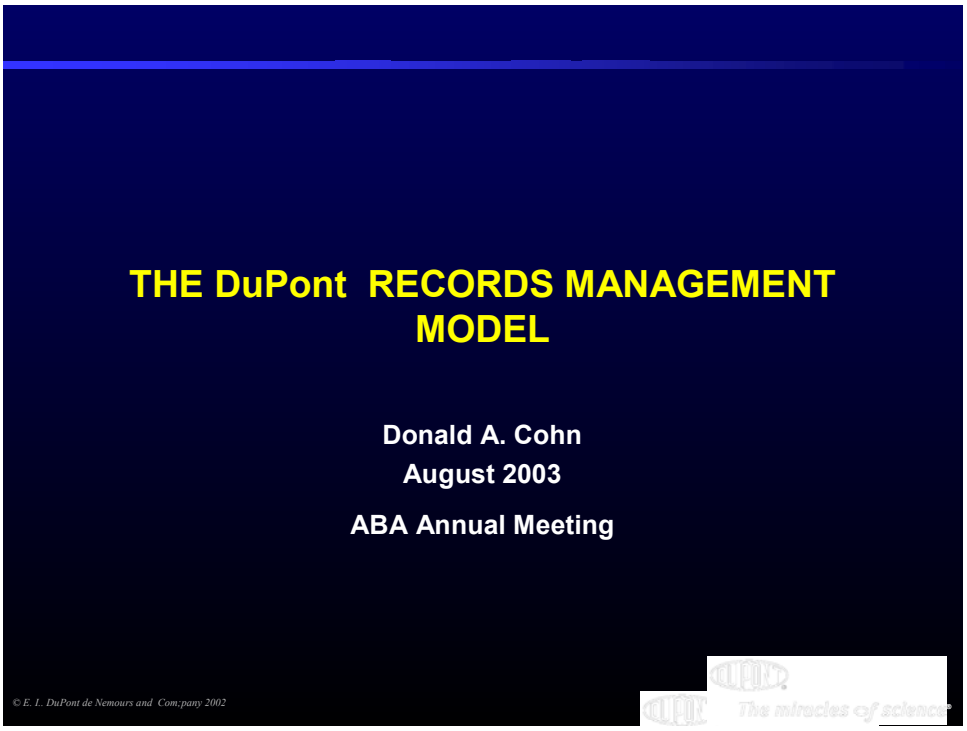
7. The relative benefits to the parties of obtaining the information.

The court ordered Defendant to produce all responsive e-mails existing on its optical disks and active servers, and five backup tapes (selected by Plaintiff), all at Defendant's expense. It stated that only after reviewing the contents of the backup tapes and the expenses related thereto would the court conduct its cost shifting analysis.

Summary

No compliance program is complete without a good record retention policy. The migration of many records to various electronic formats and media, and the legal developments in the Andersen/Enron matter, signal that now is the time for all corporate lawyers to review their clients' record retention policies to ensure that they are current, practical, comprehensive and functioning.

THE DUPONT RECORDS MANAGEMENT MODEL


THE DuPont RECORDS MANAGEMENT MODEL
Donald A. Cohn
August 2003
ABA Annual Meeting
© E. L. DuPont de Nemours and Con;pany 2002
The miracles of science

DUPONT CRIM PROGRAM

- Policy
- Issues
- Components of the Program
- Challenges

Policy

- Applies to All Records
- Responsibility & Accountable
  - Employees: Records in their Possession or Under Their Have Control
  - Line Management: Managing & Implementing Within Their Span Of Control
  - Corporate Management: Entire Program

Policy

- Permissive Retention
  - Keep Business Records For Up To 3 Years
  - Can Be Destroyed At Any Time
  - E Mail
- Mandatory Retention
  - "Schedule A" Records
  - UFTA
  - Legal Hold Orders
  - Regulatory, etc. Requirements

Policy

- Program Variances By Line Management
- All Applicable Regional Laws Will Be Followed

ISSUES

- Copies of Records
- Records Retention Period Determination
- Leaving the Company
- Inherited Records
- Custodial Records
- Records For Acquisitions, Divestitures & Mergers
- Joint Ventures and Subsidiary Records

COMPONENTS OF THE PROGRAM

- Administered by Corporate Records & Information Group
  - Central Group in Wilmington
  - Champions/Coordinators in SBU's, Function's, & Regions
  - Monthly Audio's
  - Quarterly Meetings
  - "The Glue"
  - Mantra "Creation, Implementation, Institutionalization"

COMPONENTS OF THE PROGRAM

- Swing Into Spring
- Janitor & Records Manager Information
- Ration Server Space

- CRIM and Network Activities
  - Educational Awareness
  - Records Retention Schedules Updates
  - Variance Procedures and Counsel
  - Distribution of Legal Hold Orders
  - Proper Disposition
  - Strategic Planning

COMPONENTS OF THE PROGRAM

- Addressing New Issues
- Review, Audit, & Report To Corporate Management
  - Internal Auditors
  - Special Records Audits
- Preservation of Historical Records
- Preservation of Vital Record

CHALLENGES

- ASP's/Outsourcers & Records Management
- Privacy & Records Management
- E-Contracting & Records Management
- The Supply/Value Chain & Records Management
- Discovery Issues
- The Future

EXCERPT FROM DUPONT
RECORDS MANAGEMENT GUIDE

Contents

NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION.

*NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION..

Introduction

Proper records management is an important function of every successful corporation. An effective records management program ensures that all records that are required to conduct the business of the corporation, to fulfill its legal responsibilities, and to support its tax liabilities are maintained and available.

An effective records management program also preserves the

corporate memory and protects the corporation by ensuring compliance with local and federal laws.

Significant costs are associated with the creation, maintenance, distribution, and storage of records. Therefore stewardship must be exercised by producing clear, concise documentation only when there is a business requirement. Refer to the "Corporate Business Writing Guide" for addi-tional information.

An alphabetical index is located at the back of this guide, which can be used to help you locate specific record names.

The information in this guide is also available on our Intranet Web site at _____ The Web site features a searchable special records retention database that can be used to find information about special records retention periods.

Purpose of This Guide

This guide sets forth policies and principles and describes the records management program so all employees can better manage DuPont's business records. It is intended to provide ways to identify, maintain, and dispose of company records in a timely and cost-effective manner.

This guide does *not* apply to published information such as journals, government regulations, books, vendor brochures and catalogues, or any other public information. However, in the interest of space and information management efficien-cies, as well as housekeeping considerations, these records should be managed in a cost-efficient way. All copyright laws concerning making copies must be followed. Corporate Records Management Program Guide

March 19997

Records Management Policies for DuPont Employees

All employees are responsible and accountable for the records in their possession and those records for which they have control.

All local and federal laws will be followed by every DuPont employee during the creation, retention, and disposition of company records.

DuPont line management is responsible and accountable for managing and implementing the Corporate Records Manage-ment Program as set forth in this guide.

Every effort has been made to identify the legal requirements for recordkeeping in the United States. However, in keeping with the policy that all local and federal laws be followed in regard to creating, retaining, and destroying records, employ-ees

and line management are accountable for identifying those areas that differ from the instructions in this guide.

Basic Principles of DuPont Records Management

Definition of a Record

All records created or received in the ordinary course of DuPont business are DuPont records, are the property of DuPont, and are subject to this guide. This pertains to *all* forms and *all* media, including:

• handwritten, typed, or printed documents on paper
• electronic documents (e.g., e-mail, Web sites, diskettes, CDs)
• video
• audio
• graphic representations
• network servers and document management systems

Note: A date must appear on all documents to keep records in context and to facilitate compliance with the records management program..Corporate Records Management Program Guide 8 March 1999

Copies of Records

If an official copy of a Special Record has been identified, any other copy of that record may be classified as a General Business Record (Max. 3 years). In no instance shall a copy of a record be kept longer than the official record.

Records Retention Periods

Retention periods vary by records category and are deter-mined by considering business use, tax liability, and legal requirements.

When to Destroy a Record (or Not)

A date must appear on all documents to keep records in context and to facilitate compliance with the records manage-ment program.

All DuPont business records must be properly destroyed at the end of their records retention period unless corporate management:

• has approved a variance to preserve them for business need (refer to “Variances”)
• has classified them for historical preservation (refer to “Preservation of Historical Records”)
• has identified them as subject to litigation or governmen-tal proceeding (refer to “Distribution of Legal Hold Orders”)

Leaving the Company

Upon retirement or separation from DuPont, each employee must return all DuPont records to the corporation. Line management will determine disposition by reassigning the records or properly destroying them according to the records retention described in this guide. Corporate Records Management Program Guide March 1999

Inherited Records

Records that were previously managed by someone who left the company or changed job responsibilities and are now someone else's responsibility are referred to as inherited records. As soon as these records become another person's responsibility, they must continue to be reviewed and main-tained according to this guide.

Additional Records Considerations

Custodial (Contractor) Records

Custodial records are records that are maintained by service organizations such as outside law firms, engineering contractors, accounting firms, or information technology firms. These records are either received from DuPont or prepared for DuPont and maintained by the contractor. These records belong to DuPont and are subject to compliance with our records management program. In addition, they may not be modified, destroyed, or even microfilmed without permission from DuPont.

Records from Acquisitions, Divestitures, and Mergers

Ownership of these records should be addressed in the acquisition, divestiture, or merger contract.

Joint Ventures and Subsidiaries

Because DuPont has an interest in the success of such organi-zations, each subsidiary or joint venture must have a viable records management program. Each situation is unique. Seek the advice of each organization's legal department when setting up a records management program. This Corporate Records Management Program can be used as a model; however, be sure the name of the joint venture or subsidiary appears on its records management program documents. Corporate Records Management Program Guide

10 March 1999

Components of the Program

A comprehensive records management program is administered by the Corporate Records and Information Management (CRIM) Group. The program components are described in this section.

Education and Awareness

Education and awareness of the Corporate Records Manage-ment Program will be implemented by the records analysts in the CRIM Group along with a network of records manage-ment champions. Each business has a champion who is accountable to the VP/GM or VP of that organization.

Records Retention Schedule

There are two types of records that employees must under-stand to properly manage their records—"General Business Records" and "Special Records." The retention schedule provides guidance for categorizing and describing all records and assigning a retention period for each.

General Business Records

All DuPont records may be kept for a period not to exceed three years (Max. 3 years) after the record creation date. All DuPont records are in this category unless identified as a Special Record.

Special Records

Special Records have a business, tax, or legal requirement that is more than three years. These records are in the Special Records Retention Periods listed in this guide. An explana-tion of the retention periods is also included.

Note: "Just in Case" is *not* a valid records retention period. Corporate Records Management Program Guide

March 1999 11

Review and Audit

An annual records *review* must be done by all employees who maintain company records. A "Swing Into Spring" program is coordinated between the CRIM Group and each business to ensure proper records management. The program highlights the benefits of the campaign and provides the time for all employees to review their DuPont records.

All records, both electronic and hardcopy, that have an expired retention period must be disposed of properly.

It is each employee's responsibility to ensure that Special Records are not destroyed prematurely. Special attention should be given to records that need to be held for tax or legal purposes.

In addition to periodic reviews, *audits* shall be performed and results reported as requested by the CRIMGroup.

• The self-assessment is designed to educate employees about the Corporate Records Management Program and help them perform an audit of the records under their control.

• An internal records audit is performed by a team within

each business. Internal records audits are also done by the CRIM Group.
• External records audits will be performed by an outside organization on an occasional basis. These audits will be contracted for and managed by the CRIM Group at the request of the Operating Group.

Proper Disposition

Records should be disposed of according to the level of confidentiality or content of proprietary information.
• Records with no personnel or proprietary information can be thrown in with the regular trash pickup.
• Records containing personnel or proprietary information must be shredded, incinerated, or pulped. The security of the proprietary information should be monitored until destruction is actually performed..

Distribution of Legal Hold Orders

The CRIM Group works with Legal to ensure that everyone who has records relating to pending or active litigation or government investigation is aware of the matter. Employees must then notify Legal and identify those records that must be held pending the resolution of that matter. In some instances a single record could be held for more than one matter. When the Records Hold Order is lifted, the records revert to their original categories and may be destroyed according to the retention schedule.

Preservation of Vital Records

Vital Records are included in the Corporate Records Manage-ment Program and as such are subject to the same retention guidelines. Vital records are those required to establish the:
• corporation as a legal entity (e.g., Articles of Incorpora-tion)
• corporation's fiscal and accounting position (e.g., SEC Filings)
• primary legal obligations to and of the company (e.g., Contracts)
• basic research, technical, and development know-how of the company (e.g., Laboratory Notebooks)
• basic processes, production, and operating expertise of the company's primary engineering, construction, and flow chart records (e.g., Engineering Drawings)
Each business is responsible for specifically designating their vital records. The Vital Records Group consults with the business to decide the best safeguarding method for each record.

The primary records protection method used is “geographic dispersion.” This is where the original record is kept in a different location from the electronic, paper, or microfilm copy..Corporate Records Management Program Guide March 1999 13

Preservation of Historical Records

The Hagley Museum and Library is the holder of DuPont Company historical files, dating back to 1802. The CRIM Group coordinates the gathering of records of historical significance after they have met the retention period for business, legal, and tax reasons.

After approval is given by the owners of the identified records, they are donated to Hagley and made available for scholarly research 25 years after the date of the document. Any request to view the records before that time must be approved by Legal.

Records having permanent historical value include:

• records documenting corporate managerial functions
• financial records, including audit reports, balance sheets, and statements
• records documenting key strategic decisions and changes in corporate structure
• records documenting key corporate activities
• documentation of the relationship between DuPont and its customers, society, and government
• photographs depicting work processes, innovative tech-nologies, plants, and worker housing

Records Storage Accountability

CRIM manages a contract with a national records manage-ment company that provides storage and retrieval services. Contact the CRIM Group for up-to-date information on locations and rates.

Most paper records are stored at a Wilmington facility. The records are protected against fire, water damage, theft, and vandalism. The temperature range of the facility is 60–90°F. Microfilm and electronic media are stored in a climate-controlled building maintained by DuPont..Corporate Records Management Program Guide 14 March 1999

Variances

In a limited number of cases, DuPont records may be retained **beyond** the General Records or Special Records retention periods, as appropriate, but only upon an affirmative demon-stration of business need by the employee wanting to retain the record. The burden and responsibility of requesting and

justifying an extension rests with the employee. Line man-agement has the responsibility of determining the appropri-ateness of the requested variance and the length of additional time to retain the record.

The Corporate Records Management Group will assist line management as a resource to provide guidelines and share experiences..Corporate Records Management Program Guide

Special Records Retention Periods

Retention periods for Special Records are:

• **Max. "x" number of years** means that a record may be destroyed anytime up to and including "x" years.

• **"x" number of years** means that the record must be kept for exactly "x" number of years. In the interest of effi-ciency, that can be interpreted as "x" number of years plus the current year so that file cleanup can be done once a year.

• **"x" number of years after an event** means that the record must be kept for exactly "x" number of years after the event (such as termination, completion of all obliga-tions, or settlement of claims) occurs.

• **Until Superseded** means that when a new revision is issued, the previous one should be destroyed. In some cases, one historical copy may be maintained, as noted in this section.

• **Until Obsolete** means that a record is held until no longer needed for business purposes.

• **UFTA** means Until Completion of Federal Tax Audit. Contact local management or the CRIM Web site for current information.

• **UFTA/"x" years** means that both retentions must be satisfied.

• **UFTA—an event such as closing or expiration** means that the UFTA is related to the year of the event.

• **For Life of Facility** means for as long as DuPont owns the facility or has retained control over it.

• **For Useful Life of Product** means for as long as DuPont manufactures a product plus the period of time that the product is used as intended.

• **Max. Permanent** refers to records that have long-term value and may be kept permanently but need not be.

[Schedules Deleted]

Electronic Evidence & The Sarbanes-Oxley Act of 2002[1]

By Michele C.S. Lange[2]

In response to the recent series of highly publicized business scandals, Congress passed the Sarbanes-Oxley Act.[3] President Bush signed the Act into law on July 30, 2002. The legislation aims to strengthen accounting oversight and corporate accountability by enhancing disclosure requirements, increasing accounting and auditor regulation, creating new federal crimes, and increasing penalties for existing federal crimes.

Similar to other areas of the law, Sarbanes-Oxley embraces the issues developing around the proliferation of electronic evidence. With 93% of all business documents created electronically and only 30% ever printed to paper, corporations in the last few years have been compelled to address the retention of and potential liability associated with electronic documents and communication. For example, 10 years ago, corporations tended not to keep many hard copies of documents because paper documents take up physical space. Now, companies save nearly every electronic document and email because it can be stored electronically with relative ease. In response to this techno-reality, corporations are implementing and enforcing document retention policies more than ever before.

Yet, the reality is that outdated email, antiquated files, and archival data stored on backup tapes or disks are often kept for months or years past their useful life. Case law reveals that unwieldy preservation of all electronic data and email created in the course of business can come back to haunt a corporation when litigation ensues. For example, in *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D. La. Feb. 19, 2002), the court stated, "Fluor's e-mail retention policy provided that backup tapes were recycled after 45 days. If Fluor had followed this policy, the e-mail issue would be moot." As a result of Fluor's unwieldy document retention, the parties spent considerable time and money arguing the discoverability of email messages which should have been destroyed.

---

[2] Michele C.S. Lange, mlange@krollontrack.com, is a Staff Attorney for the Electronic Evidence Services division of Kroll Ontrack, Inc. www.krollontrack.com

[3] http://financialservices.house.gov/media/pdf/H3763CR_HSE.PDF

Sarbanes-Oxley imposes new requirements on public companies and their accounting and auditing teams in regards to the retention and destruction of certain financial records. This article outlines and analyzes some of the Act's key provisions as they relate to electronic evidence.

What provisions are most concerning in regards to electronic documents?

Document Alteration or Destruction. §802 of the Act amends the Federal obstruction of justice statute by adding two new offenses. First, persons who knowingly alter, destroy, mutilate, conceal or falsify any document or tangible object with the intent to impede, obstruct, or influence proceedings involving federal agencies or bankruptcy proceedings may be fined, imprisoned up to 20 years, or both.

Mandatory Document Retention. Second, §802 directs (1) accountants to maintain certain corporate audit records or review work papers for a period of five years from the end of the fiscal period during which the audit or review was concluded and (2) the SEC to promulgate, within 180 days, any necessary rules and regulations relating to the retention of relevant records from an audit or review. This section makes it unlawful to knowingly and willfully violate these new provisions (including any rules and regulations promulgated by the SEC) and imposes fines, a maximum term of 10 years imprisonment, or both.

Obstruction of Justice. §1102 of the Act expands the obstruction-of-justice statute that prohibits tampering with witnesses. Now acting or attempting to "corruptly" alter or destroy a record or other object "with the intent to impair the object's integrity or availability for use in an official proceeding" is punishable with fines and/or imprisonment of up to 20 years.

What is the impact of these provisions?

The impact of Sarbanes-Oxley on electronic data management is basically two-fold. The first part of §802 places criminal liability on any person who knowingly destroys documents or objects relating to a Federal agency or Chapter 11 Bankruptcy. §1102 prohibits persons from corruptly altering or destroying documents with the intent to impair an official proceeding. The definition of "document" in these statutes is likely to be interpreted to include electronic document destruction. Given its breadth, these provisions give the Federal government authority to prosecute cyber-crimes and other computer hacking which results in information destruction relating to official proceedings.

Past case law reveals the Federal government's commitment to using computer forensic tools to bring hackers and cyber-criminals to court. For example, in *U.S. v. Lloyd*,[4] the Defendant was convicted under 18 U.S.C. § 1030 (Fraud and Related Activity in Connection with Computers) on one count of computer sabotage for planting a computer-based "time-bomb" in his employer's computer systems. Computer experts were essential in recovering the evidence of the "time bomb." This new provision of Sarbanes-Oxley is only likely to expand that governmental commitment to using computer forensic protocols to prosecute cyber-crime.

Further, §802 of Sarbanes-Oxley is likely to have great effect on how accounting and auditing firms handle electronic documents. Most accounting firms already retain audit and review records for at least five years, so it is perceived that the second portion of §802 might have minimal impact. However, §802 specifically references the retention of electronic records (such as workpapers, memoranda, correspondence, etc.) that are created, sent, or received in connection with an audit or review. This provision could require many accounting firms to retain more documents than they have retained in the past. Further, the §802 document retention rules and regulations to be implemented by the SEC also could force accounting professionals to give more consideration to their current electronic records policies. The breadth and depth of these rules remains to be seen.

In complying with the new provisions of Sarbanes-Oxley, accounting and auditing firms should consider electronic records when determining what should be retained and what should be destroyed. The financial industry is not the only business sector affected by the dangers of digital data, however. All business organizations should bear in mind that retained and deleted electronic evidence could become intricate minefields of liability. Even if data is effectively deleted and overwritten from a hard drive, this still does not mean that it is gone for good. Documents that have been copied to other media, saved in a routine system backup, or emailed to any one else, have effectively been copied over and over again creating numerous replicas of the "electronic footprints."

Accounting and auditing firms can mitigate the risk associated with electronic information management by creating a document retention policy.[5] The policy

---

[4] *United States v. Lloyd,* 269 F.3d 228 (3rd Cir. 2001).

[5] *See* Daniel I. Prywes, "The Sarbanes Oxley Act Raises the Stakes for E-Records Management" *Digital Discovery & E-Evidence*, October 2002 at 1.

should start with an electronic information inventory of the firm's electronic framework, including documentation of:

- all electronic hardware and software in use throughout the company (including, cell phones, PDA's, laptops, etc.),
- all locations and storage formats of archived electronic data, and
- all methods in which data can be transferred to/from the company.

The bulk of the retention policy should include methods for classifying documents, determining retention periods, setting the retention schedule and procedures, and selecting a records custodian. The policy should also create an index of active and inactive records and implement "log books" in which all destroyed documents are recorded. Most importantly, an organization must retain all relevant documents when they know or should have reason to know that the documents will become material at some point in the future.

Conclusion

In conclusion, the Sarbanes-Oxley Act compels public companies, corporate counsel, and accounting/auditing professionals to consider the impact of electronic evidence in relation to certain financial records. No longer can emails and computer files be blindly destroyed. Instead, balance must be found between appropriate destruction of stale and non-regulated documents and adequate preservation of potentially significant documents. Such balance is the key to effective electronic document management and the protection of informational assets as required by this new law.

Top Ten Tips for Effective Electronic Data Management

Sarbanes-Oxley reinforces the reality that electronic data management should garner top-priority for corporate leadership, corporate counsel, and accounting/auditing professionals. Kroll Ontrack has created the following ten tips that should be considered when developing and maintaining rules for electronic record retention:

1. Make electronic data management a business initiative, supported by corporate leadership.
2. Keep records of all types of hardware/software in use and the locations of all electronic data.

3. Create a document review, retention, and destruction policy, which includes consideration of: backup and archival procedures, any online storage repositories, record custodians, and a destroyed documents "log book."

4. Create an employee technology use program, including procedures for: written communication protocols, data security, employee electronic data storage, and employee termination/transfer.

5. Clearly document all company data retention polices.

6. Document all ways in which data can be transferred to/from the company.

7. Regularly train employees on your data retention policies.

8. Implement a litigation response team, comprised of outside counsel, corporate counsel, human resources department, business line managers, and IT staff, that can quickly alter any document destruction policy.

9. Be aware of electronic "footprints" – delete does not always mean delete, and metadata is a fertile source of information and evidence.

10. Cease document destruction policies at first notice of suit or reasonable anticipation of suit.

On a final note, make a practice of conducting routine audits of policies and enforcing violations.

Challenges for Corporate Counsel in the Land of E-Discovery: Lessons from a Case Study[1]

By Daniel L. Pelc and Jonathan M. Redgrave[2]

Introduction

"Bad facts make bad law"[3] is a maxim oft used to dismiss unfavorable decisions absent careful analysis but well employed to describe the emerging jurisprudence regarding electronic discovery, and the many examples of missteps in discovery that have led to significant sanctions.[4] If only these cases and sanctions could be dismissed by a maxim and distinguished on their facts.

The better practice is to discover the important lessons that diminish, if not preclude, the onerous consequences. This article addresses the case of Danis v. USN Communications, 2000 WL 1694325 at 2 (N.D. Ill.), which provides a number of valuable lessons concerning electronic discovery for corporate and outside counsel, many of whom are addressing such issues for the first time.

The Danis Case

Danis v. USN Communications, was decided by the Federal District Court for the Northern District of Illinois on October 23, 2000. The pertinent facts of the case are as follows:

- The case was a class action involving two groups of purchasers of common stock issued by USN Communications. The plaintiffs alleged various violations of federal securities law. Id. at 7.

---

[1] This article originally appeared in the January 21, 2002, Vol. 3, Iss. 5, edition of *E-Business Law Bulletin*. Reprinted with permission of Andrews Publications © 2002. www.andrewsonline.com

[2] Mr. Redgrave is Of Counsel with the firm of Jones, Day, Reavis & Pogue in its Washington, D.C. office. The views expressed in this article are solely those of the author and do not reflect the views or position of the firm or any of its clients. Mr. Pelc is an Attorney with Ontrack Data International, Inc. and a frequent lecturer on E-Discovery issues.

[3] See Ludwig v. State, 298 S.W.2d 166, 170 (Tex. Ct. App. 1956)

[4] See, e.g., In re Prudential Ins. Co. Sale Practices Litig., 169 F.R.D. 598 (D.N.J. 1997) (sanction of $1,000,000 for destruction of electronic data) and Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. June 16, 1999) (sanction of spoliation instruction and adverse inference to jury).

- The suit specifically named USN Communications, as well as Mr. Elliott, the Chief Executive Officer and the Board of Directors in addition to others. Id.

- Prior to the commencement of the action, USN did not have a formal document retention policy covering the categories of documents and electronic information USN regularly created and received. Id. at 39.

- USN routinely created backup tapes that were stored on computers. Id. at 11. USN maintained copies of these back-up tapes only for a period of about thirty days to facilitate disaster recovery; the tapes used to make these copies were then reused. Id. The court found that these back-up tapes were not intended to, and did not, create an archival record of the e-mail system. Id.

- Three months prior to the filing of the complaint, USN put into place a set of procedures for "preserving company assets and retrieving key records in anticipation of upcoming office closures and layoffs. This process involved deleting computer information. Id.

- Additionally in the summer of 1998, the company embarked on a program of purging the computer drives of terminated USN employees in response to security concerns and to preserve computer storage space. This process also involved the deletion of data. Id. at 12.

- On the same date that the complaint was filed, the Board of Directors met and discussed the necessity of preserving documents for the case. Mr. Elliott, the CEO, was ordered to promptly take steps to preserve documents. Id.

- Mr. Elliott took no affirmative steps to ensure that no documents were destroyed. Mr. Elliott delegated all responsibility to Mr. Monson an in-house attorney with no litigation experience. Id. at 14.

- Mr. Monson did nothing to ensure that the directives were followed as to document preservation. Mr. Monson did not review the current actions of destroying documents of terminated

employees or those of closed offices to ensure that document destruction was being halted. Id.

- Electronic documents were apparently destroyed in accordance with pre-litigation practices.

- Plaintiffs filed a motion and amended motion for sanctions following discovery of the document destruction. Plaintiffs premised their motion on the assertion that "USN employees, acting at the direction or under the supervision of the individual defendants and USN's senior officers, destroyed virtually all evidence of the massive fraud alleged in plaintiff's complaint" As a sanction for this alleged misconduct, plaintiffs sought…default judgment. Id. at 2.

- The court opined that discovery occurred at a breakneck pace and neither side had a good handle on what was occurring in the process. Id. at 4.

Lessons Learned: Document retention plans must anticipate litigation and include contingency plans.

Many corporations and other entities have document retention policies under which they destroy at stated intervals documents for which they anticipate having no further need. Cedars-Sinai Medical Center v. Superior Court, 74 Cal.Rptr.2d 248, 257 (Cal. 1998.); see also Akiona v. U.S., 938 F.2d 158, 161 (9th Cir. 1991); Lewy v. Remington Arms Co., Inc., 836 F.2d 1104, 1111-112 (8th Cir. 1988). Regardless of the nature and detail of such a program, it must be designed to account for what happens when litigation is anticipated, threatened or filed.

The most practical step, of course, is the suspension of any disposal practices for documents impacted by the litigation. In Danis, this failed to happen. The court placed the blame for the failure on the corporate executive team, stating that "when senior management fails to establish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of field office actions." Danis, 2000 WL 1694325 at 32. The court further reiterated that the obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers. Id.

In order to assess the needs of the corporation and construct a plan for when e-discovery will occur, parties cannot act in a vacuum. Attorneys from outside counsel, in-house legal staff and individuals from different areas of the corporate structure must cooperate to develop retention programs in addition to litigation hold procedures and memorialize these plans in the document retention policy. The document should include delegations of authority among departments and a meaningful reporting structure.

Litigation Response Plan

This plan must be a key component of the document retention policy for the organization. It acts as a roadmap and an action plan for the litigation response teams discussed in the subsequent subsection. This plan must account for electronic documents, both created and anticipated, archived and non-archived. In terms of electronic documents, the foundation for the plan is the current network landscape for the organization, including site information, file saving protocols, back-up protocols, past application and operating system information and planning for segregation of server space in the event of ongoing discovery efforts. The plan must include methods for capturing data, protocols for file saving, following imaging, and back-up and archive access.

Litigation Response Teams

One of the key measures that would have alleviated the consequences in Danis is the implementation of litigation response teams prior to pending litigation. The teams should be comprised of individuals from the outside counsel, experts, legal department, human resources department and IT staff, as well as individuals from key departments within the organization. The purpose of the team is to follow through on the litigation response plan discussed in the preceding subsection. The team should be familiar with the document retention policies and the need for litigation "holds" for records, including electronic records. The IT staff will be critical to ensuring that no caches of electronic documents are ignored or forgotten.

Outside Counsel

It is critical to employ outside counsel knowledgeable and skilled in the area of electronic discovery.

In Danis, the court stated that Mr. Elliott, the CEO of the Defendant organization, did not consult its retained law firm that had "scores of experienced attorneys capable of developing and implementing a suitable document

preservation program in a major securities lawsuit." Danis, 2000 WL 1694325 at 14. Instead, Mr. Elliott entrusted this vital task to Mr. Monson, an attorney with no litigation experience and no experience in formulating document retention strategies. Id. There is no evidence that the Defendant consulted their outside counsel for any assistance in the formulation or execution of the retention plan whatsoever. Id. It was this breach of duty that resulted in the sanctions placed by the court upon Mr. Elliott.

Expert Technical Assistance

It is equally critical to obtain expert technical advice to assess document retention and production issues in litigation.

The court in Danis stated that "neither side to this motion has demonstrated to this Court a complete mastery of what types of documents were generated by USN in the ordinary course of business, how they were used or their significance." Id. at 4. The court went on "as a result, both sides were the losers. They lavished huge sums of time and money on an issue that did not remotely justify the expenditure, and which would have been more profitable spent focusing on the merits of this case." Id. at 5. This summary aptly reflects the reality in many other cases: the failure to appreciate and understand electronic documents in litigation can lead to extraordinarily costly and wasteful efforts.

The forensic and discovery experts that focus on electronic discovery bring to bear experience and resources that are critical to meeting court obligations and litigation budget considerations. During the formation of the document retention policy, the electronic discovery expert can assist IT staff in assessing network structure and storage functions with an eye to any later need to locate and produce documents. Advance planning can result in more systematic storage that allows for narrowly tailored productions in litigation that can drastically reduce the costs of discovery compliance. Moreover, when faced with litigation demands, the electronic discovery expert can employ the specialized tools and personnel to locate and review documentation on a timely basis, avoiding unnecessary discovery battles that can prolong and derail litigation and can provide support for the company's due diligence in retention and production.

Corporate Leadership

Corporate leadership will be held responsible for document retention problems, including e-discovery mistakes.

The Danis court did not hesitate to impose sanctions upon the corporation and its officers for the electronic document destruction. Even though it refrained from imposing a default judgment, the court allowed an inference to the jury regarding the spoliation of evidence that presumes the evidence would have been harmful to the defendants. Id. at 53. Moreover, the court imposed a $10,000 fine on Mr. Elliott for his role in the mismanagement of the document retention issues, stating that Mr. Elliott may not "escape responsibility by virtue of the fact that he assigned Mr. Monson the task of handling document preservation. The buck must stop somewhere — and here, the Court believes that the appropriate place is with Mr. Elliott, the CEO." Id. at 41.

Conclusion

The Danis case is an example of the perils that are faced by any organization that does not take meaningful steps to address the preservation and production of electronic documents in litigation. Do not make the bad facts; do not make bad law. Know your electronic media; develop appropriate retention policies and schedules; plan for litigation contingencies; and follow through with prompt and efficient implementation.

Electronic Discovery and Computer Forensics
Case Law
(Organized by Topic)

Discoverability

- *Wright v. AmSouth Bancorp*, 320 F.3d 1198 (11th Cir. 2003). In an age discrimination suit, Plaintiff sought discovery of computer disks and tapes containing "all word processing files created, modified and/or accessed" by five of the Defendant's employees spanning a two and a half year period. The court denied the Plaintiff's motion to compel because his request was overly broad and unduly burdensome and made no reasonable showing of relevance.

- *Bryant v. Aventis Pharmaceuticals, Inc.*, 2002 WL 31427434 (S.D. Ind. Oct. 21, 2002). The Indiana court mentioned without further comment that emails were recovered from the Plaintiff's computer after her termination, confirming the general discoverability of email evidence. The court considered the content of these emails in granting summary judgment in favor of the Defendant.

- *In re CI Host, Inc.*, 92 S.W.3d 514 (Tex. 2002). Customers brought a breach of contract class action against the company hosting their web services. During discovery, the trial court ordered the Defendant to preserve and produce computer backup tapes containing potentially relevant evidence. The Defendant objected that the request was overbroad, demanded confidential information, and was in violation of the federal Electronic Communications Privacy Act. The appellate court held that in light of the Defendant's failure to produce evidence supporting its objections as required by Texas Rule of Civil Procedure 193.4(a), the trial court did not abuse its discretion in ordering the contents of the tapes to be produced.

- *Southern Diagnostic Assoc. v. Bencosme*, 833 So.2d 801 (Fla. Dist. Ct. App. 2002). The appellate court quashed an order against Southern Diagnostic, a non-party in an insurance suit brought by Bencosme, compelling discovery of certain contents of its computer system. The appellate court held that that trial court's order was overly broad, setting no parameters or limitations on the inspection of Southern Diagnostic's computer system and make no account that the computer system contained confidential and privileged information. The appellate court directed the

trial court to craft a narrowly tailored order that accomplishes the purposes of the discovery requests and provides for confidentiality.

- *Collette v. St. Luke's Roosevelt Hospital*, 2002 WL 31159103 (S.D.N.Y. Sept. 26, 2002). The New York court mentioned without further comment that emails were made available during discovery, confirming the general discoverability of email evidence.

- *MHC Investment Comp. v. Racom Corp*., 209 F.R.D. 431 (S.D. Iowa 2002). The Iowa court mentioned without further comment that emails were made available during discovery confirming the general discoverability of email evidence.

- *Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 975713 (S.D.N.Y. May 9, 2002). "Rules 26(b) and 34 for the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials."

- *Stallings-Daniel v. Northern Trust Co*., 2002 WL 385566 (N.D. Ill. Mar. 12, 2002). In an employment discrimination action, the Plaintiff moved for reconsideration of the Court's denial of electronic discovery of the Defendant's email system. The court, in denying the Plaintiff's motion for reconsideration, determined that the Plaintiff presented no new information that justified an intrusive electronic investigation.

- *Dikeman v. Stearns*, 560 S.E.2d 115 (Ga. Ct. App. 2002). In a suit brought by a law firm regarding its client's unpaid legal invoices, the Defendant requested, among other things, a full and complete copy of the law firm's computer hard drive that was used to generate documents pertaining to the Defendant's case. Refusing to order the discovery, the court found the Defendant's requests to be overbroad, oppressive, annoying.

- *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001). "... economic considerations have to be pertinent if the court is to remain faithful to its responsibility to prevent 'undue burden or expense'...If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single email. That is an awfully expensive needle to justify searching a haystack."

- *Ex Parte Wal-mart, Inc.*, 809 So.2d 818 (Ala. 2001). In a personal injury case, Plaintiff sought discovery of Wal-mart's electronic database containing customer incident reports and employee accident review forms. The appellate court held that discovery order should have been restricted to falling-merchandise incidents with geographic and temporal limits set forth by the trial court.

- *White v. White*, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001). In a divorce action, the husband filed a motion to suppress his email that had been stored on the hard drive of the family computer. The Court held that the wife did not unlawfully access stored electronic communications in violation of the New Jersey Wiretap Act and did not intrude on his seclusion by accessing those emails. "Having a legitimate reason for being in the files, plaintiff had a right to seize evidence she believed indicated her husband was being unfaithful….Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet…Not really."

- *Demelash v. Ross Stores, Inc.,* 20 P.3d 447 (Wash. Ct. App. 2001). In an action for a false shoplifting arrest, the court stated, "A trial court must manage the discovery process in a fashion that promotes full disclosure of relevant information while at the same time protecting against harmful side effects. Consequently, a court may appropriately limit discovery to protect against requests that are unduly burdensome or expensive." The court limited the scope of to a computerized summary of the store's files.

- *Milwaukee Police Assoc. v. Jones*, 615 N.W.2d 190 (Wis. Ct. App. 2000). In considering the provisions of the state's open records laws, the court concluded that the City's production of an analog tape was insufficient when a digital version existed. The court stated, "A potent open records law must remain open to technological advances so that its statutory terms remain true to the law's intent."

- *Itzenson v. Hartford Life and Accident Ins. Co*., 2000 WL 1507422 (E.D. Pa. Oct. 10, 2000). "It is difficult to believe that in the computer era" that the Defendant could not identify files and filter out information based on specific categories.

- *In re Dow Corning Corp.*, 250 B.R. 298 (Bankr. E.D. Mich. 2000). Federal Government did not satisfy its obligation to make medical records stored in computer databases available to Debtor, where Government

directed Debtor to warehouses around the world where the information was stored.

- *Van Westrienen v. Americontinental Collection Corp.,* 189 F.R.D. 440 (D. Or. 1999). Court held that "Plaintiffs are not entitled to unbridled access [of] Defendant's computer system…Plaintiffs should pursue other less burdensome alternatives, such as identifying the number of letters and their content."

- *Caldera, Inc. v. Microsoft Corp.*, 72 F.Supp.2d 1295 (D. Utah 1999). A federal district court found that a series of intra-company emails offered "direct evidence" that the corporation was actively trying to destroy a competitor.

- *Playboy Enters., Inc. v. Welles,* 60 F.Supp.2d 1050 (S.D. Cal. 1999). The Court held that Defendant's hard drive was discoverable because it was likely that relevant information was stored on it. Production of such electronic information would not be unduly burdensome upon Defendant.

- *Linnen v. A.H. Robins Co.,* 1999 WL 462015 (Mass. Super. June 16, 1999). "A discovery request aimed at the production of records retained in some electronic form is no different in principle, from a request for documents contained in any office file cabinet." The court continued, "To permit a corporation such as Wyeth to reap the business benefits of such [computer] technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results."

- *Symantec Corp. v. McAfee Assoc., Inc.*, 1998 WL 740807 (N.D. Cal. Aug. 14, 1998). Plaintiff sought to obtain the entire source code for all of Defendant's products dating back to 1995, as well as copies of all hard drives which had access to the server from which the information on the was copied. The court found that production of this magnitude would be unduly burdensome to the Defendant, both in terms of volume and in terms of the proprietary nature of the information sought.

- *Storch v. IPCO Safety Prods. Co.,* 1997 WL 401589 (E.D. Pa. July 16, 1997). "This Court finds that in this age of high-technology where much of our information is transmitted by computer and computer disks, it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff."

- *Strasser v. Yalamanchi*, 669 So.2d 1142 (Fla. Dist. Ct. App. 1996). The court ruled that the trial court's discovery order should be quashed because (1) unrestricted access to Defendant's entire computer system was overly broad and would pose a threat to confidential records and (2) there was little evidence that the purged documents could be retrieved.

- *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996). The court denied Plaintiff's broad request for discovery of Defendant's entire hard drive. The court explained that the costs, burdens, delays, and likelihood of discovering the evidence must be weighed against the importance of the requested evidence. Court held requesting party must show a "particularized likelihood of discovering appropriate material".

- *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (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…[T]oday it is black letter law that computerized data is discoverable if relevant."

- *Murlas Living Trust v. Mobil Oil Corp*., 1995 WL 124186 (N.D. Ill. Mar. 20, 1995). The court refused to require Defendant to undergo intrusive or burdensome discovery for its electronic files where the burden is not justified by the relevance of the evidence likely to be discovered.

- *Crown Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993). Computer data is discoverable under Federal Rule of Procedure 34.

- *Aviles v. McKenzie*, 1992 WL 715248 (N.D. Cal. Mar. 17, 1992). In an action involving claims of wrongful termination and employment discrimination, Plaintiff presented email messages that demonstrated he was fired for whistleblowing about unsafe and illegal company practices.

- *Lawyers Title Ins. Co. v. United States Fidelity & Guar. Co.,* 122 F.R.D. 567 (N.D. Cal. 1988). The court rejected, as broadly framed and intrusive, a request to inspect the responding party's entire computer system where it was a mere possibility that responding party might produce applicable documents. Court required a showing that this inspection would lead to evidence that had not already been produced.

- *Santiago v. Miles*, 121 F.R.D. 636 (W.D.N.Y. 1988). The court noted that "[a] request for raw information in computer banks is proper and the information is obtainable under the discovery rules."

- *Daewoo Elecs. Co. v. United States,* 650 F. Supp. 1003 (Ct. Int'l Trade 1986), *rev'd on other grounds* 6 F.3d 1511 (Fed. Cir. 1993). The court rejected the government's narrow discovery position, stating that disclosure orders should be construed liberally and should not be impeded by technical objections. The court further explained, "[I]t would be a dangerous development in the law if new techniques for easing the use of information become a hindrance to discovery of disclosure in litigation."

- *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (C.D. Utah 1985). "[C]ertain propositions will be applicable in virtually all cases, namely, that information stored in computers should be as freely discoverable as information not stored in computers, so parties requesting discovery should not be prejudiced thereby; and the party responding is usually in the best and most economical position to call up its own computer stored data."

Procedure

- *Zubulake v. UBS Warburg*, 2003 WL 21087884 (S.D.N.Y. May 13, 2003). In a gender discrimination suit against her former employer, the Plaintiff requested that the Defendant produce "[a]ll documents concerning any communication by or between UBS employees concerning Plaintiff." The Defendant produced 350 pages of documents, including approximately 100 pages of email. The Plaintiff knew that additional responsive email existed that the Defendant had failed to produce because she, in fact, had produced approximately 450 pages of email correspondence. She requested that the Defendants produce the email from archival media. Claiming undue burden and expense, the Defendant urged the court to shift the cost of production to the Plaintiff, citing the *Rowe* decision. Stating that a court should consider cost-shifting only when electronic data is relatively inaccessible (such as in this case), the court considered the *Rowe* 8-factor cost shifting test. The court noted that the application of the Rowe factors may result in disproportionate cost shifting away from large defendants, and the court modified the test to 7 factors: (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 of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation and; (7) the relative benefits to the parties of obtaining the information. The court ordered the Defendant to produce, at its own expense, all responsive email existing on

its optical disks, active servers, and five backup tapes as selected by the Plaintiff. The court determined that only after the contents of the backup tapes are reviewed and the Defendant's costs are quantified, the Court will conduct the appropriate cost-shifting analysis.

- *Go2Net, Inc. v. C I Host, Inc.*, 60 P.3d 1245 (Wash. Ct. App. 2003). After discovery commenced in a suit to collect payment due under a services contract, the parties exchanged document requests. In responding to Defendant's requests, Plaintiff provided some documents, but advised that one of its servers had crashed and was in the process of being rebuilt. Plaintiff stated that it would supplement its production at a later date. A day prior to the summary judgment hearing in the case, the Plaintiff produced the additional emails from the rebuilt server. The trial court issued summary judgment in favor of the Plaintiff. On appeal, Defendant argued that the trial court abused its discretion in refusing to vacate the summary judgment order in light of "newly discovered evidence", namely the internal email messages produced just prior to the summary judgment hearing. The appellate court found that the email messages were not "newly discovered evidence" where there was nothing to suggest that the Plaintiff deliberately tried to hide these documents.

- *Dodge, Warren, & Peters Ins. Servs. v. Riley,* 130 Cal.Rptr.2d 385 (Cal. Ct. App. 2003). Prior to termination of their employment, Defendants copied and took with them volumes of computerized data maintained in Plaintiff's files and storage media. Plaintiff sued the Defendants alleging claims of misappropriation of trade secrets, unfair business practices, breach of fiduciary duty and breach of contract. The appellate court affirmed the trial court's order issuing a preliminary injunction against Defendants, requiring the preservation of electronic evidence and ordering them to allow a court-appointed expert to copy the data, recover lost or deleted files, and perform automated searches of the evidence under guidelines agreed to by the parties or established by the court.

- *United States v. Moussaoui*, 2003 WL 548699 (E.D.Va. Jan. 7, 2003). The Defendant claims that the government failed to provide him with information retrieved from various computers used by the Defendant. The court held that the government provided the Defendant with sufficient information, including: information about the authentication of the computer hard drives, confirmation that the computer evidence had not been contaminated, the timing of the forensic examinations, and the software used to restore a hard drive image. The court further stated that the Defense possessed the computer hard drives at issue and had expert

resources and subpoena power to conduct any further investigation it deemed necessary.

- *In re Livent, Inc. Noteholders Sec. Litig.*, 2003 WL 23254 (S.D.N.Y. Jan. 2, 2003). In a securities litigation, the Defendant accounting firm produced approximately 25 email pages from the files of a particular individual at issue, in addition to 14 emails from other employees. Plaintiffs suspected this is production incomplete, and moved the court for: (1) an order "directing Deloitte to make a thorough search of all its computer systems, servers and other storage devices, back-up tapes, and the individual hard drives of employees who worked on the Livent audits" and (2) an order directing the Defendant "to produce all responsive materials found with 30 days, along with a written explanation of all the steps it has taken to find responsive materials." The court denied the Plaintiffs request and directed the Defendant to produce a written explanation of all steps taken to find responsive email. The court directed the parties to consult the *Rowe* decision and, if unable to reach resolution, to inform the court.

- *In re Amsted Indus.*, 2002 WL 31844956 (N.D.Ill. Dec. 17, 2002). In a suit by Plaintiff employees against their employer for breach of fiduciary duty and other wrongs stemming from a hostile takeover with use of employee stock assets, the court considered Plaintiffs' various discovery motions, including a motion compelling Defendants to retrieve email and documents generated on or after January 1, 1997. In response to Plaintiffs' discovery requests, Defendants limited its investigation to word searches of its backup tapes and only produced relevant documents generated after January 1, 1999. The production did not include email. Plaintiffs argued that the Defendants' search of electronic documents was inadequate, and that Defendants should have actually searched the hard drive of each individual Defendant and each person having access to relevant information. The court ordered the Defendant to re-search their backup tapes under a broader subject matter and time period. The court also indicated they should search the in-box, saved, and sent folders of any relevant individual's email in the same manner. The court determined the additional searches were not so burdensome or expensive as to require a limiting of the requests.

- *Gambale v. Deutsche Bank*, 2002 WL 31655326 (S.D.N.Y. Nov. 21, 2002). As a step toward resolving several discovery disputes, the Magistrate Judge ordered the Defendants to serve an affidavit explaining the steps they have taken to search their paper and electronic files for

documents responsive to Plaintiff's discovery requests and outlining the feasibility and cost of retrieving such electronic documents. The Magistrate then stated that the Plaintiff must choose between two options for producing the electronic data: (1) follow the protocol set forth in *Rowe Entertainment v. William Morris Agency,* 205 F.R.D. 421 (S.D.N.Y.2002), with the slight modification set forth in *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.,* 2002 WL 246439 (E.D.La. Feb. 19, 2002), or (2) confer with the Defendant and propose a joint protocol.

- *Kormendi v. Computer Associates Int'l, Inc.,* 2002 WL 31385832 (S.D.N.Y. Oct. 21, 2002). The parties in this employment case jointly wrote the Magistrate, requesting reconsideration and clarification of a prior order. The court previously had ordered Defendant to produce all email messages mentioning the Plaintiff over a one-year time period, with the Plaintiff to pay for the cost of the search. In the letter to the Magistrate, the Defendant stated that it had already produced the emails from persons involved in the suit and had no method to locate and reconstruct emails mentioning the Plaintiff for the listed period because its document retention policy called for employees to retain emails for a period of only thirty days. The Magistrate noted that the Plaintiff should seek other means of attaining the sought after emails, such as searching the computers of other employees who might have saved the emails. Plaintiff must still bear the cost of searching for these emails.

- *Advanced Micro Devices, Inc. v. Intel Corp*., 292 F.3d 664 (9th Cir. 2002). In a dispute relating to the market conduct of Intel Corp, Advanced filed a complaint with the European Commission, and sought discovery according to practices and rules in the United States under federal law. Adopting a broad interpretation of the scope of discovery rights in cases involving foreign tribunals, the Court permitted domestic-style discovery under 28 U.S.C. § 1782 in an investigation conducted by the European Community Directorate.

- *Thompson v. Thompson*, 2002 WL 1072342 (D.N.H. May 30, 2002). The copying of email messages from the hard drive of a personal computer does not constitute interception of electronic communications for the purposes of the Electronic Communications Privacy Act of 1986. The court reasoned that an interception can only occur "during transmission" of electronic communication transfers; thus, the acquisition of stored email does not qualify as an interception under the ECPA.

- *The Gorgen Co. v. Brecht*, 2002 WL 977467 (Minn. Ct. App. May 14, 2002). Plaintiff brought suit against former employees for misappropriation of trade secrets. Prior to serving the complaint, Plaintiff obtained a TRO, which prohibited Defendants from destroying or altering electronic documents and provided for expedited discovery of relevant electronic data. The Appellate Court found that the district court abused its discretion by issuing the TRO and by denying the Defendants' motion to dissolve it. The Appellate Court stated, "Although the TRO seems reasonable on its face…this issue cannot be resolved at this early stage of the litigation without a showing of irreparable harm or without complying with the rules of procedure."

- *Tulip Computers Int'l v. Dell Computer Corp*., 2002 WL 818061 (D.Del. Apr. 30, 2002). On Plaintiff's motion to compel in a patent infringement case, the Court stated that "[T]he procedure that Tulip has suggested for the discovery of email documents seems fair, efficient, and reasonable." The Court ordered the Defendant to produce the hard disks of certain company executives to the Plaintiff's electronic discovery expert for key word searching. After the expert completes the key word search, the Plaintiff will give the Defendant a list of the emails that contain those search terms. The Defendant will then produce the emails to the Plaintiff, subject to its own review for privilege and confidentiality.

- *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D. La. Feb. 19, 2002). The Court used the eight-factor balancing test set forth in *Rowe* to determine operating protocols and the cost shifting formula. It placed the burden on the producing party to elect one of two proposed protocols.

- *Rowe Entertainment, Inc. v. The William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. 2002). Denying Defendants' motion for a protective order insofar as it sought to preclude the discovery of email altogether, the Court set forth an eight factor balancing test for identifying responsive emails while protecting privileged documents. *See also Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 975713 (S.D.N.Y. May 9, 2002). After reanalyzing and reaffirming Judge Francis' eight factor balancing test, the Court upheld the January 15, 2002 Order that granted Defendants' motion to shift the costs of production of their email communications to Plaintiffs.

- *Columbia Communications v. Echostar*, 2 Fed.Appx. 360 (4th Cir. 2001). In a contract dispute, the Court held that failure of the lessor to turn over

certain computer databases during discovery did not justify a judgment for the distributor or a new trial.

- *Perez v. Volvo Car Corp.*, 247 F.3d 303 (1st Cir. 2001). In a suit under the Racketeer Influenced and Corrupt Organizations Act, internal Volvo emails, which could have made a dispositive difference on the issue of Volvo's knowledge of the fraud involved in the suit, were not called to the District Court's attention until after the Court had issued summary judgment. Volvo claimed these emails offered too little, too late. However, the First Circuit disagreed, "After all, Volvo did not produce the emails to the plaintiffs until January 2000 (the same month that Volvo filed its summary judgment motion)--and then only in Swedish. Given the timing, the sheer volume of documents involved in the case, and the need for translation, fundamental fairness counsels in favor of treating the emails as newly-discovered evidence within the purview of Federal Rule of Civil Procedure 59(e)."

- *Benton v. Allstate Ins. Co.,* 2001 WL 210685 (C.D. Cal. Feb. 26, 2001). The court refused to grant a continuance on Defendant's summary judgment motion where Plaintiff claimed that he had not had an adequate opportunity to conduct discovery of Defendant's computer system. The court concluded that the Plaintiff did not show that a further continuance was necessary to prevent irreparable harm or that further discovery will enable him to obtain evidence essential to his opposition to the motion.

- *America Online, Inc. v. Anonymous*, 542 S.E.2d 377 (Va. 2001). In a case of first impression, the court refused to allow a corporation to seek information from AOL without revealing its identity.

- *Superior Consultant Co. v. Bailey,* 2000 WL 1279161 (E.D. Mich. Aug. 22, 2000). Court ordered Defendant to create and produce for Plaintiff a backup file of Defendant's laptop computer, and a backup file of any personal computer hard-drive to which Defendant had access.

- *United States v. VISA*, 1999 WL 476437 (S.D.N.Y. July 7, 1999). In a suit against VISA and MasterCard, the parties agreed to narrow the scope of the archived email search, both in terms of the number of employees whose email is to be produced and the number of days per month for which email is to be produced. The court reserved decision about which party will ultimately bear the cost of producing email.

- *Concord Boat v. Brunswick Corp.*, 1996 WL 33347247 (E.D.Ark. Dec. 23, 1996). Plaintiffs contend that Defendant's search for and production of relevant information was insufficient because it failed to review all computer documents and email. Plaintiffs filed motions to compel discovery of electronic information and to prevent further destruction of documents. The Defendant asserted that the search was reasonable and submitted that the Plaintiffs' demands were overly broad and unduly burdensome. The court ordered the parties to have a meeting with counsel and computer experts for both sides, conducting a good faith discussion to see whether agreement can be reached on a procedure to further search the Defendant's email, the choice of an expert, the procedure for specifying the expert's responsibilities, and allocation of the costs. The court also ordered the Defendant to produce a detailed description of the Defendant's electronically stored information.

- *Carbon Dioxide Indus. Antitrust Litig.*, 155 F.R.D. 209 (M.D. Fla. 1993). "[D]epositions to identify how data is maintained and to determine what hardware and software is necessary to access the information are preliminary depositions necessary to proceed with merits discovery."

Production of Data

- *Giardina v. Lockheed Martin Corp.*, 2003 WL 1338826 (E.D.La. Mar. 14, 2003). In an employment discrimination suit, Plaintiff's discovery requests sought a list of all "non-work related Internet sites" accessed with sixteen different company computers. Defendant objected to this request as overly broad and unduly burdensome as it would require creation of detailed and lengthy reports that would take many hours to compile. The magistrate judge granted Plaintiff's motion to compel and awarded attorney fees and the District Court affirmed.

- *Lakewood Eng'g v. Lasko Prod.*, 2003 WL 1220254 (N.D.Ill. Mar. 14, 2003). In a patent infringement suit, the Plaintiff produced email and other electronic documents after the close of the discovery period. The court found that while the Plaintiff did not engage in a good faith effort to produce all requested discovery in a timely manner, the cost to the Defendant was minimal and therefore refused to issue sanctions. To the extent that it had not already done so, the Plaintiff was ordered to produce all emails generated or received by the inventor relating to the patent at issue.

- *Zhou v. Pittsburgh State University*, 2003 WL 1905988 (D.Kan. Feb. 5, 2003). In an employment discrimination suit, Plaintiff sought to compel Defendant to produce computer generated documents (instead of typewritten documents compiled by hand already produced) reflecting the salaries of Defendant's faculty. Relying on the Advisory Committee Notes to F.R.C.P. 34, the court stated, "[T]he disclosing party must take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data." The court granted the Plaintiff's motion to compel and ordered the Defendant to disclose all data compilations, computerized data and other electronically-recorded information reflecting the salaries of Defendant's faculty. The court further ordered the parties to preserve evidence that they know, or should know, is relevant to the ongoing litigation, including preservation of all data compilations, computerized data and other electronically-recorded information.

- *McPeek v. Ashcroft*, 212 F.R.D. 33 (D.D.C. 2003). In its August 1, 2001 Order, the court ordered the Defendant to search certain backup tapes to assist in ascertaining whether additional searches were justified. After completing this backup tape sample, the parties could not agree whether the search results produced relevant information such that a second search was justified. The magistrate stated, "[t]he frustration of electronic discovery as it relates to backup tapes is that backup tapes collect information indiscriminately, regardless of topic. One, therefore, cannot reasonably predict that information is likely to be on a particular tape. This is unlike the more traditional type of discovery in which one can predict that certain information would be in a particular folder because the folders in a particular file drawer are arranged alphabetically by subject matter or by author." After examining the likelihood of relevant data being contained on each of the backup tapes, the magistrate ordered additional searches of selected backup tapes likely to contain relevant evidence.

- *York v. Hartford Underwriters Ins. Co.,* 2002 WL 31465306 (N.D.Okla. Nov. 4, 2002). In a case alleging bad faith in processing an insurance claim, the Defendant opposed Plaintiff's 30(b)(6) deposition request on the subject of Defendant's use of a claims adjusting software program called "Colossus." The Court found that the Defendant failed to demonstrate that the "Colossus" program was proprietary or confidential and ordered that the Plaintiff should be given the opportunity to discover what data was inputted into "Colossus" concerning her claim. The court also ordered the Defendant to provide a Rule 30(b)(6) witness to testify to the use of the "Colossus" program. Granting part of the Defendant's

motion for a protective order, the Court held that the nature and extent of the Defendant's use of "Colossus" may be confidential and entitled to protection from third parties.

- *Eolas Technologies Inc. v. Microsoft Corp.*, 2002 WL 31375531 (N.D.Ill. Oct. 18, 2002). In a patent infringement suit against Microsoft, the parties engaged in extensive motion practice, both on dispositive summary judgment issues and on various discovery issues. With regard to one discovery motion aimed at obtaining information which the Defendant alleged was outside the scope of the issues in the case, the court restricted discovery to spreadsheet data regarding licenses, revenue and profitability of "accused server versions of Windows 2000 and Windows NT 4.0 operating system software with Internet Explorer." With regard to another discovery motion, addressing whether certain email messages in a chain of messages must be produced, the court ordered the Defendant to produce certain emails to and from one key individual so that the court could analyze the documents *in camera* and then make a determination as to whether the Plaintiff is entitled to receive them in an unredacted form.

- *Jones v. Goord*, 2002 WL 1007614 (S.D.N.Y. May 16, 2002). Plaintiffs, prison inmates bringing suit against the New York State Corrections Commission for prison overcrowding, requested the production of six different electronic databases maintained by the New York state prison system. The Plaintiffs claimed that the electronic information would be more valuable than the already produced hard copies because the information would be more manipulable. The court refused to compel discovery of the databases because the burden of the proposed discovery outweighed its likely benefit, particularly in light of the Plaintiffs failure to seek discovery in a timelier manner and the vast amount of material that had already been produced in hard copy. The court stated, "As electronic mechanisms for storing and retrieving data have become more common, it has increasingly behooved courts and counsel to become familiar with such methods, and to develop expertise and procedures for incorporating 'electronic discovery' into the familiar rituals of litigation."

- *Kaufman v. Kinko's Inc.*, Civ. Action No. 18894-NC (Del. Ch. Apr. 16, 2002). The Court granted the Plaintiffs' motion to compel the Defendants' production of certain email messages retrievable from Defendants backup system. The Defendants' argument that the burdens of the retrieval process outweighed any evidentiary benefit that the Plaintiffs would obtain from the documents was unpersuasive. Instead, the Court stated, "Upon installing a data storage system, it must be assumed that at

some point in the future one may need to retrieve the information previously stored. That there may be deficiencies in the retrieval system…cannot be sufficient to defeat an otherwise good faith request to examine the relevant information."

- *United States Fidelity & Guaranty Co. v. Braspetro Oil Servs. Co*., 2002 WL 15652 (S.D.N.Y. Jan. 7, 2002). In a discovery dispute concerning the potential waiver of privilege with respect to materials provided to Defendants' expert witnesses, the Court ordered the Defendants to produce all materials provided to their experts – privileged or unprivileged, whether in paper or electronic form.

- *Braxton v. Farmer's Ins. Group*, 209 F.R.D. 651 (N.D.Ala. 2002). In a class action brought under the Fair Credit Reporting Act, the Plaintiffs sought emails from non-party individual insurance agents of the Defendant's insurance company. The Defendant objected, claiming that enforcement of the subpoena would subject the agents to an undue burden. The court refused to require the non-party insurance agents to engage in the task of "combing through their email files and other records in search of the documents sought by the plaintiff." The court ordered the Defendant to locate and produce relevant emails, newsletters, and other correspondence that it sent to its agents.

- *McNally Tunneling v. City of Evanston*, 2001 WL 1568879 (N.D. Ill. Dec. 10, 2001). In a dispute between a construction contractor and the City of Evanston, the Court denied Evanston wide-scale access to both hard-copy and electronic versions of McNally's computer files where Evanston's need for both sets of documents was not fully briefed to the Court. However, where McNally's hard-copy productions were incomplete, the Court ordered McNally to supplement the hard-copy versions with its computer files to ensure that it has produced all of the relevant information.

- *Unnamed Physician v. Board of Trustees of St. Agnes Medical Center*, 113 Cal.Rptr.2d 309 (Cal. Ct. App. 2001). In a physician review hearing, the hospital was ordered to provide the physician with all existing documents related to the hospital's computer programs, except those of a proprietary nature.

- *Hayes v. Compass Group USA, Inc.*, 202 F.R.D. 363 (D. Conn 2001). The Plaintiff in an age discrimination action requested information on similar claims filed against the Defendant. The Defendant advised the Court of

the burden and expense involved with such a request given that some of the data was stored in a non-searchable computer format. The Court ordered the Defendant to manually search the unsearchable computer data and to produce all information for which it had computer search capabilities.

- *In re the Matter of the Application of Lees*, 727 N.Y.S.2d 254 (N.Y. Sup. Ct. 2001). A rape Defendant submitted an *ex parte* motion asking that the victim and a third party be ordered to turn over their computers for inspection. Defendant sought to uncover an email in which the victim falsely claimed to have been raped on a prior occasion. The application of the Defendant was granted to the extent that he could show cause to the court.

- *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001). In a sexual harassment action against Plaintiff's employer, Plaintiff sought to force Defendant to search its backup systems for data that was deleted by the user but was stored on backup tape. Defendant rebutted that the remote possibility of yielding relevant evidence could not justify the costs involved. Instead of ordering recovery and production of relevant documents from all of the existing backup tapes, the Magistrate ordered the Defendant to restore and produce responsive emails from one person's computer over a one year period. After this sample data was produced and accessed, the Magistrate would then determine if a broader recovery and search was warranted given the burden and expense.

- *Kleiner v. Burns*, 2000 WL 1909470 (D. Kan. Dec. 15, 2000). Court ordered Defendant Yahoo! to disclose all electronic data compilations in its possession, custody, and control that are relevant to disputed facts. Court also ordered parties to preserve evidence that they know, or should know, is relevant to the ongoing litigation, including preservation of all data compilations, computerized data and other electronically-recorded information.

- *Illinois Tool Works, Inc. v. Metro Mark Prod. Ltd*., 43 F.Supp.2d 951 (N.D. Ill. 1999). In an unfair competition case, the court ordered the Defendant to produce for inspection its computer after Plaintiff showed that the Defendant had been less than forthcoming in producing hard copies of requested documents. The court further issued sanctions, in the form reasonable attorney's fees and costs, for the failure to comply with the discovery orders.

- *Alexander v. FBI*, 186 F.R.D. 78 (D. D.C. 1998). The court concluded that it was appropriate to order an examination of employee's computer hard drive and server to determine whether responsive documents that had not been already produced actually existed. *See also Alexander v. FBI,* 188 F.R.D. 111 (D.C. Cir. 1998). The court refused to require Defendants to completely restore all deleted files and email where Plaintiff did not propose "targeted and appropriately worded searched of backed-up and archived email and deleted hard drives for a limited number of individuals."

- *Sattar v. Motorola, Inc.,* 138 F.3d 1164 (7th Cir. 1997). Plaintiff sought hard copies of over 200,000 emails, since its system was unable to read Defendant's electronic files. The appellate court affirmed the district court's ruling that a more reasonable accommodation was (1) some combination of downloading the data from the tapes to conventional computer disks or a computer hard-drive, (2) loaning Plaintiff a copy of the necessary software, or (3) offering Plaintiff on-site access to its own system. If all of those options failed, the court ordered that the parties would each bear half the cost of the copying the 200,000 emails.

- *Smith v. Texaco, Inc*., 951 F. Supp. 109, (E.D. Tex 1997), *rev'd on other grounds* 263 F.3d 394 (5th Cir. 2001). Modifying the original state court TRO in a race discrimination case, the court permitted the moving of certain documents in the ordinary and usual course of business and the deletion of electronic records in the ordinary and usual course of business, provided that hard copy records be made and kept.

- *Strauss v. Microsoft Corp.,* 1995 WL 326492 (S.D.N.Y. June 1, 1995). The court denied Microsoft's motion to exclude evidence of offensive emails in a hostile work environment lawsuit.

- *Easley, McCaleb & Assoc., Inc. v. Perry*, No. E-2663 (Ga. Super. Ct. July 13, 1994). Court ordered that deleted files on Defendant's computer hard drive are discoverable, and Plaintiff's expert must be allowed to retrieve all recoverable files. Court issued an order detailing the protocol for reviewing the electronic data.

- *Torrington Co., v. United States*, 786 F. Supp. 1027 (Ct, Int'l Trade 1992). Plaintiff requested access to confidential materials contained on a computer tape. Plaintiff also requested hard copies of the data. The court refused to order the Defendant to create the computer tapes from scratch where the Plaintiff had already received the documents in paper form. In

reaching its decision, the court stated, "Where the burden, cost and time required to produce the tapes is virtually equal on both parties, then the burden of producing the tapes falls on the party requesting the information."

- *PHE, Inc. v. Department of Justice*, 139 F.R.D. 249 (D.D.C. 1991). Court ordered Plaintiffs to produce computerized tax records even though Plaintiffs possessed no computer program to retrieve or display the records. "Although no program may presently exist to obtain the information requested, the Court is satisfied that with little effort the plaintiffs can retrieve the necessary and appropriate information…It would not be unreasonable to require the plaintiffs to incur modest additional expenditures so as to provide the defendants with the discovery necessary to establish that they are not acting in bad faith and vindictively."

- *In re Air Crash Disaster at Detroit Metro*, 130 F.R.D. 634 (E.D. Mich. 1989). In litigation brought after a passenger jet crash, the court ordered the aircraft manufacturer to provide relevant flight simulation data on computer-readable nine-track magnetic tape even though the aircraft manufacturer had already provided the data in hard copy print-outs. Because material did not currently exist on magnetic tape, the requesting party (the airline) was required to pay all reasonable and necessary costs associated with manufacture of tape.

- *Timken Co. v. United States*, 659 F. Supp 239 (Ct. Int'l Trade 1987). Court ordered production of data stored on computer tape even though it had been previously produced in a paper format.

- *Williams v. Owens-Illinois, Inc*., 665 F.2d 918 (9th Cir. 1982). In an employment discrimination suit, the court refused to order production of the electronic information on computer tape where all the data was previously produced in hard copy. Therefore, the court determined that the Appellants were not deprived of any data.

- *City of Cleveland v. Cleveland Electric Illuminating Co.*, 538 F. Supp. 1257 (N.D. Ohio 1980). In an antitrust suit brought by a city against an electric utility, the court ordered the electric utility was entitled to pretrial production by the city of computer data and calculations underlying conclusions contained in reports of certain experts the city intended to call as witnesses.

- *National Union Elec. Corp. v. Matsushita Elec. Ind. Co*., 494 F. Supp. 1257 (E.D. Pa. 1980). Defendant filed a motion to compel production of a computer tape containing the information that the Plaintiff previously produced in a hard copy. The court required Plaintiff to have computer experts create a computer-readable tape containing data previously supplied to Defendant in printed form.

- *Pearl Brewing Co. v. Joseph Schiltz Brewing Co.*, 415 F. Supp. 1122 (S.D. Tex. 1976). In an antitrust action, court allowed Defendant to inspect and copy the computer programs and systems documentation at issue and to depose the Plaintiff's computer experts as to the creation of the systems.

- *Adams v. Dan River Mills, Inc*., 54 F.R.D. 220 (W.D. Va. 1972). In an employment discrimination case, the court required the Defendant to provide an electronic version of the printouts already submitted to the Plaintiff. "Because of the accuracy and inexpensiveness of producing the requested documents in the case at bar, this court sees no reason why the defendant should not be required to produce the computer cards or tapes and the W-2 print-outs to the plaintiffs."

Costs

- *Computer Assocs. Int'l, Inc. v. Quest Software, Inc*., 2003 WL 21277129 (N.D.Ill. June 3, 2002). Plaintiff brought a copyright infringement and trade secret misappropriation suit against six of Defendant's employees arising from improper use of some of Plaintiff's software source code. Plaintiff asked Defendants to make specific work and home computer hard drives available for electronic imaging so that Plaintiff could search for and reconstruct deleted files that would be otherwise undiscoverable. Defendants argued that the drives contained privileged information relating directly to this litigation and worked with a computer consultant to remove the privileged information from the images and indicate where the removed information was located. Defendants filed a motion to require the Plaintiff to pay for the computer consultation that was necessary to prepare the drives for disclosure. After seeking advice from the *Rowe* 8-factor cost shifting test, the court determined that the Defendants' costs were analogous to the review of documents for privileged information and should not be shifted to the requesting party.

- *Medtronic v. Michelson*, 2003 WL 21212601 (W.D. Tenn. May 13, 2003). In a trade secret violation suit, the Defendant sought to compel the Plaintiff to respond fully to discovery requests by producing data

contained on a large number of computer network backup tapes. Plaintiff timely responded, claiming that the discovery requests were unduly burdensome because of the costs associated with extracting backup tape data and reviewing it for relevance and privilege. The parties did not dispute the relevance of the electronic data at issue. Agreeing that producing the backup data as a whole would be burdensome on the Plaintiff, the court applied the *Rowe* 8 factor cost-shifting test to determine burden and cost. Finding that the majority of the factors favored shifting a portion of discovery costs to the Defendant, the court outlined a detailed discovery protocol.

- *Byers v. Illinois State Police*, 2002 WL 1264004 (N.D. Ill. June 3, 2002). In an employment discrimination suit, the plaintiffs sought an order compelling the defendants to produce archived emails. The court stated, "Based on the cost of the proposed search and the plaintiffs' failure to establish that the search will likely uncover relevant information, the Court concludes that the plaintiffs are entitled to the archived emails only if they are willing to pay for part of the cost of production….Requiring the plaintiffs to pay part of the cost of producing the emails will provide them with an incentive to focus their requests." The court granted the motion to the extent that the plaintiffs bear the cost of licensing the archived email software while the defendants continue to bear the expense of review for responsive, privileged, and confidential documents.

- *In re Bristol-Myers Squibb Securities Litigation*, 2002 WL 169201 (D.N.J. Feb. 4, 2002). The Court modified the Plaintiff's original discovery cost commitment where Defendants "dumped" an extraordinary number of paper documents resulting in a prohibitive copying charge. The Court also denied the Defendant's motion for Plaintiff's one-half cost contribution for document scanning costs, but instead required Plaintiff to pay only for the nominal cost of copying compact discs. The Court reiterated the importance of a Rule 26(f) conference to discuss electronic discovery issues, including the fair and economical allocation of costs.

- *Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 63190 (S.D.N.Y. Jan. 16, 2002). Denying Defendants' motion for a protective order insofar as it sought to preclude the discovery of email altogether, the Court adopted a balancing approach, consisting of eight factors, to determine whether discovery costs should be shifted. *See also Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 975713 (S.D.N.Y. May 9, 2002). After reanalyzing and reaffirming Judge Francis' eight factor balancing test, the Court upheld the January 15, 2002

Order that granted Defendants motion to shift the costs of production of their email communications to Plaintiffs.

- *GTFM, Inc., v. Wal-Mart Stores,* 2000 WL 1693615 (S.D.N.Y. Nov. 9, 2000). The court allowed Plaintiff to recover fees for the inspection of Wal-Mart's computer records and facilities by plaintiff's expert and also upheld fees and expenses caused by Wal-Mart's failure to provide accurate discovery information in response to valid discovery requests. The court found the award of expenses "reasonable in view of the prior repeated misinformation provided by Wal-Mart concerning the availability of information…"

- *Procter & Gamble Co. v. Haugen,* 179 F.R.D. 622 (D. Utah 1998) *rev'd on other grounds* 222 F.3d 1262 (10th Cir. 2000). The court ordered Plaintiff to pay Defendant $10,000 for Plaintiff's failing to preserve email records for five key employees. Plaintiff was allowed to do a keyword search of Defendant's database that excluded competitive information.

- *Zonaras v. General Motors Corp.,* 1996 WL 1671236 (S.D. Ohio Oct. 17, 1996). In this case, Plaintiffs sought to compel discovery of data compiled concerning different crash test dummy tests. In response, Defendant GMC asserted that it produced data tracings and backup materials for all but eleven of these tests, and objects to production of the remaining tests "as unduly burdensome and expensive." After balancing the elements outlined in Rule 26(b)(2)(iii), the court ordered Defendant GMC to produce data tracings and backup materials of the eleven tests where the benefits of the discovery outweighed the expense of production. Because admissibility of the electronic evidence was still undecided, the court ordered the Plaintiffs to pay half the production costs.

- *Toledo Fair Hous. Ctr. v. Nationwide Mut. Ins. Co.,* 703 N.E.2d 340 (Ohio C.P. 1996). The court ordered discovery of certain documents from Defendant's database. Judge stated that the Defendant cannot avoid discovery simply because their own record keeping scheme makes discovery burdensome. Court ordered Defendant to pay costs of the discovery.

- *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995). The court found that the law is clear that data in computerized form is discoverable even if paper copies of the information have been produced. The producing party can be required to design a computer program to extract the data from its computerized business records. But

such an order is subject to the Court's discretion as to the allocation of the costs of designing such a computer program.

- *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 WL 360526 (N.D. Ill. June 15, 1995). Court found that expense of retrieving electronic data was mainly due to Defendant's own record-keeping scheme. As such, Court required Defendant to produce its responsive, computer-stored email at its own expense, subject to some limitations. Court also instructed Plaintiffs to narrow the scope of their request. Parties encouraged by Court to confer regarding scope of requests for emails.

- *Rhone-Poulenc Rorer, Inc. v. Home Indemnity Co.,* 1991 WL 111040 (E.D. Pa. June 17, 1991). An unwieldy computerized record-keeping system, which requires heavy expenditures in money and time to produce relevant records, is simply not an adequate excuse to frustrate discovery. Plaintiffs were required to pay for copies of any documents on microfilm/microfiche which Plaintiff requests, while Defendants bear the burden of searching and producing the documents.

- *Williams v. Du Pont*, 119 F.R.D. 648 (W.D. Ky. 1987). The discovering party must bear costs of data production and reimburse responding party for a portion of its expense in assembling the database.

- *Delozier v. First Nat'l Bank of Gatlinburg*, 109 F.R.D. 161 (E.D. Tenn. 1986). "A court will not shift the burden of discovery onto the discovering party where the costliness of the discovery procedure involved is entirely a product of the defendant's record-keeping scheme over which the plaintiff has no control."

- *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (C.D. Utah 1985). The court denied Defendant's motion requiring Plaintiffs to pay the cost Defendant incurred in producing a printout of computer data that Plaintiffs sought through discovery. The court based its holding on that the amount of money involved was not excessive or inordinate, that the relative expense and burden in obtaining the data would have been substantially greater for the Plaintiffs as compared with the Defendant, that the amount of money required to obtain the data as set forth by the Defendant would have been a substantial burden to the Plaintiffs, and that the Defendant was benefited to some degree by producing the data.

- *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340 (1982). "[W]e do not think a defendant should be penalized for not maintaining his records in

the form most convenient to some potential future litigants whose identity and perceived needs could not have been anticipated." Where the expense of creating computer programs that would locate the desired data was the same for both parties, the Court ordered that the party seeking the information must bear the cost of production.

Spoliation

- *Kucala Enters. Ltd. v. Auto Wax Co.*, 2003 WL 21230605 (N.D.Ill. May 27, 2003). In a patent suit, the district court, in response to a discovery request by the Defendant, ordered the inspection of the Plaintiff's computer. The night before the Defendant's computer forensic expert created an image of the computer hard drive in accordance with the inspection order, the Plaintiff employed "Evidence Eliminator", a wiping software utility, to delete and overwrite over 12,000 files. The forensic expert was also able to determine that 3,000 additional files were deleted and overwritten three days earlier. Even though there was no clear indication that relevant evidence was among the destroyed files, the court described the Plaintiff's actions as "egregious conduct" and emphasized the Plaintiff's apparent intent to destroy evidence that it had a duty to maintain. The Magistrate Judge recommended to the district court that the Plaintiff's case be dismissed with prejudice and that the Plaintiff be ordered to pay the Defendant's attorney fees and costs incurred in defending the motion.

- *Positive Software Solutions v. New Century Mortgage Corp.*, 2003 WL 21000002 (N.D.Tex. May 2, 2003). To ensure no other potentially relevant information was deleted, the Court ordered Defendants to preserve all backups and images of servers and personal computers that contain or contained files at issue. The court further ordered the Defendant to refrain from deleting any such files still resident on any servers or personal computers and to preserve all backups or images. Finding the scope substantially overbroad, the Court denied the Plaintiff's motion to compel imaging "of all of Defendants' media potentially containing any of the software and electronic evidence relevant to the claims in this suit" and "all images of [Defendants'] computer storage facilities, drives, and servers taken to date."

- *Liafail, Inc. v. Learning 2000, Inc.,* 2002 WL 31954396 (D.Del. Dec. 23, 2002). Defendant alleges that upon issuing its document requests, the Plaintiff engaged in electronic data spoliation including intentionally deleting computer files and damaging hardware. The court stated that the Plaintiff's position on the whereabouts of the requested documents

indicated questionable discovery tactics. Nevertheless, because the court record was unclear as to what had been produced, and what must still be produced, the court decided not to immediately sanction the Plaintiff. Rather, the court gave the Plaintiff time to correct or clarify the record by producing the requested documents which it has claimed as available. The court stated that should the Plaintiff choose not to heed the court's order, the court would order sanctions in the form of an adverse inference jury instruction.

- *Antioch v. Scrapbook Borders, Inc,* 210 F.R.D. 645 (D.Minn. 2002). In a copyright infringement action, the Plaintiff moved for issuance of an order directing the Defendant to: preserve records, expedite discovery, compel discovery, and appoint a neutral computer forensics expert. Emphasizing the potential for spoliation of the computer data, the court stated "we conclude that the Defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff's claims, or the Defendants' defenses."

- *Lombardo v. Broadway Stores, Inc.,* 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002). The Court upheld sanctions where the Defendant destroyed computerized payroll data that was the subject of Plaintiff's discovery request.

- *RKI, Inc. v. Grimes*, 177 F.Supp.2d 859 (N.D. Ill. 2001). In a trade secret misappropriation action against Plaintiff's former employee, the Court found that the Defendant defragmented his home computer in an effort to prevent plaintiff from learning that he had deleted confidential information and software. The Court ordered the Defendant to pay $100,000 in compensatory damages, $150,000 in punitive damages, attorneys' fees, and court costs.

- *Heveafil Sdn. Bhd. v. United States*, 2001 WL 194986 (Ct. Int'l Trade Feb 27, 2001). In an action challenging a U.S. Department of Commerce administrative review of an "antidumping order", the court determined that the plaintiff failed to act to the best of its ability where six months after receiving notice about maintaining its source documents, it deleted relevant data from its computer system. The court found that the plaintiff "did not cooperate to the best of its ability because after receiving notice from [the Department of Commerce], it knew or should have known to maintain th[is] source document."

- *Trigon Ins. Co. v. United States*, 204 F.R.D. 277 (E.D.Va. 2001). Based on computer forensic expert analysis, the Court found that the Defendant willfully and intentionally destroyed documents that should have been produced during discovery. The Court issued adverse inferences and reimbursement of Plaintiff's attorneys fees as damages for the spoliation. *Trigon Ins. Co. v. United States*, 2002 WL 31864265 (E.D.Va. Dec. 17, 2002.). Despite objection by the Defendant, the Court found Plaintiff's fees and expenses (in the amount of $179,725.70) for hiring and deposing computer forensics experts and briefing and adjudicating the issues related to the spoliation warranted and reasonable.

- *Pennar Software Corp. v. Fortune 500 Sys. Ltd*., 2001 WL 1319162 (N.D.Cal. Oct. 25, 2001). In a breach of contract suit, the Court imposed sanctions upon the Defendant in the form of attorney's fees for committing spoliation of evidence and prolonging the discovery process. The Court based its findings on the Defendant's failure to present a maintenance policy, log files, or backup tapes that would track the website maintenance and deletion procedures. When the evidence was produced, the Court found that the Defendant tampered with and deleted evidence in order to evade personal jurisdiction.

- *In re Pacific Gateway Exchange, Inc.*, 2001 WL 1334747 (N.D.Cal. Oct. 17, 2001). In a securities violation case, the Court lifted the discovery stay, stating "The court finds that there is a significant risk that relevant documents, both paper and electronic, could be irretrievably lost, which could result in prejudice to plaintiffs."

- *Minnesota Mining & Mfg. v. Pribyl*, 259 F.3d 587 (7th Cir. 2001). Plaintiff brought suit against three former employees for misappropriation of trade secrets. The appellate court affirmed the trial court's negative inference instruction to the jury where the one Defendant committed spoliation of evidence by downloading six gigabytes of music onto his laptop, which destroyed many files sought by the Plaintiff, the night before Defendant was to turn over his computer pursuant to the discovery request. However, the fact that hard drive space was destroyed on one Defendant's computer did not relieve the Plaintiff from proving the elements of its claims.

- *Long Island Diagnostic Imaging v. Stony Brook Diagnostic Assocs.*, 286 A.D.2d 320 (N.Y. App. Div. 2001). Where the Defendants purged their computer databases against court order and produced compromised and unusable backup tapes, the court dismissed the parties' counterclaims and

third-party complaint as spoliation sanctions. The court stated "The striking of a party's pleading is a proper sanction for a party who spoliates evidence."

- *Danis v. USN Communications,* 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000). The court found that the Defendant failed to properly preserve information on the computer database. Court allowed the trial judge to inform jury that some of the gaps in the case were caused by Defendant's failure to turn over computer tapes and documents. The court fined the CEO of Defendant company $10,000 for failing to properly preserve such electronic information, but denied Plaintiff's motion for default judgment.

- *Mathias v. Jacobs,* 197 F.R.D. 29 (S.D.N.Y. 2000), *vacated* 2001 WL 1149017 (S.D.N.Y. Sept. 27, 2001). Court found Plaintiff had a duty to preserve information contained on a Palm Pilot. Since Plaintiff's conduct did not destroy evidence, but rather just made it more difficult to discover, the court imposed monetary sanctions as a consequence of the spoliation.

- *Illinois Tool Works, Inc. v. Metro Mark Prod., Ltd.,* 43 F.Supp.2d. 951 (N.D. Ill. 1999). The court held that sanctions, in the form of attorney's fees and additional discovery costs, against the Defendant were warranted as a remedy for spoliation.

- *Linnen v. A.H. Robins Co.,* 1999 WL 462015 (Mass. Super. June 16, 1999). Defendant Wyeth failed to preserve emails and neglected turning over database information ordered by the court. The court sanctioned Wyeth for such "inexcusable conduct" and allowed spoliation inference to be given to jury.

- *Telecom Int'l Amer., Ltd. v. AT & T Corp*., 189 F.R.D. 76 (S.D.N.Y. 1999). "Even without a specific discovery order, a district court may impose sanctions for spoliation of evidence, exercising its inherent power to supervise the litigation before it."

- *United States v. Koch Ind.,* 197 F.R.D. 463 (N.D. Okla. 1998). Plaintiffs claimed that Defendant thwarted discovery attempts by destroying backup computer tapes and files. Court found that Defendant failed in its duty to preserve evidence that it should have known was relevant. Court allowed Plaintiffs to inform jury that computer tapes and files were destroyed but did not allow negative inference.

- *Lauren Corp. v. Century Geophysical Corp.,* 953 P.2d 200 (Colo. Ct. App. 1998). The court held, as a matter of first impression, that a trial court may impose attorney fees and costs as sanction for bad faith and willful destruction of evidence, even absent a specific discovery order.

- *In re Cheyenne Software, Inc. v. Securities Litig.,* 1997 WL 714891 (E.D.N.Y. Aug. 18, 1997). In a securities proceeding, the court imposed $15,000 in attorney's fees and sanctions for failing to heed the court's discovery order. The court also compelled the defendant to bear the cost of downloading and printing up to 10,000 pages of additional documents responsive to appropriate keyword searches requested by the plaintiff.

- *Chidichimo v. University of Chicago Press*, 681 N.E.2d 107 (Ill. App. Ct. 1997). Some jurisdictions recognize a tort action for negligent spoliation of evidence.

- *ABC Home Health Servs. v. IBM Corp*., 158 F.R.D. 180 (S.D. Ga. 1994). In action for breach of contract, the court sanctioned IBM for destroying computer files in anticipation of litigation.

- *First Tech. Safety Sys., Inc. v. Depinet,* 11 F.3d 641 (6th Cir. 1993). "In order to justify proceeding *ex parte*…the applicant must do more than assert that the adverse party would dispose of evidence if given notice." Instead, the party must demonstrate that the adverse party has a "history of disposing of evidence or violating court orders…"

- *Cabinetware Inc., v. Sullivan,* 1991 WL 327959 (E.D. Cal. July 15, 1991). The court issued a default judgment as a sanction for spoliation of electronic evidence. "Destruction of evidence cannot be countenanced in a justice system whose goal is to find the truth through honest and orderly production of evidence under established discovery rules."

- *Computer Assocs. Int'l, Inc. v. American Fundware, Inc*., 133 F.R.D. 166 (D. Colo. 1990). Court issued a default judgment were Defendant revised portions of the source code after being served in the action, and thus put on notice that the source code was irreplaceable evidence. Revised code was a central piece of evidence to the litigation.

- *William T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443 (C.D. Cal. 1984). GNC was ordered to preserve all records that were maintained in the ordinary course of its business; despite this, company employees were instructed that these judicial orders "should not require us

to change our standard document retention or destruction policies or practices." Court ordered a default judgment and over $450,000 in monetary sanctions, where GNC deleted electronic documents that were not otherwise available.

Sanctions

- *Hildreth Mfg. v. Semco, Inc.,* 785 N.E.2d 774 (Ohio Ct. App. 2003). The appellate court found no basis for Defendant's motion for contempt for spoliation of computer evidence. The court found that even though the Plaintiff failed to preserve data contained on the computer hard drives at issue, there was not a reasonable possibility that the hard drives contained evidence that would have been favorable to the Defendant's claims.

- *Metropolitan Opera Assoc., Inc. v. Local 100,* 212 F.R.D. 178 (S.D.N.Y. 2003). In a labor dispute, the Defendants failed to comply with discovery rules, specifically failing to search for, preserve, or produce electronic documents. The court stated "[C]ounsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, what constitutes a 'document'…; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who (at least until July 2001) did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had 'establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests,'…and (5) in the face of the Met's persistent questioning and showings that the production was faulty and incomplete, ridiculed the inquiries, failed to take any action to remedy the situation or supplement the demonstrably false responses, failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced." The court granted severe sanctions, finding liability on the part of the Defendants and ordering the Defendants to pay Plaintiff's attorneys' fees necessitated by the discovery abuse by Defendants and their counsel. The court found that lesser sanctions, such as an adverse inference or preclusion, would not be effective in this case "because it is impossible to know what the Met would have found if the Union and its counsel had complied with their discovery obligations from the commencement of the action."

- *Residential Funding Corp. v. DeGeorge Fin. Corp*., 306 F.3d 99 (2d. Cir. Sept. 26, 2002). Defendants appeal the trial court's denial of Defendants' motion for sanctions, specifically in the form of an adverse jury instruction, for the Plaintiff's failure to produce email in time for trial. The Second Circuit held that where a party breaches a discovery obligation by failing to produce evidence, the trial court has broad discretion in fashioning an appropriate sanction, including the discretion to delay the start of a trial, to declare a mistrial, or to issue an adverse inference instruction. Sanctions may be imposed where a party has not only acted in bad faith or grossly negligent, but also through ordinary negligence. Vacating the trial court's sanctions order, the Circuit Court reversed and remanded with instructions for a renewed hearing on discovery sanctions.

- *Williams v. Saint-Gobain Corp*., 2002 WL 1477618 (W.D.N.Y. June 28, 2002). In an employment discrimination suit, the Court refused to issue sanctions or attorney's fees stemming from myriad discovery disputes. Despite an earlier assertion that no further responsive documents could be located, the Defendant produced emails obtained from an executive's computer five days before trial. The Court found no evidence of any bad faith as to the withholding or destruction of the emails and issued the parties an extended time period to complete discovery. The Court ordered each party to bear its own discovery costs.

- *DeLoach v. Philip Morris Co*., 206 F.R.D. 568 (M.D.N.C. Apr. 3, 2002). Plaintiffs sought discovery sanctions alleging that the Defendant's expert report relied on computerized transaction data that was deliberately withheld from Plaintiffs during discovery. The discovery request at issue sought "[a]ll summary documents (including electronic data) relating to your leaf tobacco bids, purchases, or price paid, including but not limited to the entire Tobinet database in electronic form, but excluding individual transaction documents such as purchase orders and invoices." Plaintiffs were only provided the database data after the Defendant's expert report was issued (in which the Defendant's expert relied heavily on this other computerized data). The court held that the withholding of the data resulted in unfairness to the Plaintiffs and allowed the Plaintiffs to respond to the report and provided no opportunity for the Defendant to reply.

- *Cobell v. Norton*, 206 F.R.D. 324 (D.D.C. Mar. 29, 2002). The court issued sanctions, including attorneys fees and expenses, under Rule 37 based upon Defendants' request for a protective order clarifying that it "may produce email in response to discovery requests by producing from

paper records of email messages rather than from backup tapes and may overwrite backup tapes." The Defendants had previously been ordered to produce the email messages from the back-up tapes. The court held that the Defendants' motion for protective order clarifying their duty to produce the email was not appropriate.

- *Sheppard v. River Valley Fitness One*, 2001 U.S. Dist. LEXIS 15801 (D.N.H. Sept. 27, 2001). Plaintiffs served several requests for discovery upon Defendant which defined the term "documents" broadly, encompassing both paper documents and electronic communications. However, Defendant's attorney (Whittington) failed to turn over the requested documents in a timely fashion and some of the documents were lost or destroyed. The Court held, "Notwithstanding Whittington's habit of trying to obstruct discovery in this case, I find that in this instance Whittington's failure to produce computer records and to retain all drafts or other documents relating to the Aubin settlement reflects a lack of diligence rather than an intentional effort to abuse the discovery process. Nevertheless, Whittington's failure to fully comply with this court's March 22 order has unfairly prejudiced the plaintiffs by depriving them of the opportunity to question Aubin about the contents of the documents." The Court ordered the Defendant's attorney to pay $500 to the Plaintiff.

- *Lexis-Nexis v. Beer*, 41 F.Supp.2d 950 (D. Minn. 1999). Employer sued former employee for misappropriation of trade secrets. Court issued monetary sanctions against former employee where former employee failed to produce a specific copy of an electronic database he made at the time of his resignation.

- *New York State Nat'l Org. for Women v. Cuomo*, 1998 WL 395320 (S.D.N.Y. July 14, 1998). The court refused to impose sanctions on Defendants for destroying computer databases where there was no showing that the Defendants deleted computer databases or destroyed monthly summary reports in order to impede litigation and the plaintiffs failed to demonstrate that they were prejudiced by the loss of the records.

- *In re Prudential Ins. Co. Sale Practices Litig.,* 169 F.R.D. 598 (D.N.J. 1997). Life insurer's consistent pattern of failing to prevent unauthorized document destruction in violation of a court order, in a suit alleging deceptive sales practices, warranted sanctions requiring payment of $1 million to court and payment of some Plaintiff's attorney fees and costs.

- *Gates Rubber Co. v. Bando Chem. Ind.,* 167 F.R.D. 90 (D. Colo. 1996). The court awarded sanctions (ten percent of Plaintiff company's total attorney fees and costs) where Defendant's employees continuously destroyed (by overwriting) electronic evidence. Court criticized Defendant's expert for not making an image copy of the drive at issue for production.

- *Crown Life Ins. Co. v. Craig*, 995 F.2d 1376, 1382-83 (7th Cir. 1993). Affirmed trial court's decision to sanction insurer and enter default judgment (counterclaim) against insurer when it failed to comply with discovery order requesting raw data from database. Data from a computer said to be "documents" within the meaning of FRCP 34.

- *American Banker Ins. Co. v. Caruth*, 786 S.W.2d 427 (Tex. Ct. App. 1990). Courts can impose sanctions on parties that fail to comply with electronic discovery requests.

- *Capellupo v. FMC Corp.*, 126 F.R.D. 545 (D. Minn. 1989). In gender-based employment discrimination action, court held that employer's knowing and intentional destruction of documents warranted an order requiring employer to reimburse employees for twice resulting expenditures.

- *Leeson v. State Farm Mut. Ins. Co*., 546 N.E.2d 782 (Ill. App. Ct. 1989). Appellate Court held that Defendant's claims were justified on grounds of oppressiveness, and therefore; the trial court abused its discretion in entering default sanctions for Defendant's failure to comply with the discovery order. Such production would have been overly burdensome where compliance would have required Defendant to create a computer program to find the records and at least 15 minutes for an analyst to look through each of the 2,100 claims.

- *National Assoc. of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D. Cal. 1987). Court imposed sanctions on party that altered and destroyed computer documents in the regular course of business. Court appointed special master to over-see the discovery process.

Work Product Doctrine & Privilege

- *RLS v. United Bank of Kuwait*, 2003 WL 1563330 (S.D.N.Y. Mar. 26, 2003). In a contract dispute arising from the Defendant's alleged failure to pay the Plaintiff commissions due under the terms of written consulting

agreements, the court concluded that the Defendant did not meet its burden of demonstrating that two emails were subject to privilege protection under the common interest rule.

- *Murphy Oil USA v. Fluor Daniel*, No. 2:99-cv-03564 (E.D. La. Dec. 3, 2002). This Order follows the court's decision in *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D. La. Feb. 19, 2002) ordering the Defendant to produce relevant email communications archived on backup tapes. In this motion to compel before the court, the Plaintiff sought production of a particular email and argued that the Defendant waived the attorney-client privilege by voluntarily producing the contents of an email. Two copies of the email in question existed on the Defendant's backup tapes: (1) the email attached to a message from the mail system administrator stating that the attached email was not deliverable due to an error in the mail address and (2) a copy of the same email sent to the correct email address. The Defendant produced a privilege log identifying the subject email as an attorney-client communication, but at the same time inadvertently produced the administrator email and attachment. The court held that this inadvertent disclosure waived the attorney-client privilege and granted the Plaintiff's motion to compel.

- *eSpeed, Inc. v. Chicago Board of Trade,* 2002 WL 827099 (S.D.N.Y. May 1, 2002). Cantor Fitzgerald, a third party and partial owner of Plaintiff, asserted the attorney-client privilege with respect to a series of emails and attachments addressing a patent purchase negotiation. These emails and attachments were sent by an outside attorney to an employee of Cantor Fitzgerald. The court examined the emails and attachments *in camera* and ordered production finding that the messages and documents did not contain client confidences and were not privileged.

- *Harris v. WHMC, Inc.*, 2002 WL 1821989 (Tx. Ct. App. Aug. 8, 2002). In a medical malpractice suit, the Plaintiff appealed the trial court's exclusion from evidence certain email correspondence based on privilege. The trial court ruled that the Plaintiff could use the emails at trial for impeachment purposes, but the emails themselves would not be admitted. The Appellate Court concluded that even if the trial court erred in excluding the emails, it was harmless error and did not cause an improper judgment.

- *Hambarian v. C.I.R.*, 118 T.C. 35 (U.S. Tax Ct. June 13, 2002). For use in connection with a criminal tax proceeding, the Defendants' attorney created searchable, electronic databases containing documents turned over by the Prosecutor during discovery. The Respondent, in the civil tax

proceeding at bar, sought a motion to compel discovery of these electronic document databases from the Petitioners/Defendants. The court stated that "As the Petitioner failed to make the requisite showing of how the disclosure of the documents selected would reveal the defense attorney's mental impressions of the case, the requested documents and computerized electronic media are not protected by the work product doctrine."

- *City of Reno v. Reno Police Protective Assoc.*, 59 P.3d 1212 (Nev. 2002). The court overturned the Employee Relations Board's decision that documents sent by email cannot be considered privileged. The court stated that "[C]ourts have generally looked to the content and recipients of the email to determine if the email is protected" and held that documents transmitted by email are protected by the attorney-client privilege.

- *Koen v. Powell*, 212 F.R.D. 283 (E.D. Pa. 2002). In a legal malpractice suit, the court held that the attorney-client privilege and work product doctrine did not shield the Defendants from turning over emails relating to the threatened malpractice suit.

- *Bertsch v. Duemeland*, 639 N.W.2d 455 (N.D. 2002). *Bertsch v. Duemeland*, 639 N.W.2d 455 (N.D. 2002). In an action alleging tortious interference with a business relationship, the appellate court affirmed a lower court's denial of the Plaintiff's motion to compel discovery of data from some of the Defendant's computers. Specifically, the court denied the Plaintiff access to computers purchased by the Defendant after the transaction that gave rise to the litigation. The court reasoned that the resulting data could not be relevant to the case, and that granting access "would not lead to relevant information" and "could result in disclosure of privileged and confidential information." The court had previously permitted e-discovery of the Defendant's computer that was owned at the time of the alleged torts.

- *United States v. Sungard Data Systems*, 173 F.Supp.2d 20 (D.D.C. 2001). In an antitrust action, the Court set forth specific confidentiality requirements, including a precise method for designating confidential electronic documents.

- *Long v. Anderson University*, 2001 WL 1381512 (S.D.Ind. Oct. 30, 2001). The Court found that the attorney-client privilege applied to electronic mail sent from a University human resources director to the dean of

students regarding a conversation with counsel and his legal advice in a Civil Rights action against the University.

- *Wesley College v. Pitts*, 1997 WL 557554 (D. Del. Aug. 11, 1997). The court found that the Defendant waived its work-product privilege where the email was distributed to several third parties.

- *State of Minnesota v. Phillip Morris*, 1995 WL 862582 (Minn. Ct. App. Dec. 26, 1995). Petitioners seek relief from a trial court's discovery order claiming that the material is attorney work product. The trial court made specific findings that (a) the computerized databases include fields containing objective information, (b) release of the specified information will not reveal the impressions, opinions, or theories of counsel, and (c) respondents have met the standards for disclosure. Both the trial court and the Court of Appeals found unpersuasive the Petitioners' argument that the mere selection of documents for inclusion in the database would reveal attorney strategies.

- *Scovish v. Upjohn Co.*, 1995 WL 731755 (Conn. Super. Ct. Nov. 22, 1995). The Court found that database was within attorney work-product, but that Plaintiff had substantial need of the information in the database and undue hardship would result if it was not produced. The Court ordered Defendant to produce the database after removing any portions that contain subjective thoughts and opinions.

- *Ciba-Geigy Corp. v. Sandoz, Ltd*., 916 F. Supp. 404 (D.N.J. 1995). Defendants produced all documents from database without conducting a privilege review. The court held that privilege is waived where the disclosure is a result of "gross negligence."

- *United States v. Keystone Sanitation Co.*, 885 F. Supp. 672 (M.D. Pa. 1994). In complying with the court's discovery order, Defendants inadvertently disclosed email messages that contained potentially confidential communications. This inadvertent disclosure waived any attorney-client privilege that may have protected portions of the email.

- *IBM v. Comdisco, Inc.,* 1992 WL 52143 (Del. Super. Ct. Mar. 11, 1992). The court allowed production of a portion of an email message claimed to be privileged because a portion of the email message was intended to be disclosed to persons outside the attorney/client privilege. Because it relayed legal advice from IBM's counsel, the other portion of the email was found to be privileged.

- *Burroughs v. Barr Lab., Inc*., 143 F.R.D. 611 (E.D.N.C. 1992), *vacated in part on other grounds* 40 F.3d 1223 (Fed. Cir. 1994). The court held that the attorney work product privilege applied to printed results of computerized database searches.

- *Indiana Coal Council v. Nat'l Trust for Historic Preservation,* 118 F.R.D. 264 (D. D.C. 1988). The court held that the work product doctrine prevented the Plaintiff from gaining access to the Defendant's legal research resources and findings conducted through a computer assisted legal research system.

- *Hoffman v. United Telecomms., Inc*., 117 F.R.D. 436 (D. Kan. 1987). In an interrogatory, Plaintiff requested specific information concerning a computer file containing information regarding possible employment discrimination. The court denied requesting party's motion to compel finding that since the data would reveal Defendant's discovery plan, the information was protected by the work-product doctrine.

- *Transamerican Computer Co. v. IBM*, 573 F.2d 646 (9th Cir. 1978). The court was more lenient regarding waiver of privilege where the party was required to produce larger amounts of data and where they actually performed some degree of privilege review.

Experts

- *Premier Homes and Land Corp. v. Cheswell, Inc*., 240 F.Supp.2d 97 (D.Mass. 2002). In a property dispute, Plaintiff used an email purportedly sent from one of Defendant's stockholders to Plaintiff's president to form the core of its claim that the Defendant was not complying with the terms of a lease. The Defendant filed an ex parte motion to preserve certain electronic evidence and expedite the production of electronic records. The court, stating that it was necessary to determine the origin of the disputed email, ordered Defendant's experts to create mirror images of Plaintiff's computer hard drives, backup tapes, and other data storage devices. Soon thereafter, the Plaintiff confessed to his attorney that he had fabricated the email by pasting most of a heading from an earlier, legitimate message and altering the subject matter line. The Defendant's motion to dismiss was granted and the court ordered the Plaintiff to pay the Defendant's attorney and expert fees and court costs for committing a fraud on the court.

- *Taylor v. State*, 93 S.W.3d 487 (Tex.App. 2002). On appeal, the Defendant argued that the trial court's refusal to order the State to provide him with a complete copy of the hard drive in question as "material physical evidence" for inspection requires reversal. Likening the situation to a drug case in which the Defendant has the right to have the contraband reviewed by an independent expert, the appellate court stated, "mere inspection of the images … is not the same as an inspection of the drive itself (or an exact copy thereof). It is certainly not the same as an independent forensic examination of the contents of the hard drive by an expert."

- *In re Pharmatrak, Inc. Privacy Litigation*, 220 F.Supp.2d 4 (D. Mass. 2002), *rev'd on other grounds*, *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003). In a class action Privacy matter, the Plaintiffs alleged that Defendants had secretly intercepted and accessed Plaintiffs' personal information and Web browsing habits through the use of "cookies" and other devices, in violation of state and federal law. The Plaintiffs raised claims under The Wiretap Act, The Stored Communications Act, and The Computer Fraud and Abuse Act. Using computer forensic tools, Plaintiffs' expert was able to analyze the Defendant's Website tracking logs and determine that the Defendant had captured and possessed detailed private information about the Plaintiffs, including their: names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, occupations, and email content. Finding that the Plaintiffs failed to establish necessary elements of each of the above listed statutes, the Court issued Summary Judgment in favor of the Defendant.

- *United States v. Lloyd,* 269 F.3d 228 (3rd Cir. 2001). The Third Circuit has ruled that a man convicted of planting a computer "time bomb" that crippled operations at New Jersey-based Omega Engineering Corp. is not entitled to a new trial on the basis of a juror prejudice. The ruling reinstates the verdict in which the Defendant was convicted on one count of computer sabotage. Computer experts were essential in recovering the evidence of the "time bomb".

- *Munshani v. Signal Lake Venture Fund II*, 13 Mass.L.Rptr. 732 (Mass.Super. 2001). In a dispute over authentication of an email message, the Court appointed a neutral computer forensics expert. Based on the expert's analysis and report, the Court found that the Plaintiff intentionally fabricated the disputed email and then attempted to hide that fabrication.

The Court dismissed the Plaintiff's suit and ordered him to pay the Defendant's expert and attorney fees.

- *Northwest Airlines v. Local 2000*, C.A. No. 00-08DWF/AJB (D. Minn. Feb. 2, 2000) (Order on Defendants' Motion for Protective Order and Plaintiff's Motion to Compel Discovery); *Northwest Airlines v. Local 2000*, C.A. No. 00-08DWF/AJB (D. Minn. Feb. 29, 2000) (Memorandum Opinion and Order). Court ordered Plaintiff's expert to act as a neutral 3rd party expert; on behalf of the court, the expert collected and imaged the Defendants' personal hard drives and provided the parties with a complete report of all data "deemed responsive." Court issued detailed protocol for conducting the electronic discovery.

- *Simon Property Group v. mySimon, Inc.,* 194 F.R.D. 639 (S.D. Ind. 2000). On Plaintiff's motion to compel in a trademark case, the court held that Plaintiff was entitled to attempt to recover deleted computer files from computers used by Defendant's employees. The court required that protective measures be taken, including Plaintiff's appointment of an expert who would serve as an officer of the court and turn over the recovered information to Defendant's counsel for appropriate review.

- *Playboy Enters., Inc. v. Welles,* 60 F.Supp.2d 1050 (S.D. Cal. 1999). The court appointed a computer expert who specialized in the field of electronic discovery to create a "mirror image" of Defendant's hard drive. Court reserved Respondent's right to object to production after data capture by expert and review of materials.

- *National Assoc. of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D. Cal. 1987). Court imposed sanctions on party that altered and destroyed computer documents in the regular course of business. Court appointed special master to oversee the discovery process.

- *United States v. IBM,* 76 F.R.D. 97 (S.D.N.Y. 1977) Where Defendant was to produce information to plaintiff pursuant to prior court orders, but production did not comport with spirit and intent of those orders and was highly technical and complex in nature, the court determined that "exceptional conditions" existed, warranting appointment of examiner. The examiner's duties included reporting to court as to information that Defendant possessed and produced and supervising discovery.

Computer Forensic Protocols

- *Four Seasons Hotels and Resorts v. Consorcio Barr*, 2003 WL 21212185 (S.D.Fla. May 9, 2003). The Plaintiff brought an action against the Defendant licensee alleging, among other things, violations of the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Uniform Trade Secrets Act. A computer forensic investigation revealed that the Defendant accessed the Plaintiff's computer network, downloaded confidential data onto backup tapes, fabricated electronic evidence, and deleted files and overwrote data prior to his computer being turned over for inspection to the Plaintiff. The court held that the Defendant acquired the Plaintiff's confidential customer information through improper means, namely, by theft and by espionage through electronic means. The court issued a judgment for the Plaintiff and ordered monetary damages, among other relief.

- *People v. Carratu*, 755 N.Y.S.2d 800 (N.Y. Sup. Ct. 2003). Defendant moved to suppress computer evidence seized from his home and subsequently searched by the police department's computer forensic examiners. The Defendant claimed that the search warrants and supporting affidavits limited the search to documentary evidence relating to his illegal cable box operation and thus, the forensic examiner violated the Defendant's Fourth Amendment rights upon inspection of non-textual files with folder names clearly relating to other illegal activity. Granting the suppression motion, in part, the court stated, "In view of the Fourth Amendment's 'particularity requirement,' a warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity."

- *United States v. Triumph Capital Group*, 211 F.R.D. 31 (D.Conn. 2002). In order to prevent spoliation of evidence in a public corporation case, the government sought and obtained a search warrant to search and seize a laptop computer at issue. The warrant did not limit the search to any particular area of the hard drive. However, it did limit the government to search for and seize only certain evidence relating specifically to the charges and to follow detailed protocols to avoid revealing any privileged information. So that the data would not be altered, the government made mirror images of the hard drive and then proceeded with the computer forensic investigation. The Defendants argued that this mirroring amounted to a search and seizure of the entire hard drive and moved to suppress all evidence from the laptop. The court determined that although

the search warrant limited the scope of the information that investigators could search for, technical realities required the government to make complete mirror images of the hard drive. Furthermore, the court ruled that copying a file does not necessarily constitute seizure of that file and that examining a file more than once does not constitute multiple searches under the Fourth Amendment.

- *United States v. Al-Marri*, 230 F.Supp.2d 535 (S.D.N.Y. 2002). In the wake of the September 11th attacks, the FBI visited the Defendant's home perusing tips of the Defendant's allegedly suspicious activity. The FBI agents obtained the Defendant's consent to search his home and, with his affirmative consent and cooperation, seized his laptop computer, disks, and CDs for further investigation. Investigation of the computer hardware revealed evidence of credit card fraud. The Defendant moved to suppress the computer evidence, arguing that even if he validly consented to a search of his home, that consent did not encompass the contents of his computer. The Court denied the motion to suppress and ruled that the FBI's lawful search of the Defendant's home encompassed the right to search the computer as a closed container.

- *State v. Townsend,* 57 P.3d 255 (Wash. 2002) (Bridge, J. concurring). The principal issue the court resolved was whether a police officer violated a provision in Washington's privacy act when he saved and printed email and real time client-to-client ICQ messages between Defendant and a fictitious child. The court upheld the conviction and held that the act was not violated. In a concurring opinion, one judge further addressed the unique aspects of electronically created and stored email. "Technically, email messages are permanently recorded since 'most email programs keep copies of every message a user ever wrote, every message the user ever received, and every message the user deleted.'…Although some email services may offer the possibility of 'shredding' an email message, arguably the equivalent of actually deleting it, the email file may still be retrievable using certain software. 'A deleted file is really not a deleted file, it is merely organized differently.' "

- *Moench v. Red River Basin Board*, 2002 WL 31109803 (Minn. Ct. App. Sept. 24, 2002). Plaintiff was forced to resign from his executive director position after being confronted with allegations that pornographic images were found on his computer. The Plaintiff's employer used a computer forensic expert to investigate the pornographic material stored in the cache file of the Plaintiff's computer. Given that the Plaintiff's employment was terminated for cause, the Commissioner of Economic Security refused to

issue unemployment benefits. The appellate court reversed the denial of benefits stating that the evidence in the record did not support the finding that the Plaintiff intentionally downloaded or stored any pornographic material on his computer.

- *Ingenix, Inc. v. Lagalante*, 2002 U.S. Dist. LEXIS 5795 (E.D. La. Mar. 28, 2002). Defendant left his employment with the Plaintiff to work for Plaintiff's competitor as a vice president of sales. The Plaintiff (Defendant's former employer) filed suit against Defendant alleging fraudulent, abusive, and knowing misappropriation of computer files and proprietary information causing damage in excess of $5,000 in violation of the Computer Fraud and Abuse Act. While the CFAA is a criminal statute, the court affirmed the rule that a violation of the statute can provide the basis for civil liability. Plaintiff's allegations were based upon evidence that the Defendant had misused his company laptop and took steps to appropriate data relating to customers "in the sales funnel" for his new employer. A computer forensic examination of email messages sent by Defendant and the pattern of Defendant's use and downloading of files from his laptop revealed that he had, in fact, downloaded and deleted confidential and proprietary customer information for use by Plaintiff's competitor.

- *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002). In a criminal prosecution for possession of child pornography, Yahoo! technicians retrieved, pursuant to a search warrant, all information from the Defendant's email account. The lower court ruled that the seizure of the emails by Yahoo! was unlawful because police were not present when the Defendant's email account was searched. Reversing the lower court's opinion, the appellate court held that Yahoo!'s search of the Defendant's emails without a police officer present was reasonable under the Fourth Amendment and did not violate the Defendant's privacy rights.

- *United States v. Tucker*, 150 F.Supp.2d 1263 (D. Utah 2001). The Defendant was found guilty of knowing possession of child pornography. The conviction was largely supported by computer forensic evidence found in the form of deleted Internet cache files that were saved to the Defendant's hard drive when he viewed the various websites.

- *State v. Guthrie*, 627 N.W.2d 401 (S.D. 2001). In a criminal prosecution for murder, a computer specialist conducted several forensic searches on a computer used by the Defendant, finding that the computer had been used to conduct numerous Internet searches on subjects related to the incidents

surrounding the murder. In addition, the forensic analysis was able to reveal that a computer printed suicide note, offered to exculpate the Defendant, was created several months after the victim's death. *State v. Guthrie*, 2002 WL 31618440 (S.D. Nov. 20, 2002). Anticipating that the State would not have time to thoroughly examine the evidence against the Defendant for murdering his wife, Defense counsel failed to disclose the victim's purported computerized suicide note during the discovery period. The appellate court affirmed the trial court's finding that defense counsel acted in bad faith by holding this evidence back from discovery. The appellate court also held that the fees of the State's computer forensic expert were reasonable because the expert was highly qualified in computer forensics.

- *Adobe Sys., Inc. v. Sun South Prod., Inc.,* 187 F.R.D. 636 (S.D. Cal. 1999). In a computer piracy suit, the Court denied Plaintiff's *ex parte* application for a temporary restraining order. The Court based its decision on the fact that it is more difficult to erase evidence that is magnetically encoded on a computer hard disk than it is to physically destroy floppy disks, compact discs, invoices, and other tangible forms of evidence. "Manual or automated deletion of that software may remove superficial indicia, such as its icons or presence in the user's application menu. However, telltale traces of a previous installation remain, such as abandoned subdirectories, libraries, information in system files, and registry keys…Even if an infringer managed to delete every file associated with Plaintiffs' software, Plaintiffs could still recover many of those files since the operating system does not actually *erase* the files, but merely marks the space consumed by the files as free for use by other files."

- *Byrne v. Byrne,* 650 N.Y.S.2d 499 (N.Y. Sup. Ct. 1996). In a divorce proceeding, the wife sought access to her husband's computer, which husband used for both business and personal purposes even though computer was provided by husband's employer. The wife was awarded such access to search the computer for information about the couple's finances and marital assets.

Admissibility

- *J.P. Morgan Chase Bank v. Liberty Mutual Ins.*, 2002 WL 31867731 (S.D.N.Y. Dec. 23, 2002). In a suit against insurance companies that had guaranteed payment in the event of Enron's bankruptcy, the court weighed the admissibility of several emails. The court determined that emails authored by senior bank officials would be allowed into evidence and that

a reasonable juror could find these emails probative of the Defendants' central proposition that the transactions were actually uninsurable "off-the-books" loans.

- *Kearley v. Mississippi,* 843 So.2d 66 (Miss. Ct. App. 2002). A criminal defendant was convicted of sexual battery and appealed on several issues including proper authentication of emails which he allegedly sent to the victim. The appellate court held that the victim's testimony that she had received and printed the emails on her computer was sufficient authentication under the rules of evidence, and the court upheld the conviction.

- *State v. Cook*, 2002 WL 31045293 (Ohio Ct. App. Sept. 13, 2002). Defendant appealed his conviction for possessing nude images of minors, claiming in part that the trial court erred in admitting materials, over the Defendant's objection, that were generated from a "mirror image" of the Defendant's hard drive. After a detailed discussion of the mirror imaging process, the authenticity of the data taken from the image, and the possibility for tampering, the appellate court found that the trial court properly admitted the evidence.

- *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146 (C.D. Cal. April 22, 2002). In a copyright and trademark infringement action, the Court refused to find that all evidence printed from websites is inauthentic and inadmissible. Instead, the Court found that the printouts were properly authenticated under Fed.R.Evid. 901(a) where the plaintiff's CEO adequately established that the exhibits attached to his declaration were "true and correct copies of pages printed from the Internet that were printed by [him] or under his direction."

- *New York v. Microsoft Corp.*, 2002 WL 649951 (D.D.C. Apr. 12, 2002). Microsoft challenged several emails appended to the written testimony of one of the Plaintiff's witnesses, claiming that the statements contained therein were inadmissible hearsay. The court excluded multiple email messages using the following reasoning: (1) they were offered for the truth of the matters they asserted, (2) had not been shown to be business records as required under Rule 803(6), and (3) contained multiple levels of hearsay for which no exception had been established.

- *Sea-Land Service, Inc. v. Lozen Int'l,* 285 F.3d 808 (9th Cir. April 3, 2002). The Court ruled that the trial court should have admitted an internal company email, which an employee of the plaintiff had forwarded to the

defendant. The defense persuasively argued on appeal that the email was not excludable hearsay because her remarks in forwarding the email manifested an adoption or belief in truth of the information contained in the original email. The Court ruled that this satisfied the requirements for an adoptive admission under Fed.R.Evid. 801(d)(2)(B).

- *Harveston v. State*, 798 So.2d 638 (Miss. Ct. App. 2001). In a criminal burglary prosecution, the Court refused to allow in computer database print-outs under the State's business records exception to the hearsay rule. The Court held that the State failed to meet its burden because "[T]here was no evidence offered as to the means by which the information…was compiled. The only testimony came from an investigating officer who limited his testimony to the fact that law enforcement officers routinely make use of such information. [However, t]he reliability of the information in 'business records' is determined by the competence of the *compiler* of the information and not the extent of the *consumer's* reliance on information received from another source."

- *V Cable Inc. v. Budnick*, 23 Fed.Appx. 64 (2nd Cir. 2001). In an investigation of illegal sales and distribution of cable equipment, the police seized computers believed to contain relevant evidence of the crime. After holding the computers in question, the police sent them to an independent software company for analysis. Appellant's argument implies that, once they left police custody, the computers and any records obtained there from became corrupted and, therefore, inadmissible under Rule 803(6) of the Federal Rules of Evidence. The Court found the documents to be sufficiently trustworthy to be admitted under Rule 803(6).

- *United States v. Meienberg*, 263 F.3d 1177 (10th Cir. 2001). The government introduced print-outs of computerized records and the Defendant objected to these print-outs based on lack of authentification. The Court held that the government met its burden by presenting a witness who testified that the print-outs were a record of all transactions. The Court held that this was in accordance with Federal Rule of Evidence 901(b)(7).

- *Bowe v. State*, 785 So.2d 531 (Fla. Dist. Ct. App. 2001). "An email 'statement' sent to another is always subject to the limitations of the hearsay rule."

- *People v. Markowitz*, 721 N.Y.S.2d 758 (N.Y. Sup. Ct. 2001). In a larceny and possession of stolen property suit, the court admitted

computer databases that indicated how much money should have been collected by the defendant toll-booth worker. The testimony of an employee of the company that prepared the databases was sufficient foundation for admission of the electronic records.

- *Hardison v. Balboa Ins. Co*., 4 Fed. Appx. 663 (10th Cir. 2001). To prove that an insurance company had followed notice of cancellation requirements, the court admitted computer files and print-outs regarding how the cancelled policy was processed and maintained. The court stated that computer business records are admissible under Rule 803(6) "if the offeror establishes a sufficient foundation in the record for [their] introduction."

- *Broderick v. State*, 35 S.W.3d 67 (Tex. App. 2000). In child sex abuse prosecution, the court affirmed the trial court's admission of a duplicate of defendant's hard drive, in place of the original. The court concluded that the state's best evidence rule did not preclude admission because the computer expert testified that the copy of the hard drive exactly duplicated the contents of the hard drive.

- *St. Clair v. Johnny's Oyster & Shrimp*, 76 F.Supp.2d 773 (S.D. Tex. 1999). "[A]ny evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception."

- *SKW Real Estate Ltd. v. Gallicchio*, 716 A.2d 903 (Conn. App. Ct. 1998). A computer-generated document is admissible in a foreclosure action, pursuant to the business records exception to the hearsay rule.

- *Monotype Corp. v. Int'l Typeface Corp*., 43 F.3d 443 (9th Cir. 1994). The court declined admission of a detrimental email in a license infringement action, due to the prejudicial nature of the message and fact that the email was not admissible under the business record exception.

- *United States v. Bowers*, 920 F.2d 220 (4th Cir. 1990). Computer data consisting of IRS taxpayer data compilations is admissible as official records.

- *United States v. Catabran*, 836 F.2d 453 (9th Cir. 1988). Computer printouts are admissible as business records under the Federal Rules of Evidence 803(6), provided that proper foundational requirements are first established.

- *State of Wash. v. Ben-Neth*, 663 P.2d 156 (Wash. Ct. App. 1983). Computer-generated evidence is hearsay but may be admitted as a business record provided a proper foundation is laid.

- *United States v. Vela,* 673 F.2d 86 (5th Cir. 1982). The court admitted computerized telephone bills under the Business Records exception where a telephone company employee laid the proper foundation for the reliability of the telephone bills record-keeping process. In describing the reliability of the computer generated documents, the court stated that the computerized reports "would be even more reliable than ... average business record(s) because they are not even touched by the hand of man."

SAMPLE PRESERVATION LETTER - TO OPPONENT OR 3RD PARTY

June 1, 2003

_____
_____
_____

RE: [Case Name] - Data Preservation

Dear _____:

Please be advised that [Plaintiffs / Defendants / Third Party] believe electronically stored information to be an important and irreplaceable source of discovery and / or evidence in the above-referenced matter.

The discovery requests served in this matter seek information from [Plaintiffs' / Defendants'] computer systems, removable electronic media and other locations. This includes, but is not limited to, e-mail and other electronic communication, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, Internet usage files, and network access information.

The laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence. Due to its format, electronic information is easily deleted, modified or corrupted. Accordingly, [Plaintiffs / Defendants / Third Party] must take every reasonable step to preserve this information until the final resolution of this matter. This includes, but is not limited to, an obligation to discontinue all data destruction and backup tape recycling policies.

If this correspondence is in any respect unclear, please do not hesitate to call me.

Sincerely,

_____

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

LAURA ZUBULAKE,

Plaintiff,

-against-

UBS WARBURG LLC, UBS WARBURG, and UBS AG,

Defendants.

- x

OPINION AND ORDER

02 Civ. 1243 (SAS)

SHIRA A. SCHEINDLIN, U.S.D.J.:

The world was a far different place in 1849, when Henry David Thoreau opined (in an admittedly broader context) that "[t]he process of discovery is very simple."[1] That hopeful maxim has given way to rapid technological advances, requiring new solutions to old problems. The issue presented here is one such problem, recast in light of current technology: To what extent is inaccessible electronic data discoverable, and who should pay for its production?

I. INTRODUCTION

The Supreme Court recently reiterated that our "simplified notice pleading standard relies on liberal discovery rules and summary judgment motions to define disputed facts and issues and to dispose of unmeritorious

[1] Henry David Thoreau, A Week on the Concord and Merrimack Rivers (1849).

claims."[2] Thus, it is now beyond dispute that "[b]road discovery is a cornerstone of the litigation process contemplated by the Federal Rules of Civil Procedure."[3] The Rules contemplate a minimal burden to bringing a claim; that claim is then fleshed out through vigorous and expansive discovery.[4]

In one context, however, the reliance on broad discovery has hit a roadblock. As individuals and corporations increasingly do business electronically[5] -- using computers to create and store documents, make deals, and exchange e-mails the universe of discoverable material has expanded exponentially.[6] The more information there is to discover, the more expensive it is to discover all the relevant information until, in the end, "discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.[7]

This case provides a textbook example of the difficulty of balancing the competing needs of broad discovery and manageable costs. Laura

---

[2] Swierkiewicz v. Sorema, N.A., 534 U.S. 506, 512 (2002).

[3] Jones v. Goord, No. 95 Civ. 8026, 2002 Wh 1007614, at (S.D.N.Y. May 16, 2002).

[4] See Hickman v. Taylor, 329 U.S. 495, 500-01 (1947).

[5] See Wendy R. Liebowitz, Digital Discovery Starts to Work, Nat'l L.J., Nov. 4, 2002, at 4 (reporting that in 1999, ninety-three percent of all information generated was in digital form).

[6] Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 429 (S.D.N.Y. 2002) (explaining that electronic data is so voluminous because, unlike paper documents, "the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it"), aff'd, 2002 WL 975713 (S.D.N.Y. May 9, 2002).

[7] Rowe, 205 F.R.D. at 423.

Zubulake is suing UBS Warburg LLC, UBS Warburg, and UBS AG (collectively, "UBS" or the "Firm") under Federal, State and City law for gender discrimination and illegal retaliation. Zubulake's case is certainly not frivolous[8] and if she prevails, her damages may be substantial.[9] She contends that key evidence is located in various e-mails exchanged among UBS employees that now exist only on backup tapes and perhaps other archived media. According to UBS, restoring those e-mails would cost approximately $1"75,000.00, exclusive of attorney time in reviewing the e-mails.[10] Zubulake now moves for an order compelling UBS to produce those e-mails at its expense.[11]

II. BACKGROUND

A. Zubulake's Lawsuit

UBS hired Zubulake on August 23, 1999, as a director and senior salesperson on its U.S. Asian Equities Sales Desk (the "Desk"), where she

[8] Indeed, Zubulake has already produced a sort of "smoking gun": an e-mail suggesting that she be fired "ASAP" after her EEOC charge was filed, in part so that she would not be eligible for year-end bonuses. See 8/21/01 e-mail from Mike Davies to Rose Tong ("8/21/01 e-Mail"), Ex. G to the 3/17/03 Affirmation of James A. Batson, counsel for Zubulake ("Batson Aff.").

[9] At the time she was terminated, Zubulake's annual salary was approximately $500,000. Were she to receive full back pay and front pay, Zubulake estimates that she may be entitled to as much as $13,000,000 in damages, not including any punitive damages or attorney's fees. See Memorandum of Law in Support of Plaintiff's Motion for an Order Compelling Defendants to Produce E-mails, Permitting Disclosure of Deposition Transcript and Directing Defendants to Bear Certain Expenses ("P1. Mem.") at 2-3.

[10] See 3/26/03 Oral Argument Transcript (113/26/03 Tr.") at 14, 44-45.

[11] Zubulake also moves for an order (1) directing UBS to pay for the cost of deposing Christopher Behny, UBS's information technology expert and (2) permitting her to disclose the transcript of Behny's deposition to certain securities regulators. Those motions are denied in a separate Opinion and Order issued today.

reported to Dominic Vail, the Desk's manager. At the time she was hired, Zubulake was told that she would be considered for Vail's position if and when it became vacant.

In December 2000, Vail indeed left his position to move to the Firm's London office. But Zubulake was not considered for his position, and the Firm instead hired Matthew Chapin as director of the Desk. Zubulake alleges that from the outset Chapin treated here differently than the other members of the Desk, all of whom were male. In particular, Chapin "undermined Ms. Zubulake's ability to perform her job by, inter alia: (a) ridiculing and belittling her in front of co-workers; (b) excluding her from work-related outings with male co-workers and clients; (c) making sexist remarks in her presence; and (d) isolating her from the other senior salespersons on the Desk by seating her apart from them.[12] No such actions were taken against any of Zubulake's male co-workers.

Zubulake ultimately responded by filing a Charge of (gender) Discrimination with the EEOC on August 16, 2001. On October 9, 2001, Zubulake was fired with two weeks' notice. On February 15, 2002, Zubulake filed the instant action, suing for sex discrimination and retaliation under Title VII, the New York State Human Rights Law, and the Administrative Code of the City of New York. UBS timely answered on March 12, 2002, denying the allegations. UBS's argument is, in essence, that Chapin's conduct was not

[12] Pl. Mem. at 2.

unlawfully discriminatory because he treated everyone equally badly. On the one hand, UBS points to evidence that Chapin's anti-social behavior was not limited to women: a former employee made allegations of national origin discrimination against Chapin, and a number of male employees on the Desk also complained about him. On the other hand, Chapin was responsible for hiring three new females employees to the Desk.[13]

B. The Discovery Dispute

Discovery in this action commenced on or about June 3, 2002, when Zubulake served UBS with her first document request. At issue here is request number twenty-eight, for "[a]ll documents concerning any communication by or between UBS employees concerning Plaintiff."[14] The term document in Zubulake's request include[es], without limitation, electronic or computerized data compilations." On July 8, 2002, USB responded by producing approximately 350 pages of documents, including approximately 100 pages of e-mails. UBS also objected to a substantial portion of Zubulake's requests.[15]

---

[13] See Defendants' Memorandum of Law in Opposition to Plaintiff's Motion for an Order Compelling Defendants to Produce E-Mails, Permitting Disclosure of Deposition Transcript and Directing Defendants to Bear Certain Expenses ("Def. Mem.") at 2.

[14] Plaintiff's First Request for Production of Documents ¶ to the 28, Ex. E to Declaration of Kevin B. Leblang, counsel to UBS ("Leblang Dec.").

[15] See Defendants' Response to Plaintiff's First Request for Production of Documents, Ex. F to the Leblang Dec.

On September 12, 2002 -- after an exchange of angry letters[16] and a conference before United States Magistrate Judge Gabriel W. Gorenstein -- the parties reached an agreement (the "9/12/02 Agreement"). With respect to document request twenty-eight, the parties reached the following agreement, in relevant part:

> Defendants will [] ask UBS about how to retrieve e-mails that are saved in the firm's computer system and will produce responsive e-mails if retrieval is possible and Plaintiff names a few individuals.[17]

Pursuant to the 9/12/02 Agreement, UBS agreed unconditionally to e-mails from the accounts of five individuals Matthew Chapin, Rose Tong (a human relations representation who was assigned to handle issues concerning Zubulake), Vinay Datta (a co-worker on the Desk), Andrew Clarke (another co-worker on the Desk), and Jeremy Hardisty (Chapin's supervisor and the individual to whom Zubulake originally complained about Chapin). UBS was to produce such e-mails sent between August 1999 (when Zubulake was hired) and December 2001 (one month after her termination), to the extent possible.

UBS, however, produced no additional e-mails that its initial production (the 100 pages of e-mails) was complete. As UBS's opposition to the

---

[16] See Exs. G and H to the Leblang Dec.

[17] 9/18/02 Letter from James A. Batson to Kevin B. Leblang, Ex. I to the Leblang Dec. (emphasis added). See also 9/25/02 Letter from Kevin B. Leblang to James A. Batson, Ex. K to the Leblang Dec. (confirming the above as the parties' agreement).

instant motion makes clear -- although it remains unsaid -- UBS never searched for responsive e-mails on any of its backup tapes. To the contrary, UBS informed Zubulake that the cost of producing e-mails on backup tapes would be prohibitive (estimated approximately $300,000.00).[18]

Zubulake, believing that the 9/12/02 Agreement included production of e-mails from backup tapes, objected to UBS's non-production. In fact, Zubulake knew that there were additional responsive e-mails that UBS had failed to produce because she herself had produced approximately 450 pages of e-mail correspondence. Clearly, numerous responsive e-mails had been created and deleted[19] at UBS, and Zubulake wanted them.

On December 2, 2002, the parties again appeared before Judge Gorenstein, who ordered UBS to produce for deposition a person with knowledge of UBS's e-mail retention policies in an effort to determine whether the backup tapes contained the deleted e-mails and the burden of producing them. In

---

[18] See 3/26/03 Tr. at 14 (Statement of Kevin B. Leblang).

[19] The term "deleted" is sticky in the context of electronic data. "'Deleting' a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status -- thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted -- even if neither the computer user nor the computer itself is aware of their existence. Such data is referred to as 'residual data.'" Shira A. Scheindlin & Jeffrey Rabkin, Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?, 41 B.C. L. Rev. 327, 337 (2000) (footnotes omitted). Deleted data may also exist because it was backed up before it was deleted. Thus, it may reside on backup tapes or similar media. Unless otherwise noted, I will use the term "deleted" data to mean residual data, and will refer to backed-up data as "backup tapes."

response, UBS produced Christopher Behny, Manager of Global Messaging, who was deposed on January 14, 2003. Mr. Behny testified to UBS's e-mail backup protocol, and also to the cost of restoring the relevant data.

C. UBS's E-Mall Backup System

In the first instance, the parties agree that e-mail was an important means of communication at UBS during the relevant time period. Each salesperson, including the salespeople on the Desk, received approximately 200 e-mails each day.[20] Given this volume, and because Securities and Exchange Commission regulations require it,[21] UBS implemented extensive e-mail backup and preservation protocols. In particular, e-mails were backed up in two distinct ways: on backup tapes and on optical disks.

1. Backup Tape Storage

UBS employees used a program called HP OpenMail, manufactured by Hewlett-Packard,[22] for all work-related e-mail

---

[20] See 3/26/03 Tr. at 14 (Statement of Kevin B. Leblang).

[21] SEC Rule 17a-4, promulgated pursuant to Section 17(a) of the Securities Exchange Act of 1934, provides in pertinent part:

> Every [] broker and dealer shall preserve for a period of not less than 3 years, the first two years in an accessible place … [o]riginals of all communications received and copies of all communications sent by such member, broker or dealer (including inter-office memoranda and communications) relating to his business as such.

17 C.F.R. § 240.17a-4(b) and (4).

[22] Hewlett-Packard has since discontinued sales of HP OpenMail, although the company still supports the product and permits existing customers to purchase new licenses. See http://www.openmail.com/.

communications.[23] With limited exceptions, all e-mails sent or received by any UBS employee are stored onto backup tapes. To do so, UBS employs a program called Veritas NetBackup,[24] which creates a "snapshot" of all e-mails that exist on a given server at the time the backup is taken. Except for scheduling the backups and physically inserting the tapes into the machines, the backup process is entirely automated.

UBS used the same backup protocol during the entire relevant time period, from 1999 through 2001. Using NetBackup, UBS backed up its e-mails at three intervals: (1) daily, at the end of each day, (2) weekly, on Friday nights, and (3) monthly, on the last business day of the month. Nightly backup tapes were kept for twenty working days, weekly tapes for one year, and monthly tapes for three years. After the relevant time period elapsed, the tapes were recycled.[25]

Once e-mails have been stored onto backup tapes, the restoration process is lengthy. Each backup tape routinely takes approximately five days to

---

[23] See 1/14/03 Deposition of Christopher Behny ("Behny Dep."), Ex. M to the Leblang Dec. Unless otherwise noted, all information about UBS's e-mail systems is culled from the Behny Dep. Because that document has been sealed, repeated pin cites are unnecessary and thus omitted.

[24] See generally VERITAS NetBackup Release 4.5 Technical Overview, available at http://www.veritas.com.

[25] Of course, periodic backups such as UBS's necessarily entails the loss of certain e-mails. Because backups were conducted only intermittently, some e-mails that were deleted from the server were never backed up. For example, if a user both received and deleted an e-mail on the same day, it would not reside on any backup tape. Similarly, an e-mail received and deleted within the span of one month would not exist on the monthly backup, although it might exist on a weekly or daily backup, if those tapes still exist. As explained below, if an e-mail was to or from a "registered trader," however, it may have been stored on UBS's optical storage devices.

restore, although resort to an outside vendor would speed up the process (at greatly enhanced costs, of course). Because each tape represents a snapshot of one server's hard drive in a given month, each server/month must be restored separately onto a hard drive. Then, a program called Double Mail is used to extract a particular individual's e-mail file. That mail file is then exported into a Microsoft Outlook data file, which in turn can be opened in Microsoft Outlook, a common e-mail application. A user could then browse through the mail file and sort the mail by recipient, date or subject, or search for key words in the body of the e-mail.

Fortunately, NetBackup also created indexes of each backup tape. Thus, Behny was able to search through the tapes from the relevant time period and determine that the e-mail files responsive to Zubulake's requests are contained on a total of ninety-four backup tapes.

2. Optical Disk Storage

In addition to the e-mail backup tapes, UBS also stored certain e-mails on optical disks. For certain "registered traders," probably including the members of the Desk,[26] a copy of all e-mails sent to or received from outside

[26] In using the phrase "registered trader," Behny referred to individuals designated to have their e-mails archived onto optical disks. Although Behny could not be certain that such a designation corresponds to Series 7 or Series 63 broker-dealers, he indicated that examples of registered traders include "equity research people, [and] equity traders type people." See Behny Dep. at 35. He admitted that members of the Desk were probably "registered" in that sense:

> Q: Do you know whether the Asian Equities Sales desk was registered to keep a secondary copy in 1999?

sources (i.e., e-mails from a "registered trader" at UBS to someone at another entity, or vice versa) was simultaneously written onto a series of optical disks. Internal e-mails, however, were not stored on this system.

UBS has retained each optical disk used since the system was put into place in mid-1998. Moreover, the optical disks are neither erasable nor rewritable. Thus, UBS has every e-mail sent or received by registered traders (except internal e-mails) during the period of Zubulake's employment, even if the e-mail was deleted instantaneously on that trader's system.

The optical disks are easily searchable using a program called Tumbleweed.[27] Using Tumbleweed, a user can simply log into the system with the proper credentials and create a plain language search. Search criteria can include not just "header" information, such as the date or the name of the sender or recipient, but can also include terms within the text of the e-mail itself. For example, UBS personnel could easily run a search for e-mails containing the words "Laura" or "Zubulake" that were sent or received by Chapin, Datta, Clarke, or Hardisty.[28]

A: I can't say conclusively.

Q: Do you have an opinion?

A: My opinion is yes.

Id. at 36. See also id. (admitting that the same was probably true in 2000 and 2001).

[27] See generally http://www.tumbleweed.com/en/products/solutions/archive.html.

[28] Rose Tong, the fifth person designated by Zubulake's document request, would probably not have been a "registered trader" as she was a human resources employee.

III. LEGAL STANDARD

Federal Rules of Civil Procedure 26 through 37 govern discovery in all civil actions. As the Supreme Court long ago explained,

> The pre-trial deposition-discovery mechanism established by Rules 26 to 37 is one of the most significant innovations of the Federal Rules of Civil Procedure. Under the prior federal practice, the pre-trial functions of notice-giving issue-formulation and fact-revelation were performed primarily and inadequately by the pleadings. Inquiry into the issues and the facts before trial was narrowly confined and was often cumbersome in method. The new rules, however, restrict the pleadings to the task of general notice-giving and invest the deposition-discovery process with a vital role in the preparation for trial. The various instruments of discovery now serve (1) as a device, along with the pre-trial hearing under Rule 16, to narrow and clarify the basic issues between the parties, and (2) as a device for ascertaining the facts, or information as to the existence or whereabouts of facts, relative to those issues. Thus civil trials in the federal courts no longer need to be carried on in the dark. The way is now clear, consistent with recognized privileges, for the parties to obtain the fullest possible knowledge of the issues and facts before trial.[29]

Consistent with this approach, Rule 26(b)(1) specifies that,

> Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having

[29] Hickman, 329 U.S. at 500-01 (emphasis added).

> knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(i), (ii), and (iii).[30]

In turn, Rule 26(b)(2) imposes general limitations on the scope of discovery in the form of a "proportionality test":

> The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.[31]

Finally, "[u]nder [the discovery] rules, the presumption is that the responding party must bear the expense of complying with discovery requests, but [it] may invoke the district court's discretion under Rule 26(c) to grant orders protecting

---

[30] Fed. R. Civ. P. 26(b)(1) (emphasis added).

[31] Fed. R. Civ. P. 26 (b) (2) .

[it] from 'undue burden or expense' in doing so, including orders conditioning discovery on the requesting party's payment of the costs of discovery.[32]

The application of these various discovery rules is particularly complicated where electronic data is sought because otherwise discoverable evidence is often only available from expensive-to-restore backup media. That being so, courts have devised creative solutions for balancing the broad scope of discovery prescribed in Rule 26(b)(1) with the cost-consciousness of Rule 26(b)(2). By and large, the solution has been to consider cost-shifting: forcing the requesting party, rather than the answering party, to bear the cost of discovery.

By far, the most influential response to the problem of cost-shifting relating to the discovery of electronic data was given by United States Magistrate Judge James C. Francis IV of this district in Rowe Entertainment. Judge Francis utilized an eight-factor test to determine whether discovery costs should be shifted. Those eight factors are:

> (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefits to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its

[32] Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).

> incentive to do so; and (8) the resources available to each party.[33]

Both Zubulake and UBS agree that the eight-factor Rowe test should be used to determine whether cost-shifting is appropriate.[34]

IV. DISCUSSION

A. Should Discovery of UBS's Electronic Data Be Permitted?

Under Rule 34, a party may request discovery of document, "including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations …"[35] The "inclusive description" of the term document "accord[s] with changing technology."[36] "It makes clear that Rule 34 applies to electronics [sic] data compilations." Thus, "[e]lectronic documents are not less subject to disclosure than paper records."[37] This is true not only of electronic documents that are currently in use, but also of documents that may have been deleted and now reside only on backup disks.[38]

---

[33] 205 F.R.D. at 429.

[34] Zubulake mistakenly identifies the Rowe test as a "marginal utility" test. In fact, "marginal utility" -- a common term among economists, see Istvan Meszaros, Beyond Capital § 3.2 (1995) (describing the intellectual history of marginal utility) -- refers only to the second Rowe factor, the likelihood of discovering critical information. See Rowe, 205 F.R.D. at 430 (quoting McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001)).

[35] Fed. R. Civ. P. 34(a).

[36] Advisory Committee Note to Fed. R. Civ. P. 34.

[37] Rowe, 205 F.R.D. at 428 (collecting cases).

[38] See Antioch Co. v. Scapbook 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

That being so, Zubulake is entitled to discovery of the requested e-mails so long as they are relevant to her claims,[39] which they clearly are. As noted, e-mail constituted a substantial means of communication among UBS employees. To that end, UBS has already produced approximately 100 pages of e-mails, the contents of which are unquestionably relevant.[40]

Nonetheless, UBS argues that Zubulake is not entitled to any further discovery because it already produced all responsive documents, to wit, the 100 pages of e-mails. This argument is unpersuasive for two reasons. First, because of the way that UBS backs up its e-mail files, it clearly could not have searched all of its e-mails without restoring the ninety-four backup tapes (which UBS admits that it has not done). UBS therefore cannot represent that it has produced all responsive e-mails. Second, Zubulake herself has produced over 450 pages of relevant e-mails, including e-mails that would have been responsive to her discovery requests but were never produced by UBS. These two facts strongly suggest that there are e-mails that Zubulake has not received that reside on UBS's backup media.[41]

---

discoverable."); Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("First, computer records, including records that have been 'deleted,' are documents discoverable under Fed. R. Civ. P. 34.").

[39] See Fed. R. Civ. P. 26(b)(1).

[40] See, e.g., 8/21/01 e-Mail.

[41] UBS insists that "[f]rom the time Plaintiff commenced her EEOC action in August 2001 … UBS collected and produced all existing responsive e-mails sent or received between 1999 and

B. Should Cost-Shifting Be Considered?

Because it apparently recognizes that Zubulake is entitled to the requested discovery, UBS expends most of its efforts urging the court to shift the cost of production to "protect [it] … from undue burden or expense."[42] Faced with similar applications, courts generally engage in some sort of cost-shifting analysis, whether the refined eight-factor Rowe test or a cruder application of Rule 34's proportionality test, or something in between.[43]

The first question, however, is whether cost-shifting must be considered in every case involving the discovery of electronic data, which -- in today's world -- includes virtually all cases. In light of the accepted principle, stated above, that electronic evidence is no less discoverable than paper evidence, the answer is, "No." The Supreme Court has instructed that "the presumption is that the responding party must bear the expense of complying with discovery requests… ."[44] Any principled approach to electronic evidence must respect this presumption.

2001 from these and other employees' computers." Def. Mem. at Even if this statement is completely accurate, a simple search employees' computer files would not have turned up e-mails deleted prior to August 2001. Such deleted documents exist only on the backup tapes and optical disks, and their precisely why UBS's production is not complete.

[42] Def. Mem. at 9 (quoting Fed. R. Civ. P. 26(c)).

[43] See, e.g., Byers v. Illinois State Police, No. 99 C. 8105, 2002 WL 1264004 (N.D. Ill. June 3, 2002); In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437, 443 (D.N.J. 2002); 205 F.R.D. 421; McPeek, 202 F.R.D. 31.

[44] Oppenheimer Fund, 437 U.S. at 358.

Courts must remember that cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As large companies increasingly move to entirely paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases. This will both undermine the "strong public policy favor[ing] resolving disputes on their merits,"[45] and may ultimately deter the filing of potentially meritorious claims.

Thus, cost-shifting should be considered only when electronic discovery imposes an "undue burden or expense" on the responding party.[46] The burden or expense of discovery is, in turn, "undue" when it "outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues."[47]

Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved.[48] This makes

---

[45] Pecarsky v. Galaxiworld.com. Inc., 249 F.3d 167, 172 (2d Cir. 2001).

[46] Fed. R. Civ. P. 26 (c).

[47] Fed. R. Civ. P. 26 (b) (2) (iii). As noted, a court is also permitted to impose conditions on discovery when it might be duplicative, see Fed. R. Civ. P. 26(b)(2)(i), or when a reasonable discovery deadline has lapsed, see id. 26(b)(2)(ii). Neither of these concerns, however, is likely to arise solely because the discovery sought is of electronic data.

[48] See e.g., Murphy Oil USA, Inc. v. Fluor Daniel., Inc., No. Civ.A. 99-3564, 2002 WL 246439, at *3 (E.D. La. Feb. 19, 2002) (suggesting that application of Rowe is appropriate whenever "a

no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it 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.[49]

In fact, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production). In the world of paper documents, for example, a document is accessible if it is readily available in a usable format and reasonably indexed. Examples of inaccessible paper documents could include (a) documents in storage in a difficult to reach place; (b) documents converted to microfiche and not easily readable; or (c) documents kept haphazardly, with no indexing system, in quantities that make page-by-page searches impracticable. But in the world of electronic data, thanks to search engines, any data that is retained in a machine readable format is typically accessible.[50]

---

party, as does Flour [sic], contends that the burden or expense of the discovery outweighs the benefit of the discovery").

[49] See generally Scheindlin & Rabkin, Electronic Discovery, 41 B.C. L. Rev. at 335-341 (describing types of discoverable electronic data and their differences from paper evidence).

[50] See Scheindlin & Rabkin, Electronic Discovery, 41 B.C. L. Rev. at 364 ("By comparison [to the time it would take to search through 100,000 pages of paper], the average office computer could search all of the documents for specific words or combination[s] of words in minute, perhaps less."); see also Public Citizen v. Carlin, 184 F.3d 900, 908-10 (D.C. Cir. 1999).

Whether electronic data is accessible or inaccessible turns largely on the media on which it is stored. Five categories of data, listed in order from most accessible to least accessible, are described in the literature on electronic data storage:

1. Active, online data: "On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life -- when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds."[51] Examples of online data include hard drives.

2. Near-line data: "This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape."[52] Examples include optical disks.

3. Offline storage/archives: "This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-

[51] Cohasset Associates, Inc., White Paper: Trustworthy Storage and Management of Electronic Records: The Role of Optical Storage Technology 10 (April 2003) ("White Paper").

[52] Id. at 11.

effectiveness of the storage facility."[53] The principled difference between nearline data and offline data is that offline data lacks "the coordinated control of an intelligent disk subsystem," and is, in the lingo, JBOD ("Just a Bunch Of Disks").[54]

4. Backup tapes: "A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably … The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks."[55] As a result, "[t]he data on a backup tape are not organized for retrieval of individual documents or files [because] … the organization of the data mirrors the computer's structure, not the human records management structure.[56] Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.[57]

5. Erased, fragmented or damaged data: "When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters … . As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and

---

[53] Id.

[54] CNT, The Future of Tape 2, available at http://www.cnt.com/literature/documents/pl556.pdf.

[55] Webopedia, at http://inews.webopedia.com/TERM/t/tape drive.html.

[56] Kenneth J. Withers, Computer-Based Discovery in Federal Civil Litigation (unpublished manuscript) at 15.

[57] See generally SDLT, Inc., Making a Business Case for Tape, at http://quantum.treehousei.com/Surveys/publishing/survey_148/pdfs/ making- a-business _case for_tape.pdf (June 2002); Jerry Stern, The Perils of Backing Up, at http://www.grsoftware.net/backup/articles/jerry_perils.html (last visited May 5, 2003).

> randomly placed throughout the disk."[58] Such broken--up files are said to be "fragmented," and along with damaged and erased data can only be accessed after significant processing.[59]

Of these, the first three categories are typically identified as accessible, and the latter two as inaccessible.[60] The difference between the two classes is easy to appreciate. Information deemed "accessible" is stored in a readily usable format. Although the time it takes to actually access the data ranges from milliseconds to days, the data does not need to be restored or otherwise manipulated to be usable. "Inaccessible" data, on the other hand, is not readily usable. Backup tapes must be restored using a process similar to that previously described, fragmented data must be de-fragmented, and erased data must be reconstructed, all before the data is usable. That makes such data inaccessible.[61]

---

[58] Sunbelt Software, Inc., White Paper: Disk Defragmentation for Windows NT/2000: Hidden Gold for the Enterprise 2, at http://www.sunbelt-software.com/evaluation/455/web/documents/idc-white-paper-english.pdf (last visited May 5, 2003).

[59] See Executive Software, Inc., Identifying Common Reliability/Stability Problems Caused by File Fragmentation, at http://www.execsoft.com/Reliability_Stability_Whitepaper.pdf (last visited May 1, 2003) (identifying problems associated with file fragmentation, including file corruption, data loss, crashes, and hard drive failures); Stan Miastkowski, When Good Data Goes Bad, PC World, Jan. 2000, available at http://www.pcworld.com/resource/printable/article/0,aid,13859,00.asp.

[60] See generally White Paper 10-13.

[61] A report prepared by the Sedona Conference recently propounded "Best Practices" for electronic discovery. See The Sedona Conference, The Sedona Principles: Best Practices Recommendations & Principles for Address in Electronic Document Production (March 2003), ("Sedona Principles"), available at http://www.thesedonaconference.org/publications html. Although I do not endorse or indeed agree with all of the Sedona Principles, they do recognize the difference between "active data" and data stored on backup tapes or "deleted, shadowed, fragmented or residual data," see id. (Principles 8 and 9), a distinction very similar to the accessible/inaccessible test employed here.

The case at bar is a perfect illustration of the range of accessibility of electronic data. As explained above, UBS maintains e-mail files in three forms: (1) active user e-mail files; (2) archived e-mails on optical disks; and (3) backup stored on tapes. The active (HP OpenMail) data is obviously most accessible: it is online data that resides on an active server, and can be accessed immediately. The optical disk (Tumbleweed) data is only slightly less accessible, and falls into either the second or third category. The e-mails are on optical disks that need to be located and read with the correct hardware, but the system is configured to make searching the optical disks simple and automated once they are located. For these sources of e-mails -- active mail files and e-mails stored on optical disks -- it would be wholly inappropriate to even consider cost-shifting. UBS maintains the data in an accessible and usable format, and can respond to Zubulake's request cheaply and quickly. Like most typical discovery requests, therefore, the producing party should bear the cost of production.

E-mails stored on backup tapes (via NetBackup), however, are an entirely different matter. Although UBS has already identified the ninety-four potentially responsive backup tapes, those tapes are not currently accessible. In order to search the tapes for responsive e-mails, UBS would have to engage in the costly and time-consuming process detailed above. It is therefore appropriate to consider cost shifting.

C. What Is the Proper Cost-Shifting Analysis?

In the year since Rowe was decided, its eight factor test has unquestionably become the gold standard for courts resolving electronic discovery disputes.[62] But there is little doubt that the Rowe factors will generally favor cost-shifting. Indeed, of the handful of reported opinions that apply Rowe or some modification thereof, all of them have ordered the cost of discovery to be shifted to the requesting party.[63]

In order to maintain the presumption that the responding party pays, the cost-shifting analysis must be neutral; close calls should be resolved in favor of the presumption. The Rowe factors, as applied, undercut that presumption for three reasons. First, the Rowe test is incomplete. Second, courts have given equal weight to all of the factors, when certain factors should predominate. Third, courts applying the Rowe test have not always developed a full factual record.

---

[62] See In re Livent Inc. Noteholders Sec. Litig., No. 98 Civ. 7161, 2003 WL 23254, at *3 (S.D.N.Y. Jan. 2, 2003) ("the attorneys should read Magistrate Judge Francis's opinion in [Rowe]. Then Deloitte and plaintiffs should confer, in person or by telephone, and discuss the eight factors listed in that opinion."); Bristol-Myers Squibb, 205 F.R.D. at 443 ("For a more comprehensive analysis of cost allocation and cost shifting regarding production of electronic information in a different factual context, counsel are directed to the recent opinion in [Rowe].")

[63] See Murphy Oil, 2002 WL 246439; Bristol-Myers Squibb, 205 F.R.D. 437; Byers, 2002 WL 1264004.

1. The Rowe Test Is Incomplete

a. A Modification of Rowe: Additional Factors

Certain factors specifically identified in the Rules are omitted from Rowe's eight factors. In particular, Rule 26 requires consideration of "the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues."[64] Yet Rowe makes no mention of either the amount in controversy or the importance of the issues at stake in the litigation. These factors should be added. Doing so would balance the Rowe factor that typically weighs most heavily in favor of cost-shifting, "the total cost associated with production." The cost of production is almost always an objectively large number in cases where litigating cost-shifting is worthwhile. But the cost of production when compared to "the amount in controversy" may tell a different story. A response to a discovery request costing $100,000 sounds (and is) costly, but in a case potentially worth millions of dollars, the cost of responding may not be unduly burdensome.[65]

Rowe also contemplates "the resources available to each party." But here too -- although this consideration may be implicit in the Rowe test -- the absolute wealth of the parties is not the relevant factor. More important than

---

[64] Fed. R. Civ. P. 26(b)(2)(iii).

[65] A word of caution, however: in evaluating this factor courts must look beyond the (often inflated) value stated in the ad damnum clause of the complaint.

comparing the relative ability of a party to pay for discovery, the focus should be on the total cost of production as compared to the resources available to each party. Thus, discovery that would be too expensive for one defendant to bear would be a drop in the bucket for another.[66]

Last, "the importance of the issues at stake in the litigation" is a critical consideration, even if it is one that will rarely be invoked. For example, if a case has the potential for broad public impact, then public policy weighs heavily in favor of permitting extensive discovery. Cases of this ilk might include toxic tort class actions, environmental actions, so-called "impact" or social reform litigation, cases involving criminal conduct, or cases implicating important legal or constitutional questions.

b. A Modification of Rowe: Eliminating Two Factors

Two of the Rowe factors should be eliminated:

First, the Rowe test includes "the specificity of the discovery request." Specificity is surely the touchstone of any good discovery request,[67] requiring a party to frame a request broadly enough to obtain relevant evidence, yet narrowly enough to control costs. But relevance and cost are already two of

[66] UBS, for example, reported net profits after tax of 942 million Swiss Francs (approximately $716 million) for the third quarter of 2002 alone. See 11/12/02 UBS Press Release, available at http://www.ubswarburg.com/e/port genint/index-genint.html.

[67] See Sedona Principles (Principle 4: "Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.").

the Rowe factors (the second and sixth). Because the first and second factors are duplicative, they can be combined. Thus, the first factor should be: the extent to which the request is specifically tailored to discover relevant information.

Second, the fourth factor, "the purposes for which the responding party maintains the requested data" is typically unimportant. Whether the data is kept for a business purpose or for disaster recovery does not affect its accessibility, which is the practical basis for calculating the cost of production.[68] Although a business purpose will often coincide with accessibility -- data that is inaccessible is unlikely to be used or needed in the ordinary course of business -- the concepts are not coterminous. In particular, a good deal of accessible data may be retained, though not in the ordinary course of business. For example, data that should rightly have been erased pursuant to a document retention/destruction

---

[68] Indeed, although Judge Francis weighed the purpose for which data is retained, his analysis also focused on accessibility:

> If a party maintains electronic data for the purpose of utilizing it in connection with current activities, it may be expected to respond to discovery requests at its own expense… Conversely, however, a party that happens to retain vestigal data for no current business purpose, but only in case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it.

205 F.R.D. at 431 (emphasis added). It is certainly true that data kept solely for disaster recovery is often relatively inaccessible because it is stored on backup tapes. But it is important not to conflate the purpose of retention with accessibility. A good deal of accessible, easily produced material may be kept for no apparent business purpose. Such evidence is no less discoverable than paper documents that serve no current purpose and exist only because a party failed to discard them. See, e.g., Fidelity Nat. Title Ins. Co. of. New York v. Intercounty Nat. Title Ins. Co., No. 00 C. 5658, 2002 WL 1433584, at *6 (N.D. Ill. July 2, 2002) (requiring production of documents kept for no purpose, maintained "chaotic[ally]" and "cluttered in unorganized stacks" in an off-site warehouse); Dangler v. New York Cit Off Track Betting Corp., No. 95 Civ. 8495, 2000 WL 1510090, at *1 (S.D.N.Y. Oct. 11, 2000) (requiring production of documents kept "disorganized" in "dozens of boxes").

policy may be inadvertently retained. If so, the fact that it should have been erased in no way shields that data from discovery. As long as the data is accessible, it must be produced.

Of course, there will be certain limited instances where the very purpose of maintaining the data will be to produce it to the opposing party. That would be the case, for example, where the SEC requested "communications sent by [a] broker or dealer (including inter-office memoranda and communications) relating to his business as such." Such communications must be maintained pursuant to SEC Rule 17a-4.[69] But in such cases, cost-shifting would not be applicable in the first place; the relevant statute or rule would dictate the extent of discovery and the associated costs.[70] Cost-shifting would also be inappropriate for another reason -- namely, that the regulation itself requires that the data be kept "in an accessible place."

c. A New Seven-Factor Test

Set forth below is a new seven-factor test based on the modifications to Rowe discussed in the preceding sections.

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

---

[69] See supra, note 20.

[70] However, while Zubulake is not the stated beneficiary of SEC Rule 17a-4, see Touche Ross & Co. v. Redinaton, 442 U.S. 560, 569-70 (1979), to the extent that the e-mails are accessible because of it, it inures to her benefit.

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 of 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.

2. The Seven Factors Should Not Be Weighted Equally

Whenever a court applies a multi-factor test, there is a temptation to treat the factors as a check-list, resolving the issue in favor of whichever column has the most checks.[71] But "we do not just add up the factors."[72] When evaluating cost-shifting, the central question must be, does the request impose an "undue burden or expense" on the responding party?[73] Put another way, "how important is the sought-after evidence in comparison to the cost of production?" The seven-factor test articulated above provide some guidance in answering this

[71] See, e.g., Big O Tires, Inc. v. Bigfoot 4X4, Inc., 167 F. Supp. 2d 1216, 1227 (D. Colo. 2001) ("A majority of factors in the likelihood of confusion test weigh in favor of Big O. I therefore conclude that Big O has shown a likelihood of success on the merits.").

[72] Noble v. United States, 231 F.3d 352, 359 (7th Cir. 2000).

[73] Fed. R. Civ. P. 26 (b)(iii).

question, but the test cannot be mechanically applied at the risk of losing sight of its purpose.

Weighting the factors in descending order of importance may solve the problem and avoid a mechanistic application of the test. The first two factors -- comprising the marginal utility test -- are the most important. These factors include: (1) The extent to which the request is specifically tailored to discover relevant information and (2) the availability of such information from other sources. The substance of the marginal utility test was well described in McPeek v. Ashcroft:

> The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the [responding party] search at its own expense. The less likely it is, the more unjust it would be to make the [responding party] search at its own expense. The difference is "at the margin."[74]

The second group of factors addresses cost issues: "How expensive will this production be?" and, "Who can handle that expense?" These factors include: (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 and (5) the relative ability of each party to control costs and its incentive to do so. The third "group" -- (6) the importance of the litigation itself -- stands alone, and as noted earlier will only rarely come into play. But where it does, this factor has

[74] 202 F.R.D. at 34.

the potential to predominate over the others. Collectively, the first three groups correspond to the three explicit considerations of Rule 26(b)(2)(iii). Finally, the last factor -- (7) the relative benefits of production as between the requesting and producing parties -- is the least important because it is fair to presume that the response to a discovery request generally benefits the requesting party. But in the unusual case where production will also provide a tangible or strategic benefit to the responding party, that fact may weigh against shifting costs.

D. A Factual Basis Is Required to Support the Analysis

Courts applying Rowe have uniformly favored cost-shifting largely because of assumptions made concerning the likelihood that relevant information will be found. This is illustrated in Rowe itself:

> Here, there is a high enough probability that a broad search of the defendants' e-mails will elicit some relevant information that the search should not be precluded altogether. However, there has certainly been no showing that the e-mails are likely to be a gold mine. No witness has testified, for example, about any e-mail communications that allegedly reflect discriminatory or anti-competitive practices. Thus, the marginal value of searching the e-mails is modest at best, and this factor, too, militates in favor of imposing the costs of discovery on the plaintiffs.[75]

[75] 205 F.R.D. at 430. See also Murphy Oil, 2002 WL 246439, at *5 (determining that "the marginal value of searching the e-mail is modest at best" and weighs in favor of cost-shifting because "Murphy has not pointed to any evidence that shows that 'the e-mails are likely to be a gold mine'").

But such proof will rarely exist in advance of obtaining the requested discovery. The suggestion that a plaintiff must not only demonstrate that probative evidence exists, but also prove that electronic discovery will yield a "gold mine," is contrary to the plain language of Rule 26(b)(1), which permits discovery of "any matter" that is "relevant to [a] claim or defense."

The best solution to this problem is found in McPeek:

> Given the complicated questions presented [and] the clash of policies … I have decided to take small steps and perform, as it were, a test run. Accordingly, I will order DOJ to perform a backup restoration of the e-mails attributable to Diegelman's computer during the period of July 1, 1998 to July 1, 1999. … The DOJ will have to carefully document the time and money spent in doing the search. It will then have to search in the restored e-mails for any document responsive to any of the plaintiff's requests for production of documents. Upon the completion of this search, the DOJ will then file a comprehensive, sworn certification of the time and money spent and the results of the search. Once it does, I will permit the parties an opportunity to argue why the results and the expense do or do not justify any further search.[76]

Requiring the responding party to restore and produce responsive documents from a small sample of backup tapes will inform the cost-shifting analysis laid out above. When based on an actual sample, the marginal utility test will not be an exercise in speculation -- there will be tangible evidence of what the backup tapes may have to offer. There will also be tangible evidence of the time and cost

[76] 202 F.R.D. at 34-35.

required to restore the backup tapes, which in turn will inform the second group of cost-shifting factors. Thus, by requiring a sample restoration of backup tapes, the entire cost-shifting analysis can be grounded in fact rather than guesswork.[77]

V. CONCLUSION AND ORDER

In summary, deciding disputes regarding the scope and cost of discovery of electronic data requires a three-step analysis:

First, it is necessary to thoroughly understand the responding party's computer system, both with respect to active and stored data. For data that is kept in an accessible format, the usual rules of discovery apply: the responding party should pay the costs of producing responsive data. A court should consider cost-shifting only when electronic data is relatively inaccessible, such as in backup tapes.

Second, because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases.

[77] Of course, where the cost of a sample restoration significant compared to the value of the suit, or where the itself is patently frivolous, even this minor effort may be inappropriate.

Third, and finally, in conducting the cost-shifting analysis, the following factors should be considered, weighted more-or-less 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 of 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.

Accordingly, UBS is ordered to produce all responsive e-mails that exist on its optical disks or on its active servers (i.e., in HP OpenMail files) at its own expense. UBS is also ordered to produce, at its expense, responsive e-mails from any five backups tapes selected by Zubulake. UBS should then prepare an affidavit detailing the results of its search, as well as the time and money spent. After reviewing the contents of the backup tapes and UBS's certification, the Court will conduct the appropriate cost-shifting analysis.

A conference is scheduled in Courtroom 12C at 4:30 p.m. on June 17, 2003.

SO ORDERED:

Shira A. Scheindlin
U.S.D.J.

Dated: New York, New York
May 13, 2003

- Appearances -

For Plaintiff:

James A. Batson, Esq.
Christina J. Kang, Esq.
Liddle & Robinson, LLP
685 Third Avenue
New York, New York 10017
(212) 687-8500

For Defendants:

Kevin B. Leblang, Esq.
Norman C. Simon, Esq.
Kramer Levin Naftalis & Frankel LLP
919 Third Avenue
New York, New York 10022
(212) 715-9100

Electronic Records: What to Look/Ask For

By Lori J. Marco and Katie M. Connolly[78]

"Computerized data have become commonplace in litigation."[79] Through minor amendment and judicial interpretation, the rules by which we conduct litigation have come to acknowledge and accept this fact. In 1970, Federal Rule of Civil Procedure 34 was amended to provide for discovery of "data compilations from which information can be obtained…."[80] In 1993, the addition of the initial disclosure requirement to Federal Rule of Civil Procedure 26 specifically included "data compilations" within its purview of discoverable documents.[81] Federal Rule of Evidence Rule 803(6) follows suit and includes in its definition of business records "a . . . data compilation, in any form . . . ."[82]

It is clear, then, that clients' computerized data will be subject to discovery. This is often true even if hard copies of documents have been produced.[83] At the outset of litigation, it is imperative to make clear to all

---

[78] Lori J. Marco is an associate with Briggs and Morgan in Minneapolis, MN. Katie M. Connolly is a student at the University of Minnesota Law School serving as a summer law clerk for Briggs and Morgan.

[79] MANUEL FOR COMPLEX LITIGATION (THIRD) § 21.446 (1995).

[80] FED. R. CIV. P. 34.

[81] FED. R. CIV. P. 26(a)(1)(B).

[82] FED. R. EVID. 803(6).

[83] *See, e.g.*, Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, 1 (S.D.N.Y. Nov. 3, 1996) (stating that, "the law is clear that data in computerized form is discoverable even if paper 'hard

involved that the duty to preserve evidence extends to data compilations, computerized data and other electronically recorded information.[84] Whether intentional or inadvertent, failure to preserve email and electronic documents is sanctionable as spoliation of evidence.[85]

---

copies' of the information have been produced…"); Linnen v. A.H. Robins Co., 1999 WL 462015, 10 (Mass. Super. June 16, 1999) (holding that because the plaintiff had specifically requested electronic data along with hard copy documents, the defendant had a duty to produce responsive data); Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1382-83 (7th Cir. 1993) (holding that sanctions were appropriate because the sanctioned party had failed to fully respond to a discovery request, including failure to supply "raw data" responsive to the discovery request). *See also* Zubulake v. UBS Warburg, 02 Civ. 1243 (SAS) (S.D. N.Y. May 13, 2003) (noting that despite the defendant's offering of 100 pages of hard copy emails, further electronic production was required.)

[84] *See* Kleiner v. Burns, 2000 WL 1909470, 3-4 (D. Kan. Dec. 15 2000) (requiring the defendant to turn over all responsive electronic data to the plaintiff pursuant to the discovery request); Danis v. USN Communications, 2000 WL 1694325, 12-19 (N.D. Ill. Oct. 23, 2000) (discussing the culpability of managers in failing to adequately preserve electronic data for purposes of document retrieval).

[85] *See generally*, Metropolitan Opera Assoc., Inc. v. Local 100, 2003 WL 186645 (S.D.N.Y. Jan. 28, 2003) (sanctions awarded where the defendant and defense attorneys failed to take adequate steps to preserve and produce responsive electronic data); Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. Sept. 26, 2002) (discussing the similarities between withholding electronic back-up tapes and typical spoliation of evidence cases and the evidence required to show the withholding party should be sanctioned); Gates Rubber Co. v. Bando Chem. Inc., 167 F.R.D. 90 (D. Colo. 1996) (describing in detail the elements required to prove spoliation, including mental state and the degree of prejudice caused by the destruction of the evidence); William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984) (describing repeated destruction of requested electronic materials and violations of court orders and applying the prejudice to requesting party and "bad faith" tests similar to those implemented by the court in *Gates*). Jacob Hart and Anna Marie Plum provide the following list of electronic information that should be attended to in their "spoliation checklist." They suggest identification and preservation of:

- word processing documents, including drafts;
- databases and spreadsheets;
- email, voicemail and other electronically-maintained communications;
- system records, such as logs, Internet use history files, and access records;
- active files on network servers;
- computer files on desktops and local hard drives;
- laptops, home computers and other satellite devices; and

Once a case has been filed and counsel has taken steps to ensure preservation of the client's relevant electronic data, the next step is offensive discovery. We know, or at least suspect, that a wealth of information—and the fabled smoking gun—is located in our opponent's electronic files ripe for the picking. (*See* Zubulake, supra note 5. How do we access this information? Where do we look? What do we ask for?

A. Step One: Discovery Planning[86]

Electronic discovery poses unique problems that attorneys often did not face in conventional discovery. Most of an organization's paper files will be centrally located or reside in a limited number of locations. Electronic files can be located virtually anywhere. In today's mobile, PC-based work force, an organization's electronic files may be found on employees' desktop computers, storage disks or tapes, laptops, personal organizers, and even employee's home computers.[87] Large organizations may also have network servers that store data for multiple PCs as well as archival and back up data. Even third parties, such as

---

• media or hardware that may contain recoverable information.
Jacob P. Hart & Anna Marie Plum, *Litigating the Production of Electronic Media: "Disk-covery" Issues for the 21st Century*, SG007 ALI-ABA 169, 186-87 (2001).

[86] *See generally*, Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 FED. CTS. L. REV. 2 (2000) (appendix to this article is particularly helpful as a checklist when planning for discovery).

[87] *Id*. § II. B. 1.

internet service providers and offsite storage facilities, may possess discoverable data.

As early as possible in the litigation, counsel for both sides should meet to discuss electronic discovery.[88] Counsel should identify the categories of electronic information that they intend to seek.[89] They should try to agree on the steps each will take to locate, segregate and preserve electronic data. They should also discuss: (1) the form of production, whether hard copy or electronic;[90] (2) whether on-site inspection will be necessary; (3) search protocols; (4) identification and protection of privileged information; and (5) whether it will be necessary to appoint a neutral expert to review electronic information. Any agreement reached can be discussed at the pretrial conference and memorialized in a pretrial order.[91]

---

[88] Withers suggests that electronic discovery is likely to play a significant role in discovery when:
- the substantive allegations involve electronic records;
- authenticity or completeness of electronic records may be contested;
- substantial disclosure will involve electronic records;
- when one or more parties routinely uses electronic records;
- when one or more parties has converted substantial records to electronic form;
- when experts will base testimony on electronic data or computer modeling; or
- when an anticipated large volume of documents is involved.

Id. at app. I. *See also Id*. § III. I. 2.

[89] *Id*. at app. II.

[90] When the agreed-upon form of production is electronic, courts have required discovery targets to provide the discovering party with the hardware or software necessary to read electronically-produced material. *See, e.g.* Saltar v. Motorola, 138 F.3d 1164, 1171 (7th Cir. 1998).

[91] FED. R. CIV. P. 16(c) and 16(c)(6). For discussions of the special problems faced when conducting electronic discovery and suggestions for solving them, *see generally* Richard L.

Depending on the degree to which counsel are able to reach an agreement, counsel may wish to use formal methods to obtain information about an opponents' use of electronic media and data storage procedures. Initial interrogatories may ask the opponent to identify: (1) the types of software used; (2) the types of hardware used, including desktops, personal organizers, handheld devices, laptop computers, and cell phones; (3) all users who potentially have generated relevant electronic files; (4) locations of all devices, including backup storage media; (5) the opponent's computer network, including the type of network operating system, the names of all users of the system, and the names of those responsible for operation and maintenance of the system; (6) data back-up protocols, storage form, and location of stored information; (7) hardware that has been erased or reformatted such that information has been lost; (8) data retention policies; (9) file naming conventions; and (10) corporate computer policies.[92]

Alternatively, this information may be obtained by conducting a deposition of the corporation.[93] The deposition notice should seek testimony from someone with knowledge of the opponent's computer systems and practices.[94]

Marcus, *Confronting the Future: Coping with Discovery of Electronic Material*, 64 LAW & CONTEMP. PROBS. 253 (2001); Hart & Plum, *supra* note 85.

[92] Kroll Ontrack provides a comprehensive set of Sample Interrogatories for use in the federal district courts. *See* Kroll OnTrack, *Sample Interrogatories*, *available at* http://www.krollontrack.com/practicaltools/interrogatory_mailer.pdf, (last visited May 22, 2003). *See generally*, Hart & Plum, *supra,* note 7; Withers, *supra*, note 8.

[93] FED. R. CIV. P. 30(b)(6).

B. Step Two: What to Look For

Now that you know how your opponent stores data and where it is located, what do you ask for? The depth and comprehensiveness of your search depends primarily on case-specific factors such as the claims themselves, as well as the budget and the size and sophistication of the opponent's electronic systems. You will want to consider requesting the following categories of information.

1. Email

Email correspondence is now pervasive in our professional and personal lives. The volume of email correspondence that passes through an organization each day is staggering. Magistrate Judge Jacob P. Hart estimates that the average American worker sends or receives 24 emails a day.[95] For a company with 100 employees, this translates to over a half million emails per year.[96]

---

[94] *See In re* Carbon Dioxide Industry Antitrust Litigation, 155 F.R.D. 209, 214 (M.D. Fla. 1993) (stating, "[n]evertheless, Plaintiffs' 30(b)(6) depositions to identify how data is maintained and to determine what hardware and software is necessary to access the information are preliminary depositions necessary to proceed with merits discovery"). Withers notes that, although Rule 26 would not normally allow formal discovery prior to the Rule 26(f) conference, a party seeking information regarding his opponent's electronic systems may request the judge to specially order such preliminary discovery as is necessary to enable a productive Rule 26(f) conference and Rule 16(c) pretrial conference. Withers, *supra* note 8, §III.A.3. *See also* Anthony Tarricone, *Discovery and Spoliation of Electronic Evidence*, TRIAL, Dec., 1999, at 57.

[95] Hart & Plum, *supra* note 7, at 173. *See also* Zubulake, *supra* note 5, at *3. In the Zubulake case, it was shown that "each salesperson ... received approximately 200 emails each day." *Id.* at 9.

[96] *Id.*

Email often also has the disadvantage of lacking a coherent filing system.[97] Even if an organization's email system provides for file management and retrieval of emails by topic, the system works only as well as the email recipients' discipline in placing their emails into the appropriate files. Finally, relevant email is mixed with irrelevant, privileged and often personal email messages. The language itself is often filled with "slang, jargon, and jokes."[98]

With these negative characteristics and large volume, seeking useful information in an organization's email may be the modern version of the proverbial search for a needle in a haystack. Yet email is a popular discovery target.[99] Why bother? Because another fundamental characteristic of email is its informality. Employees often speak much more frankly in email messages than

[97] Lack of coherent filing is not specific to email recording systems. Organization of electronic data is a significant obstacle for all electronic discovery requests. *See Id.*, at 178-82; Withers, *supra,* note 8, §II. E. 1.

[98] *See* Withers, *supra* note 8, §II.C.1.

[99] *See generally,* Lakewood Eng'g v. Lasko Prod., 2003 WL 1220254 (N.D. Ill. Mar. 14, 2003) (holding that requested emails must be produced per the discovery request); Braxton v. Farmer's Ins. Group, 2002 WL 31132933 (N.D. Ala. Sept. 13, 2002) (stating that emails of parties to the suit must be produced when requested if not unusually burdensome); Collette v. St. Luke's Roosevelt Hosp., 2002 WL 31159103 (S.D.N.Y. Sept. 26, 2002) (email used as evidence in a case of retaliatory discharge); MHC Investment Corp. v. Racom Corp., 209 F.R.D. 431 (S.D. Iowa 2002) (email used as evidence in a frivolous claims case); Caldera, Inc. v. Microsoft Corp., 72 F. Supp. 2d 1295 (D. Utah 1999) (antitrust case for which emails were the foundation of the case); Aviles v. McKenzie, 1992 WL 715248 (N.D. Cal. Mar. 17, 1992) (email used as evidence in an action for wrongful termination and employment discrimination); Tulip Computers Int'l B.V. v. Dell Computer Corp., 2002 WL 818061 (D. Del. Apr. 30, 2002) (ordering production of emails from named persons' files).

they would in formal correspondence or even face-to-face.[100] Walt Disney executive Michael Eisner recently stated, "I have come to believe that if anything will bring about the downfall of a company, or maybe even a country, it is blind copies of e-mails that should never have been sent in the first place."[101] Email quotes from Microsoft executives played a central role in the Microsoft antitrust cases.[102]

When requesting email messages or searching for one's own email messages, counsel should not confine the inquiry to the discovery target's in-box. Saved, deleted, and sent folders are easily accessible and can also contain relevant information.[103]

2. Backup and Archival Files

---

[100] *See* James H.A. Pooley & David M. Shaw, *The Emerging Law of Computer Networks, Finding What's Out There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57, 63 (1995) (stating that the implied privacy of email creates a comfort level for people not present in written documents). *See also* Withers, *supra* note 19 and accompanying text.

[101] John Janes, *Brought Down by the Click of a Mouse*, 20 LEGAL MGMT. 92 (March/April 2001).

[102] The opinions of the district court and the circuit court of appeals contain many quotes from Microsoft executives' emails. *See, e.g.,* United States v. Microsoft Corp., 253 F.3d 34, 73 (C.A.D.C. 2001); 65 F. Supp. 2d 9, 49 (D.D.C. 1999); 1998 WL 614485 (D.D.C. Sept. 14, 1998); 1997 WL 769542 (D.D.C. Dec. 4, 1997); 1997 WL 656528 (D.D.C. Oct. 20, 1997); *see generally*, Caldera, Inc. v. Microsoft Corp., 72 F. Supp.2d 1295 (D. Utah 1999) (finding a series of intra-company emails offered direct evidence of the company's attempts to destroy a competitor). Email has also come to Microsoft's rescue on occasion. See Karen Donovan, *E-Mails Help Microsoft in Connecticut Victory*, NAT'L L.J., AUG. 2, 1999 AT A1 (reporting emails that showed plaintiff deliberately extended litigation against Microsoft to increase discovery costs to encourage a high settlement played a central role in this jury's deliberations).

[103] *See In re* Amsted Indus., 2002 WL 31844956, 2 (N.D. Ill. Dec. 17, 2002) (ordering defendant to search the in-box, saved folders and sent folders of relevant individual's emails).

Data that has been edited, deleted or written over in current forms of documents may be retrieved from backup tapes.[104] Courts routinely order retrieval of data from back-up files.[105]

Prudent data management practices dictate that computer users periodically back up their data onto disks or tapes in case their systems crash and data must be restored. Many companies create daily or weekly backups to store everything on their systems and then store the files offsite.[106] Small businesses and individuals can back up their computer files by sending them over the Internet to a third party's computer. Several internet companies even offer computer users free storage space on their web sites.[107]

---

[104] Withers, supra note 8, §II C-D. Additionally, many programs feature automatic backup systems that save temporary backup files of the active documents while it is in use. These are known as "replicant data," "temporary files" or "file clones" and are intended to allow recovery of data lost due to power outage or program lock-ups. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation*: Is *Rule 34 Up to the Task?* 41 BOSTON COL. L.R. 327, 337 (2000).

[105] *See* Hart & Plum, *supra* note 7, at 174; *see also, e.g., In re* Amsted Indus., 2002 WL 31844956 (N.D. Ill. Dec. 17, 2002) (requiring defendants to search backup tapes a second time); McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) (ordering defendant to restore and produce responsive emails over a one year period as a sample to determine if a broader recovery and search was warranted); Kleiner v. Burns, 2000 WL 1909470, 4 (D. Kan. Dec. 15, 2000) (holding that "[t]he disclosing party shall take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data"); Zubulake, *supra* note 5, at 9-11 (detailing the methods by which the defendant employer backed-up the email system, and the court's order to produce all responsive data at the expense of the defendant).

[106] Withers, *supra* note 8, at §II.E. 1-2; Gregory Johnson, *A Paractitioner's Overview of Digital Discovery*, 33 GONZ. L. REV. 347, 364 (1997-1998) (describing the nature of "digital discovery" in detail).

[107] Scheindlin & Rabkin, *supra* note 26 at 337.

Whereas archival files should be more formally organized for identification and retrieval of specific documents, many organizations, instead, keep unorganized raw backup tapes and do not create organized archival files.[108] Standard backup media do not organize data for retrieval. The purpose of backups is complete, emergency uploading of saved data when the existing version has been lost or damaged.[109] The organization of the backup information, therefore, mirrors the computer's data storage structure and will not reflect organized record management practices.[110] Furthermore, old backup tapes may be impossible to read using current software and hardware; special programs may be needed to recover target information; and the process may be expensive and time-consuming.[111]

3. Metadata

As Professor Richard L. Marcus stated, "[h]ard copy discovery usually discloses only that which the inventor decided to put on the page.[112] Even if one obtains prior drafts and notations, it is often impossible to track changes or even place them into chronological order.

---

[108] *See Withers, supra*, note 8, at §II.F.1.

[109] *Id.,* at II.E.1.

[110] *Id.*

[111] *See* Saltar, 138 F.3d at 1171, *supra* note 11 and accompanying text.

[112] Marcus, *supra* note 13, at 263.

Electronically stored data, on the other hand, often includes this type of information. Word processing programs store embedded data or "metadata" along with the document file itself. This data presents information regarding when and by whom a document was created, modified and accessed.[113] Such information may allow reconstruction of each change to a document to determine whether a document had been altered or falsified.[114] It can be extremely valuable. In a murder case, computer forensic evidence was able to reveal that a computer-printed suicide note offered by the defense had been created several months after the murder.[115]

4. Network System Logs, Access Monitoring and Access Control Information

Networked systems often require users to log on to the system by entering a password unique to the individual user. The server typically records when and by whom the system was accessed.[116] More sophisticated systems will also track

---

[113] Scheindlin & Rabkin, *supra*, note 26, at 337. *See* Jones v. Goord, 2002 WL 1007614, 7 (S.D. N.Y. May 16, 2002) (noting production of the electronic form of materials also reveals information about the manner in which the data is managed and organized).

[114] *See* Marcus, *supra*, note 13, at 263-74. Even the "undo" file in WordPerfect may store 250 document alterations. Gregory Johnson, *A Practitioner's Overview of Digital Discovery*, 33 GONZ. L. REV. 347, 360 (1997-1998).

[115] State v. Guthrie, 627 N.W.2d 401, 409-10 (S.D. 2001) (husband on trial for murdering his wife, was convicted partially based on evidenced plucked from his computer, including an unsent email and web searches conducted).

[116] Marcus, supra note 13, at 338.

which programs a user accesses, how long he or she spends in a program and whether he or she has edited specific files.[117] Some of these systems also track which websites their employees access and what files they download from the Internet.[118]

Along this same line, companies often grant certain employees greater access to certain parts of the computer network. For example, only certain employees may have access to edit a file, or certain sensitive information may be available only to a small number of users.[119]

All of this logged and accessed information would fall into the rules' definitions of "data compilation." Depending on the claims involved in the specific litigation, such information could be relevant and very valuable.

5. Information Recoverable from Individual Hard Drives

Emails, Internet postings and backup data can often be produced in either hard or disk copy. Certain categories of electronic data, however, may reside only, or primarily, on the hard drive of an individual PC. Discovery of information from personal hard drives is generally granted.[120] Such discovery is

---

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *See, e.g.,* Superior Consultant Co. v. Bailey, 2000 WL 1279161, 12 (E.D. Mich. Aug. 22, 2000) (plaintiff sought to prevent destruction of electronic data on hard drive); Northwest Airlines v.

generally thought of as taking the form of an on-site inspection.[121] The nature of such an inspection, however, makes it almost impossible to protect irrelevant, private, trade secret and even privileged information.[122] Further, inspection conducted by the opposing side or its agents poses potential for manipulation of the computer or information stored therein.[123]

It has become preferred protocol in these cases to appoint a neutral computer forensics expert to create a "mirror image" of the electronic evidence.[124] The procedure often prescribed for such inspections is as follows:[125]

1) The parties agree, or the court appoints, a third party expert who will carry out the inspection as an officer of the court.

Local 2000, C.A. No. 00-08DWF/AJB (D. Minn. Feb. 2, 2000) (Order on Defendants' Motion for Protective Order and Plaintiff's Motion to Compel Discovery); Northwest Airlines v. Local 2000, C.A. No. 00-08DWF/AJB (D. Minn. Feb. 29, 2000) (Memorandum Opinion and Order); see also Byrne v. Byrne, 650 N.Y.S.2d 499, 499-500 (N.Y. Sup. Ct. 1996) (awarding wife access to husband's computer to search for information about the couple's finances and marital assets); Alexander v. FBI, 188 F.R.D. 111, 117 (D.D.C. 1998) (granting plaintiff's discovery request to examine the hard drives of particular individuals).

[121] Withers, *supra* note 8, § II.G.1.

[122] *Id*.

[123] *Id*.

[124] *See* Playboy Enters., Inc. v. Welles, 60 F. Supp.2d 1050, 1055 (S.D. Cal. 1999) (court appointed a computer expert specifically in the creation of "mirror images"); Superior Consultant Co. v. Bailey, 2000 WL 129161, 12 (E.D. Mich., August 22, 2000) (ordering defendant to produce to plaintiff a backup file of defendant's laptop and any PC hard drive to which defendant had access.)

[125] The following list was modified from the list found in Withers' article. *See* Withers, *supra* note 8, § II.G.3.

2) The parties and expert agree on the scope of the inspection and identify target computers, servers, individuals, departments, data collections, date ranges, search terms and other necessary criteria. They also agree on a form at for eventual production

3) The expert creates a "mirror image" of the target data, preserving the data's integrity.

4) The expert searches the "mirror image" for the target information according to the agreed-upon protocol.

5) Respondent's counsel receives the responsive data from the expert and reviews it for privilege and relevance.

6) The relevant, non-privileged data is produced to the requesting party.[126]

Whereas it is a relatively simple task for a computer forensics expert to obtain the target data, the service can be very expensive and time-consuming.[127] Although the general rule is that parties bear their own discovery costs, courts have shown a willingness to engage in cost-shifting or cost-sharing to protect a party under the undue burden standard.[128] At their initial meetings, counsel

[126] *See* Northwest Airlines, Inc. v. Local 2000 Int'l Brotherhood of Teamsters, et al., Civil Action No. 00-08 (D. Minn. Feb. 2, 2000) (Order on Defendants' Motion for Protective Order and Plaintiff's Motion to Compel Discovery); Simon Property Group, L.P. v. MySimon, Inc., 2000 WL 863035 (S.D. Ind. June 7, 2000) (Entry on Plaintiff's Motion to Compel); Playboy Enters., Inc., 60 F. Supp. 2d at 1054 (holding that only "relevant, responsive, and non-privileged" matters would e produced for the plaintiff); *see also* Tulip Computers Int' B.V. v. Dell Computer Corp., 2002 WL 818061, 7 (D. Del., Apr. 30, 2002) (holding that the defendant is adequately protected by restricting the search to terms provided by plaintiff to the third party expert).

[127] Withers, supra note 8, § II.G.5.

[128] *See, e.g.,* Byers v. Illinois State Police, 2002 WL 1264004, 12 (N.D. Ill. June 3, 2002) (allowing the plaintiffs to recover archived e-mails only if they were willing to pay for the costs of

should attempt to ascertain whether a computer forensics expert will be necessary and attempt to agree on how costs will be handled.[129]

a. Deleted Documents

The delete function on the computer does not actually erase anything in the way "erase" is generally perceived. On a computer, the delete function removes the file from the disk directory immediately. On the disk itself, however, the location at which the data is stored is merely reclassified to a "not used" status, permitting the computer to use the disk space for another purpose.[130] The

---

production, thereby "provid[ing] them with an incentive to focus their requests[]"); Proctor & Gamble Co. v. Haugen, 179 F.R.D. 622, 632-33 (D. Utah 1998) (allowing the plaintiff to do a keyword search of defendant's database and ordering the plaintiff to pay $10,000 for its failure to preserve email records); Williams v. DuPont, 119 F.R.D. 648, 657 (W.D. Ky. 1987) (requiring the discovering party to bear costs of data production and reimburse the discovery target for a portion of the expense of assembling the database); Delozier v. First Nat'l Bank of Gatlinburg, 109 F.R.D. 161, 164 (E.D. Tenn. 1986) (stating that "[a] court will not shift the burden of discovery onto the discovering party where the costliness of the discovery procedure involved is entirely a product of the defendant's record-keeping scheme over which the plaintiff has no control."). *See also* Rowe Entertainment, Inc. v. The William Morris Agency, 2002 WL 63190, 4-11 (S.D.N.Y. Jan. 16, 2002) (adopting an eight-factor balancing approach to determining whether to shift the costs of production). Recently, however, Judge Shiva Scheindlin modified the Rowe eight factor test in Zubulake. The test implemented in Zubulake "actually creates a test closer to the Federal Rules of Civil Procedure, which start from the presumption that the producing party pays the cost." Jason Krause, E-Discovery Order Changing the Rules: Federal Decision Deals With Who Pays The Cost, 2 ABA Journal E-Report, ¶ 8 (June 6, 2003), *at* http://www.abanet.org/journal/ereport;bdiscovr.html.

[129] *See, supra* §A and accompanying text.

[130] Withers, *supra* note 8, § II.D.1.

material remains saved on the disk until it is overwritten.[131] Deleted electronic evidence is fully discoverable.[132]

b. Information Generated by Internet Web Sites

(i) Cache Files

Internet web sites are viewed by means

of web browser programs which translate the Internet website data into readable form on the user's PC. Browser programs typically store the Internet addresses of visited websites in a cache file. This saves time when the website is next accessed because it allows the computer to access the website address directly from local memory.[133]

These cache files also create a history of the websites a user visits, including the time it was visited. The user is often unaware of the creation of

[131] *See* Scheindlin & Rabkin, *supra,* note 26, at 337; Withers, *supra* note 337. Withers, *supra* note 8, §II.D.2. Even overwritten information may be restored in some circumstances. Marcus, *supra* 8, note 13, at 266.

[132] *See generally* Dodge, Warren & Peters Ins. Servs. v. Riley, 2003 WL 245586 (Cal. Ct. App. Feb. 5, 2003) (employer sued former employees and obtained an injunction requiring employees to preserve electronic evidence); Simon Property Group v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000) (deleted electronic files are permissible discovery requests and the defendant must comply); Easley, McCaleb & Assoc., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994); Alexander v. F.B.I., 188 F.R.D. 111 (D.C. Cir. 1998).

[133] Scheindlin & Rabkin, *supra* note 26, at 340. Cache files may be also stored on the server level of networked systems. *Id.* at 340 n.48. *See also* Johnson, *supra* note 28, at 368-69.

these cache files because they are created automatically. Such information is discoverable.[134] It can also be very valuable in certain cases.[135]

(ii) Cookies

Cookies are another type of file generated by websites and stored on the user's computer when he or she accesses the website. For example, a weather forecasting website may store a cookie on the computer's hard drive that records the user's zip code to allow for automatic retrieval of weather information for the user's location. Much like cache files, examination of the cookies on a computer allow a forensic expert to determine which websites a user has visited.[136]

C. Definitions[137]

Archival records records of data backup in which all files are copied to a backup storage device

[134] *See, e.g.*, Moench v. Red River Basin Board, 2002 WL 31109803 (Minn. Ct. App. 2002) (deciding a case regarding denial of unemployment benefits in which the employer engaged a computer forensic expert to investigate pornographic material stored in the cache file of the plaintiff's computer); *see also* cases cited infra note 135.

[135] *See generally* United States v. Tucker, 150 F. Supp. 2d 1263 (D. Utah 2001) (convicting defendant of possession of child pornography based on computer forensic evidence in the form of Internet cache files); State v. Guthrie, 627 N.W.2d 401 (S.D. 2001) (finding defendant who was accused of murder conducted numerous Internet searches on subjects related to the murder).

[136] Scheindlin & Rabkin, *supra* note 26, at 340-41.

[137] Excellent sources of definitions for technical terms may be found at the following websites http://www.webopedia.com; http://www.merriam-webster.com and http://www.krollontrack.com/LawLibrary/GlossaryOfTerms.

Archives disk, tape, or directory that contains files that have been backed up

Back-up tapes copy of data maintained on digital audio tape

Business record[138] a memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation

Cache file a high-speed storage mechanism that can either be a reserved section of main memory or an independent storage device

Cookie a message given to a Web browser by a Web server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them.

Data compilations collection of information, usually formatted in a special manner, stored on a computer system

Disc mirroring method of protecting data from hard disk failure by creating a mirror copy on a second hard disk or different part of the same disk

E-mail/Electronic mail the transmission of messages over communications networks

File collection of data or information that has a name and is stored in a specified location

Hard drive the mechanism that reads and writes data on a hard disk, which is a magnetic disk on which you can store computer data

Internet an electronic communications network that connects computer networks and organizational computer facilities around the world and uses the TCP/IP protocol to facilitate information exchange

[138] FED. R. EVID. 803(6).

Internet transaction an exchange or transfer of information over the global network connecting millions of computers using the TCP/IP protocol to facilitate information exchange

Intranet a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization.

IP Protocol/Internet Protocol an agreed-upon format for transmitting data between two devices that allows the addressee to deliver information through the system, without creating a direct link between the addressee and the recipient

Log record of an action

Metadata data about data that describes how, when, and by whom a particular set of data was collected, and how the data is formatted

Network a group of two or more computer systems linked together

System records the collection of data from computers or devices connected together

TCP Protocol/Transmission Control Protocol an agreed-upon format for transmitting data between two devices that enables two hosts to establish a connection and exchange streams of data

TCP/IP Protocol an agreed-upon format for transmitting data between two devices that establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Webpage postings information affixed to a collection of documents that can be viewed in a browser

World Wide Web system of Internet servers that support specially formatted documents

THE DuPont RECORDS MANAGEMENT MODEL

Donald A. Cohn

August 2003

ABA Annual Meeting

DUPONT CRIM PROGRAM

- Policy
- Issues
- Components of the Program
- Challenges

Policy

- Applies to All Records
- Responsibility & Accountable
  - Employees: Records in their Possession or Under Their Have Control
  - Line Management: Managing & Implementing Within Their Span Of Control
  - Corporate Management: Entire Program

Policy

- Permissive Retention
  - Keep Business Records For Up To 3 Years
  - Can Be Destroyed At Any Time
  - E Mail
- Mandatory Retention
  - "Schedule A" Records
  - UFTA
  - Legal Hold Orders
  - Regulatory, etc. Requirements

Policy

- Program Variances By Line Management
- All Applicable Regional Laws Will Be Followed

ISSUES

- Copies of Records
- Records Retention Period Determination
- Leaving the Company
- Inherited Records
- Custodial Records
- Records For Acquisitions, Divestitures & Mergers
- Joint Ventures and Subsidiary Records

COMPONENTS OF THE PROGRAM

- Administered by Corporate Records & Information Group
  - Central Group in Wilmington
  - Champions/Coordinators in SBU's, Function's, & Regions
  - Monthly Audio's
  - Quarterly Meetings
  - "The Glue"
  - Mantra "Creation, Implementation, Institutionalization"

COMPONENTS OF THE PROGRAM

- Swing Into Spring
- Janitor & Records Manager Information
- Ration Server Space

- CRIM and Network Activities
  - Educational Awareness
  - Records Retention Schedules Updates
  - Variance Procedures and Counsel
  - Distribution of Legal Hold Orders
  - Proper Disposition
  - Strategic Planning

COMPONENTS OF THE PROGRAM

- Addressing New Issues
- Review, Audit, & Report To Corporate Management
  - Internal Auditors
  - Special Records Audits
- Preservation of Historical Records
- Preservation of Vital Record

CHALLENGES

- ASP's/Outsourcers & Records Management
- Privacy & Records Management
- E-Contracting & Records Management
- The Supply/Value Chain & Records Management
- Discovery Issues
- The Future

Contents

NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION.

*NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION..

Introduction

Proper records management is an important function of every successful corporation. An effective records management program ensures that all records that are required to conduct the business of the corporation, to fulfill its legal responsibilities, and to support its tax liabilities are maintained and available.

An effective records management program also preserves the corporate memory and protects the corporation by ensuring compliance with local and federal laws.

Significant costs are associated with the creation, maintenance, distribution, and storage of records. Therefore stewardship must be exercised by producing clear, concise documentation only when there is a business requirement.

Refer to the “Corporate Business Writing Guide” for addi-tional information.

An alphabetical index is located at the back of this guide, which can be used to help you locate specific record names.

The information in this guide is also available on our Intranet Web site at _____ The Web site features a searchable special records retention database that can be used to find information about special records retention periods.

Purpose of This Guide

This guide sets forth policies and principles and describes the records management program so all employees can better manage DuPont’s business records. It is intended to provide ways to identify, maintain, and dispose of company records in a timely and cost-effective manner.

This guide does *not* apply to published information such as journals, government regulations, books, vendor brochures and catalogues, or any other public information. However, in the interest of space and information management efficien-cies, as well as housekeeping considerations, these records should be managed in a cost-efficient way. All copyright laws concerning making copies must be followed. Corporate Records Management Program Guide

March 19997

Records Management Policies for DuPont Employees

All employees are responsible and accountable for the records in their possession and those records for which they have control.

All local and federal laws will be followed by every DuPont employee during the creation, retention, and disposition of company records.

DuPont line management is responsible and accountable for managing and implementing the Corporate Records Manage-ment Program as set forth in this guide.

Every effort has been made to identify the legal requirements for recordkeeping in the United States. However, in keeping with the policy that all local and federal laws be followed in regard to creating, retaining, and destroying records, employ-ees and line management are accountable for identifying those areas that differ from the instructions in this guide.

Basic Principles of DuPont Records Management

Definition of a Record

All records created or received in the ordinary course of DuPont business are DuPont records, are the property of DuPont, and are subject to this guide. This pertains to *all* forms and *all* media, including:

• handwritten, typed, or printed documents on paper

• electronic documents (e.g., e-mail, Web sites, diskettes, CDs)

• video

• audio
• graphic representations
• network servers and document management systems

Note: A date must appear on all documents to keep records in context and to facilitate compliance with the records management program..

Copies of Records

If an official copy of a Special Record has been identified, any other copy of that record may be classified as a General Business Record (Max. 3 years). In no instance shall a copy of a record be kept longer than the official record.

Records Retention Periods

Retention periods vary by records category and are deter-mined by considering business use, tax liability, and legal requirements.

When to Destroy a Record (or Not)

A date must appear on all documents to keep records in context and to facilitate compliance with the records manage-ment program.

All DuPont business records must be properly destroyed at the end of their records retention period unless corporate management:

• has approved a variance to preserve them for business need (refer to “Variances”)
• has classified them for historical preservation (refer to “Preservation of Historical Records”)
• has identified them as subject to litigation or governmen-tal proceeding (refer to “Distribution of Legal Hold Orders”)

Leaving the Company

Upon retirement or separation from DuPont, each employee must return all DuPont records to the corporation. Line management will determine disposition by reassigning the records or properly destroying them according to the records retention described in this guide.

Inherited Records

Records that were previously managed by someone who left the company or changed job responsibilities and are now someone else’s responsibility are referred to as inherited records. As soon as these records become another person’s responsibility, they must continue to be reviewed and main-tained according to this guide.

Additional Records Considerations

Custodial (Contractor) Records

Custodial records are records that are maintained by service organizations such as outside law firms, engineering contractors, accounting firms, or information technology firms.

These records are either received from DuPont or prepared for DuPont and maintained by the contractor. These records belong to DuPont and are subject to compliance with our records management program. In addition, they may not be modified, destroyed, or even microfilmed without permission from DuPont.

Records from Acquisitions, Divestitures, and Mergers

Ownership of these records should be addressed in the acquisition, divestiture, or merger contract.

Joint Ventures and Subsidiaries

Because DuPont has an interest in the success of such organi-zations, each subsidiary or joint venture must have a viable records management program. Each situation is unique. Seek the advice of each organization's legal department when setting up a records management program. This Corporate Records Management Program can be used as a model; however, be sure the name of the joint venture or subsidiary appears on its records management program documents.

Components of the Program

A comprehensive records management program is administered by the Corporate Records and Information Management (CRIM) Group. The program components are described in this section.

Education and Awareness

Education and awareness of the Corporate Records Manage-ment Program will be implemented by the records analysts in the CRIM Group along with a network of records manage-ment champions. Each business has a champion who is accountable to the VP/GM or VP of that organization.

Records Retention Schedule

There are two types of records that employees must under-stand to properly manage their records—"General Business Records" and "Special Records." The retention schedule provides guidance for categorizing and describing all records and assigning a retention period for each.

General Business Records

All DuPont records may be kept for a period not to exceed three years (Max. 3 years) after the record creation date. All DuPont records are in this category unless identified as a Special Record.

Special Records

Special Records have a business, tax, or legal requirement that is more than three years. These records are in the Special Records Retention Periods listed in this guide. An explana-tion of the retention periods is also included.

Note: "Just in Case" is *not* a valid records retention period.

Review and Audit

An annual records *review* must be done by all employees who maintain company records. A “Swing Into Spring” program is coordinated between the CRIM Group and each business to ensure proper records management. The program highlights the benefits of the campaign and provides the time for all employees to review their DuPont records.

All records, both electronic and hardcopy, that have an expired retention period must be disposed of properly.

It is each employee’s responsibility to ensure that Special Records are not destroyed prematurely. Special attention should be given to records that need to be held for tax or legal purposes.

In addition to periodic reviews, *audits* shall be performed and results reported as requested by the CRIMGroup.

• The self-assessment is designed to educate employees about the Corporate Records Management Program and help them perform an audit of the records under their control.

• An internal records audit is performed by a team within each business. Internal records audits are also done by the CRIM Group.

• External records audits will be performed by an outside organization on an occasional basis. These audits will be contracted for and managed by the CRIM Group at the request of the Operating Group.

Proper Disposition

Records should be disposed of according to the level of confidentiality or content of proprietary information.

• Records with no personnel or proprietary information can be thrown in with the regular trash pickup.

• Records containing personnel or proprietary information must be shredded, incinerated, or pulped. The security of the proprietary information should be monitored until destruction is actually performed..

Distribution of Legal Hold Orders

The CRIM Group works with Legal to ensure that everyone who has records relating to pending or active litigation or government investigation is aware of the matter. Employees must then notify Legal and identify those records that must be held pending the resolution of that matter. In some instances a single record could be held for more than one matter. When the Records Hold Order is lifted, the records revert to their original categories and may be destroyed according to the retention schedule.

Preservation of Vital Records

Vital Records are included in the Corporate Records Manage-ment Program and as such are subject to the same retention guidelines. Vital records are those required to establish the:

• corporation as a legal entity (e.g., Articles of Incorpora-tion)
• corporation's fiscal and accounting position (e.g., SEC Filings)
• primary legal obligations to and of the company (e.g., Contracts)
• basic research, technical, and development know-how of the company (e.g., Laboratory Notebooks)
• basic processes, production, and operating expertise of the company's primary engineering, construction, and flow chart records (e.g., Engineering Drawings)

Each business is responsible for specifically designating their vital records. The Vital Records Group consults with the business to decide the best safeguarding method for each record.

The primary records protection method used is "geographic dispersion." This is where the original record is kept in a different location from the electronic, paper, or microfilm copy..

Preservation of Historical Records

The Hagley Museum and Library is the holder of DuPont Company historical files, dating back to 1802. The CRIM Group coordinates the gathering of records of historical significance after they have met the retention period for business, legal, and tax reasons.

After approval is given by the owners of the identified records, they are donated to Hagley and made available for scholarly research 25 years after the date of the document. Any request to view the records before that time must be approved by Legal.

Records having permanent historical value include:
• records documenting corporate managerial functions
• financial records, including audit reports, balance sheets, and statements
• records documenting key strategic decisions and changes in corporate structure
• records documenting key corporate activities
• documentation of the relationship between DuPont and its customers, society, and government
• photographs depicting work processes, innovative tech-nologies, plants, and worker housing

Records Storage Accountability

CRIM manages a contract with a national records manage-ment company that provides storage and retrieval services. Contact the CRIM Group for up-to-date information on locations and rates.

Most paper records are stored at a Wilmington facility. The records are protected against fire, water damage, theft, and vandalism. The temperature range of the facility is 60–90°F. Microfilm and electronic media are stored in a climate-controlled

building maintained by DuPont..Corporate Records Management Program Guide
14 March 1999

Variances

In a limited number of cases, DuPont records may be retained **beyond** the General Records or Special Records retention periods, as appropriate, but only upon an affirmative demon-stration of business need by the employee wanting to retain the record. The burden and responsibility of requesting and justifying an extension rests with the employee. Line man-agement has the responsibility of determining the appropri-ateness of the requested variance and the length of additional time to retain the record.

The Corporate Records Management Group will assist line management as a resource to provide guidelines and share experiences..Corporate Records Management Program Guide

Special Records Retention Periods

Retention periods for Special Records are:

• **Max. "x" number of years** means that a record may be destroyed anytime up to and including "x" years.

• **"x" number of years** means that the record must be kept for exactly "x" number of years. In the interest of effi-ciency, that can be interpreted as "x" number of years plus the current year so that file cleanup can be done once a year.

• **"x" number of years after an event** means that the record must be kept for exactly "x" number of years after the event (such as termination, completion of all obliga-tions, or settlement of claims) occurs.

• **Until Superseded** means that when a new revision is issued, the previous one should be destroyed. In some cases, one historical copy may be maintained, as noted in this section.

• **Until Obsolete** means that a record is held until no longer needed for business purposes.

• **UFTA** means Until Completion of Federal Tax Audit. Contact local management or the CRIM Web site for current information.

• **UFTA/"x" years** means that both retentions must be satisfied.

• **UFT**A—**an event such as closing or expiration** means that the UFTA is related to the year of the event.

• **For Life of Facility** means for as long as DuPont owns the facility or has retained control over it.

• **For Useful Life of Product** means for as long as DuPont manufactures a product plus the period of time that the product is used as intended.

• **Max. Permanent** refers to records that have long-term value and may be kept permanently but need not be.

[Schedules Deleted]

Contents

NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION.

*NOTE: PAGE NUMBERS IN THIS PDF DOCUMENT ARE NOT THE SAME AS IN THE PRINTED VERSION..

Introduction

Proper records management is an important function of every successful corporation. An effective records management program ensures that all records that are required to conduct the business of the corporation, to fulfill its legal responsibilities, and to support its tax liabilities are maintained and available.

An effective records management program also preserves the corporate memory and protects the corporation by ensuring compliance with local and federal laws.

Significant costs are associated with the creation, maintenance, distribution, and storage of records. Therefore stewardship must be exercised by producing clear, concise documentation only when there is a business requirement.

Refer to the “Corporate Business Writing Guide” for addi-tional information.

An alphabetical index is located at the back of this guide, which can be used to help you locate specific record names.

The information in this guide is also available on our Intranet Web site at _____ The Web site features a searchable special records retention database that can be used to find information about special records retention periods.

Purpose of This Guide

This guide sets forth policies and principles and describes the records management program so all employees can better manage DuPont’s business records. It is intended to provide ways to identify, maintain, and dispose of company records in a timely and cost-effective manner.

This guide does *not* apply to published information such as journals, government regulations, books, vendor brochures and catalogues, or any other public information. However, in the interest of space and information management efficien-cies, as well as housekeeping considerations, these records should be managed in a cost-efficient way. All copyright laws concerning making copies must be followed. Corporate Records Management Program Guide

March 19997

Records Management Policies for DuPont Employees

All employees are responsible and accountable for the records in their possession and those records for which they have control.

All local and federal laws will be followed by every DuPont employee during the creation, retention, and disposition of company records.

DuPont line management is responsible and accountable for managing and implementing the Corporate Records Manage-ment Program as set forth in this guide.

Every effort has been made to identify the legal requirements for recordkeeping in the United States. However, in keeping with the policy that all local and federal laws be followed in regard to creating, retaining, and destroying records, employ-ees and line management are accountable for identifying those areas that differ from the instructions in this guide.

Basic Principles of DuPont Records Management

Definition of a Record

All records created or received in the ordinary course of DuPont business are DuPont records, are the property of DuPont, and are subject to this guide. This pertains to *all* forms and *all* media, including:

• handwritten, typed, or printed documents on paper

• electronic documents (e.g., e-mail, Web sites, diskettes, CDs)

• video

• audio
• graphic representations
• network servers and document management systems

Note: A date must appear on all documents to keep records in context and to facilitate compliance with the records management program..

Copies of Records

If an official copy of a Special Record has been identified, any other copy of that record may be classified as a General Business Record (Max. 3 years). In no instance shall a copy of a record be kept longer than the official record.

Records Retention Periods

Retention periods vary by records category and are deter-mined by considering business use, tax liability, and legal requirements.

When to Destroy a Record (or Not)

A date must appear on all documents to keep records in context and to facilitate compliance with the records manage-ment program.

All DuPont business records must be properly destroyed at the end of their records retention period unless corporate management:

• has approved a variance to preserve them for business need (refer to “Variances”)
• has classified them for historical preservation (refer to “Preservation of Historical Records”)
• has identified them as subject to litigation or governmen-tal proceeding (refer to “Distribution of Legal Hold Orders”)

Leaving the Company

Upon retirement or separation from DuPont, each employee must return all DuPont records to the corporation. Line management will determine disposition by reassigning the records or properly destroying them according to the records retention described in this guide.

Inherited Records

Records that were previously managed by someone who left the company or changed job responsibilities and are now someone else’s responsibility are referred to as inherited records. As soon as these records become another person’s responsibility, they must continue to be reviewed and main-tained according to this guide.

Additional Records Considerations

Custodial (Contractor) Records

Custodial records are records that are maintained by service organizations such as outside law firms, engineering contractors, accounting firms, or information technology firms.

These records are either received from DuPont or prepared for DuPont and maintained by the contractor. These records belong to DuPont and are subject to compliance with our records management program. In addition, they may not be modified, destroyed, or even microfilmed without permission from DuPont.

Records from Acquisitions, Divestitures, and Mergers

Ownership of these records should be addressed in the acquisition, divestiture, or merger contract.

Joint Ventures and Subsidiaries

Because DuPont has an interest in the success of such organi-zations, each subsidiary or joint venture must have a viable records management program. Each situation is unique. Seek the advice of each organization's legal department when setting up a records management program. This Corporate Records Management Program can be used as a model; however, be sure the name of the joint venture or subsidiary appears on its records management program documents.

Components of the Program

A comprehensive records management program is administered by the Corporate Records and Information Management (CRIM) Group. The program components are described in this section.

Education and Awareness

Education and awareness of the Corporate Records Manage-ment Program will be implemented by the records analysts in the CRIM Group along with a network of records manage-ment champions. Each business has a champion who is accountable to the VP/GM or VP of that organization.

Records Retention Schedule

There are two types of records that employees must under-stand to properly manage their records—"General Business Records" and "Special Records." The retention schedule provides guidance for categorizing and describing all records and assigning a retention period for each.

General Business Records

All DuPont records may be kept for a period not to exceed three years (Max. 3 years) after the record creation date. All DuPont records are in this category unless identified as a Special Record.

Special Records

Special Records have a business, tax, or legal requirement that is more than three years. These records are in the Special Records Retention Periods listed in this guide. An explana-tion of the retention periods is also included.

Note: "Just in Case" is *not* a valid records retention period.

Review and Audit

An annual records *review* must be done by all employees who maintain company records. A “Swing Into Spring” program is coordinated between the CRIM Group and each business to ensure proper records management. The program highlights the benefits of the campaign and provides the time for all employees to review their DuPont records.

All records, both electronic and hardcopy, that have an expired retention period must be disposed of properly.

It is each employee’s responsibility to ensure that Special Records are not destroyed prematurely. Special attention should be given to records that need to be held for tax or legal purposes.

In addition to periodic reviews, *audits* shall be performed and results reported as requested by the CRIMGroup.

• The self-assessment is designed to educate employees about the Corporate Records Management Program and help them perform an audit of the records under their control.

• An internal records audit is performed by a team within each business. Internal records audits are also done by the CRIM Group.

• External records audits will be performed by an outside organization on an occasional basis. These audits will be contracted for and managed by the CRIM Group at the request of the Operating Group.

Proper Disposition

Records should be disposed of according to the level of confidentiality or content of proprietary information.

• Records with no personnel or proprietary information can be thrown in with the regular trash pickup.

• Records containing personnel or proprietary information must be shredded, incinerated, or pulped. The security of the proprietary information should be monitored until destruction is actually performed..

Distribution of Legal Hold Orders

The CRIM Group works with Legal to ensure that everyone who has records relating to pending or active litigation or government investigation is aware of the matter. Employees must then notify Legal and identify those records that must be held pending the resolution of that matter. In some instances a single record could be held for more than one matter. When the Records Hold Order is lifted, the records revert to their original categories and may be destroyed according to the retention schedule.

Preservation of Vital Records

Vital Records are included in the Corporate Records Manage-ment Program and as such are subject to the same retention guidelines. Vital records are those required to establish the:

• corporation as a legal entity (e.g., Articles of Incorpora-tion)
• corporation's fiscal and accounting position (e.g., SEC Filings)
• primary legal obligations to and of the company (e.g., Contracts)
• basic research, technical, and development know-how of the company (e.g., Laboratory Notebooks)
• basic processes, production, and operating expertise of the company's primary engineering, construction, and flow chart records (e.g., Engineering Drawings)

Each business is responsible for specifically designating their vital records. The Vital Records Group consults with the business to decide the best safeguarding method for each record.

The primary records protection method used is "geographic dispersion." This is where the original record is kept in a different location from the electronic, paper, or microfilm copy..

Preservation of Historical Records

The Hagley Museum and Library is the holder of DuPont Company historical files, dating back to 1802. The CRIM Group coordinates the gathering of records of historical significance after they have met the retention period for business, legal, and tax reasons.

After approval is given by the owners of the identified records, they are donated to Hagley and made available for scholarly research 25 years after the date of the document. Any request to view the records before that time must be approved by Legal.

Records having permanent historical value include:
• records documenting corporate managerial functions
• financial records, including audit reports, balance sheets, and statements
• records documenting key strategic decisions and changes in corporate structure
• records documenting key corporate activities
• documentation of the relationship between DuPont and its customers, society, and government
• photographs depicting work processes, innovative tech-nologies, plants, and worker housing

Records Storage Accountability

CRIM manages a contract with a national records manage-ment company that provides storage and retrieval services. Contact the CRIM Group for up-to-date information on locations and rates.

Most paper records are stored at a Wilmington facility. The records are protected against fire, water damage, theft, and vandalism. The temperature range of the facility is 60–90°F. Microfilm and electronic media are stored in a climate-controlled

building maintained by DuPont..Corporate Records Management Program Guide
14 March 1999

Variances

In a limited number of cases, DuPont records may be retained **beyond** the General Records or Special Records retention periods, as appropriate, but only upon an affirmative demon-stration of business need by the employee wanting to retain the record. The burden and responsibility of requesting and justifying an extension rests with the employee. Line man-agement has the responsibility of determining the appropri-ateness of the requested variance and the length of additional time to retain the record.

The Corporate Records Management Group will assist line management as a resource to provide guidelines and share experiences..Corporate Records Management Program Guide

Special Records Retention Periods

Retention periods for Special Records are:

• **Max. "x" number of years** means that a record may be destroyed anytime up to and including "x" years.

• **"x" number of years** means that the record must be kept for exactly "x" number of years. In the interest of effi-ciency, that can be interpreted as "x" number of years plus the current year so that file cleanup can be done once a year.

• **"x" number of years after an event** means that the record must be kept for exactly "x" number of years after the event (such as termination, completion of all obliga-tions, or settlement of claims) occurs.

• **Until Superseded** means that when a new revision is issued, the previous one should be destroyed. In some cases, one historical copy may be maintained, as noted in this section.

• **Until Obsolete** means that a record is held until no longer needed for business purposes.

• **UFTA** means Until Completion of Federal Tax Audit. Contact local management or the CRIM Web site for current information.

• **UFTA/"x" years** means that both retentions must be satisfied.

• **UFT**A—**an event such as closing or expiration** means that the UFTA is related to the year of the event.

• **For Life of Facility** means for as long as DuPont owns the facility or has retained control over it.

• **For Useful Life of Product** means for as long as DuPont manufactures a product plus the period of time that the product is used as intended.

• **Max. Permanent** refers to records that have long-term value and may be kept permanently but need not be.

[Schedules Deleted]