AIA Trust
Where smart architects manage risk®

# THE ABC'S OF E-DATA: A Discussion Related to the Issues Raised by Electronic Information

by Jannea S. Rogers, Esquire (1)

Table of Contents



**This paper is intended to provide the reader a basic knowledge of the law pertaining to electronic data. In addition, there are specific suggestions provided on how to create a document management plan with contact information included to address a mixed data environment and dealing with possible electronic discovery process if involved in a production request or litigation.**

Published by the AIA Trust, theaiatrust.com

## I. INTRODUCTION

The law pertaining to electronic data is still being developed, and it is essential for professional firms conducting business in today's world to have an awareness of the issues raised by electronic data. This awareness should include familiarity with what rules of discovery require when production of the data become appropriate. Specifically, professional firms should be able to identify what electronic data is involved in their daily operations, know how to properly store and discard electronic information in the day to day operation of business and know the extent to which they may be required to produce electronic information in the event of litigation.

This paper is intended to provide the reader knowledge through analysis of the newly amended federal discovery rules and cases applying those rules. This paper will provide you with the information necessary to identify and manage electronically stored information so that it can be preserved and produced in the event of litigation. This will paper will also identify disclosure issues with hidden data and provide suggestions on how to establish a system and manage same. Finally, information will be provided in the addendums to assist you to locate vendors to assist you with production, with metadata management as well as provide samples of document retention policies that may be of benefit to professional firms conducting business in today's world.

## II. IDENTIFICATION OF ELECTRONIC INFORMATION

Electronic data can be anything that is created, revised or stored electronically. The sources of electronic data are multiplying and the formats are proliferating with each new advance in technology. The electronic form of communication has supplanted oral

communications in the computer age and has created records of communications that previously did not exist. The most obvious form of electronic data is email and other electronic communications such as instant messages and text messaging.

While most companies have a routing and filing system for mail and other physical documents, few companies proactively manage the storage of electronic information. Even fewer companies have written policies mandating how electronic data will be retained, disseminated, destroyed or even created. The lack of policies is in most instances due not to lack of desire to properly manage but a general lack of awareness of the issues raised.

Another difference in electronic data deals with its raw volume. The volume of electronic data is increasing daily as 99% of all new information is stored electronically mostly on hard discs. By the end of 2006, almost 60 billion email messages were being sent each day. The source of electronic data has multiplied from emails sent from personal computers and stored on servers to electronic voice mail systems, PDAs, telephones, as well as a variety of backup media. The formats have proliferated as Outlook, Word, Lotus Notes, Interwoven, Excel, AutoCAD and other proprietary software are created.

A popular music storage product sold in stores today carries 180 gigabyte of memory in a space smaller than your palm. To describe the amount of information that has or can be reduced to that size, it should be noted 1 megabyte is the equivalent of a short novel. In more descriptive terms, 50 megabytes is the equivalent of one bankers box of documents. A gigabyte is the equivalent of a pickup truck filled with novels. A terabyte is the same as 50,000 trees reduced to paper. An average laptop hard drive can store

between 500 and 1,000 bankers boxes of documents in an area smaller than a CD. The palm sized music device now sold can hold the equivalent of upwards to 150 truck loads of books.

Electronic data is also different in the type of information it retains. Historically, a letter would be sent from which either a carbon copy or a photocopy was made. The only information stored with the carbon or photocopy was the exact information contained on the face of the letter. Electronic data however retains three dimensions of a document.

The first dimension stored by electronically is the front of the document. This is the image such as contained on a letter face. This is not searchable nor does it hold hidden information. It is the equivalent of a photocopy or carbon copy.

The second dimension in electronic format is the middle of the document which is the text. The text contains what the document "says" and is fully searchable in certain programs. Specifically, a word or name may be selected and search through the middle of the document to pull and locate documents buried within the hard drive that contain the sought after text.

The third dimension of electronic data is the back of the document which is *metadata*. Metadata is defined as that hidden data that describes the document. This includes information such as the date the document was created, who was carbon copied or blind copied, links to attachments, links to revisions, format information, as well as a record of information deleted or substituted. Metadata may come from many sources in addition to the original creator of the document. A person using the document as a form can make revisions including people outside your office. The metadata may not be correct as to date, time, manner of creation or edits as it can be altered. Metadata also provides

additional information about the document not found in a paper version such as the date of latest access to the document, and also provides a link between the document itself, any attachments, any email conversation thread as well as the origination of the documents. Metadata also allows for de-duplication of a document.

## III. MANAGEMENT OF ELECTRONICALLY STORED INFORMATION

The hallmarks of an effective information management system include the adoption of an information retention policy, implementation of procedures implemented to require compliance with the policy as well as instruction on permissible creation and storage of electronic information and appropriate destruction of same. An effective system must reflect the interest of the organization and be tailored to its needs. The system must identify and preserve necessary documents and reflect an interest other than elimination of potentially damaging evidence. A proper system should consider whether the system is best served by a policy that minimizes the number of documents retained. The system also should identify sensitive documents such as those containing confidential or proprietary information on the front end and outline a method to retain same by flagging those for preservation. Data should be organized so it can be easily retrieved with designated individuals or departments identified to track and monitor electronic data. The system should encourage strict enforcement of security measures, a policy for regularly scheduled destruction of email, voice mail and stored data. The system should also outline measures to avoid inadvertent disclosure. The policy must be reviewed regularly, contain a clear litigation hold policy and discuss issues related to electronically stored information held by third party vendors.

## A. PRESERVATION OF ELECTRONIC INFORMATION

The previous Federal Rules of Civil Procedure created upon companies a duty to preserve documents they reasonably anticipate may be discoverable if there was a reasonable belief there may be litigation.[2] Once a party had notice of the relevance of electronic information to imminent or current litigation, the duty to preserve the data arose.[3] Once a party reasonably anticipates litigation, it has a duty to suspend any routine document purging system that might be in effect and to put in place a litigation hold to ensure the preservation of relevant documents. The failure to do so constitutes spoliation.[4]

The scope of the duty to preserve electronic information has been expanded in recent years. There may be a distinction related to electronic document retention requirements between privately held and publicly owned entities. Certain public and traded entities have exchanged related requirements as well as industry based regulatory requirements. While there is a general duty to preserve all relevant information, a company does not have to preserve every shred of paper, email, or backup tape simply because of the threat of litigation.[5] A company generally need not preserve all back up tapes even when it reasonably anticipates litigation.[6] But "one who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might by useful to an adversary."[7] The duty to preserve information extends to all employees who are "likely to have discoverable information that the disclosing party may use to support its claims or defenses."[8] Also, any and all relevant documents in existence at the time the duty to preserve attaches, and any relevant documents created thereafter should be retained.[9]

### (1) Litigation Hold

Companies should generally have a routine document retention policy created to keep documents from the hands of others, and "it is not wrongful for a manager or company to instruct its employees to comply with a valid document retention policy under normal circumstances."[10] Yet, a company must suspend its usual retention/destruction policy and implement a litigation hold once that company reasonably anticipates litigation.[11] Once the company is aware they possess information relevant to the potential litigation they must preserve those documents, and courts have stated it is the responsibility of the company's legal counsel to ensure the documents are preserved.[12] This preservation is accomplished by instituting a litigation hold.[13] The obligation to ensure preservation of the electronic documents does not, however, end by merely advising the employers of the litigation hold: counsel and company leaders must actively locate all potentially relevant information and ensure the continued preservation of electronic documents.[14]

To accomplish this task, counsel and the company leaders should locate all potentially relevant information. This task requires time and cooperation so the company's counsel and leaders can become familiar with the issues raised by the claim and how the document retention policy may impact relevant information.[15] If it is not feasible for every key player in a company to be involved or interviewed then either counsel or company leaders should run a system-wide keyword search to ensure any pertinent documents are retrieved and the documents are retained. Therefore, counsel and the company jointly have an affirmative duty to monitor compliance so that all sources of discoverable information are identified and preserved.

Next, there is a continuing duty to ensure preservation. Once the company and counsel have identified relevant information they must ensure it is retained.[16] Further, there is a continuing duty to supplement any responses made to the opposing party.[17] The counsel ultimately has the duty to periodically recheck all interrogatories and canvass all new information.[18] However, because of the continued duty to seasonably supplement responses, it is "strongly suggested that companies also have a duty to make sure that discoverable information is not lost."[19] To ensure the documents are not lost, a company should follow three steps laid out by prior court decisions.

First, after issuing the litigation hold, the company should periodically reissue the hold so as to make new employees aware of it and refresh the minds of all employees. [20] Second, "the company should communicate directly with 'key players' in any litigation" and stress the importance of the duty to preserve.[21] The key players should also be reminded the litigation hold is still in place.[22] "Finally, the company should instruct all employees to produce electronic copies of their relevant active files[,]" and should ensure all relevant backup tapes are identified and stored in a safe place.[23] The burden may be great but past situations have shown that with effective communication between the company, its employees and its counsel all the relevant electronic information can be preserved and properly produced when required by the court. [24]

**(2) Scope of Preservation Obligations**

When involved in litigation either as a party or a witness it is important to note the court can require disclosure of any matter, not privileged, that is relevant to the claim or defense of any party."[25] Courts can thus order production of any electronic information it

deems *relevant* to the litigation. Courts have interpreted relevant to mean the evidence that "appears reasonably calculated to lead to the discovery of admissible evidence."[26] Relevancy is determined at the discretion of the trial court and is generally broadly interpreted. Any potentially relevant document including "copies of emails, original pages from notepads, schedule printouts, letters, and other "items" must be disclosed.[27] Relevant documents may also include personal calendars, voice mail recordings and information held on a company laptop, cell phone, or PDA. If the court can formulate a link between any fact and a document, the court could rule it relevant; therefore, it should be retained.

The Rules do provide limitations on the scope of discovery in the form of a "proportionality test" which states discovery can be limited by the court if the discovery sought is unreasonably cumulative or is available from a more convenient, less burdensome, less expensive source, or the burden or expense outweighs the benefit.[28] Usually, if a company believes the request to be too broad or expensive they can argue the request is overly burdensome and overly broad in an attempt to lessen the amount of documents they must produce.[29] It must be noted however that judicial description in this area is broad and universally courts tend to err on the side of more rather than less production.

**B. Disclosure Format**

Generally courts have required companies to produce all electronic documents in their native format.[30] The Rules provide "a party who produces documents for inspection shall 'produce them as they are kept in the usual course of business.'"[31] When a court

specifically requests documents for production to be produced in a certain format, the rules require the company to produce those documents in the specified format.[32] Often, if the documents are converted then they do not contain the same information as in the native form and the deleted or altered information might be relevant and discoverable.[33] For example, a Word document often contains information in "back of" the document such as Metadata to be discussed herein. Courts have held that because the information sought may be relevant at the discovery stage, and unless a company suggests the electronic media contains privileged or classified information, the company will be required to produce the information in its stored format.[34] Therefore, unless the company can argue the information in its native format is privileged or classified, it must produce the electronic documentation in the specific electronic format.[35] Importantly, while courts generally require production in native format, prior to court's order the lawyers representing the company are free to negotiate the format with the other party.[36] Many lawyers opt for a hard copy printout of a document without realizing there may be electronic information hidden in the original format.

**(1) Metadata Issues**

Included in production format consideration is the issue of metadata, which is a large issue when producing the electronic documents in their native format. Metadata is commonly referred to as "information about information"[37] meaning it is "information describing the history, tracking, or management of an electronic document.[38] When using word processing software information other than the face of the document is stored and as described earlier, this is the metadata.[39] Examples of metadata a company may not want disclosed include the creator of the documents name, initials, company name, name of

computer used, name of the network, summary of information, names of previous authors, document revisions, hidden test, and comments.[40] This becomes an issue if a party claims an alternate design should have been used and the metadata holds a record of all prior revisions. It is difficult and time consuming to remove all metadata and some online tools can help users discover even deeply hidden metadata. Yet, metadata can be hidden or "scrubbed" from the document if one utilizes one of various programs available such as iScrub and Workshare. [41]

Metadata can also be hidden if the documents are converted to another form such as PDF, TIFF or JPEG format. [42] For example, a PDF or TIFF file is usually a snapshot of a document but there may be ownership and security information available to the semi-sophisticated user of the format. A JPEG document almost always contains a significant amount of information such as information on the camera used to capture the photographs, its settings, author and in some instances GPS or location data. For the architect and engineer community, a BIM (Building Information Modeling) Project has as an inherent part the inclusion of information such as building component characteristics including lost information, fire rating, materials, finishes, installation instructions, analysis and properties.

The possibility of deleting or hiding metadata leads to the question of whether a company producing documents should convert the documents to another format or scrub the metadata. In other words, are the documents to be provided in native format with the metadata or can they be scrubbed to prevent someone from receiving the metadata. Often a question arising during litigation is whether a document can be scrubbed without either the agreement of the parties or the company providing notice through an objection

or motion for protective order. Various groups and organizations have attempted to address the issue of "whether emerging standards of electronic discovery articulate a presumption against production of metadata." Courts have previously determined the rules provided no guidance in this area and have therefore turned to principals of various groups to hold that when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. [43]

Thus, the general rule is that the responding company must provide the metadata with the document provided unless the responding company timely objects to the inclusion of the metadata. Some common objections are relevancy, reliability, and privilege.[44] Courts have limited production to hard copies only when the responding company has timely objected. The information can be provided on a disk as long as it is in native format and accessible to the requesting party. However, it should be noted the Rules allow a company to agree to a production format and allow the documents to be produced in a format other than native format if an agreement has been reached before court intervention was had. [45]

## IV. TECHNICAL PROBLEMS AND COSTS OF PRODUCTION

Recovering data that is no longer readily available because it is stored on backup tapes presents several challenges including the cost of recovering the information, searching for the information, reviewing the information, and producing the information. [46]

Generally, backup tapes take a snapshot of the data system at a certain point in time. The snapshots may be taken several times a day or once a day but in either instance the backup tapes will contain repetitive and identical information and may not contain all the information. For example, if an email was sent and received and deleted prior to the snapshot being taken then that email will not be available on the tape. The largest issue by far with regard to discovering documents on backup tapes is the cost of retrieval, review, and production of the data.

**a. Forensic Cost of Retrieval**

The price of the cost of retrieval of the information stored on backup tapes can be astronomical depending on the size of the company and how the company utilizes email and other documents that are saved onto backup tapes. One law review article has reported the actual or estimated restoration costs of several cases [47] and has identified costs that have ranged from several hundred thousand dollars to almost ten million dollars. [48]

There are several reasons for the level of expense to retrieve data, one mainly being "sheer magnitude."[49] Because companies in today's world communicate electronically and those electronic communications are saved several times a day on backup tapes or some other type of electronic media, the amount of duplicate documents can be astounding. Also most of the saved documents are redundant. For instance, if one individual sends an email to five people and then four of those recipients forward it to five others there are now 25 versions of the original message.[50] Then if the company backups its data each night, 50 copies exist the next day.[51] In order for the company to produce the data in a manner consistent with the Rules of Discovery, the company must review

each document to determine whether it is merely duplicative of another document, which is not only time consuming but expensive. Yet another reason it is problematic is that the electronic storage devices are meant for disaster recovery not for "ready, text-searchable access" which makes recovering data even more time consuming and expensive. [52] Overall, the cost of retrieval of documents from backup sources storing electronic data is expensive for the company because of the magnitude of information, the redundancy of information, and the costs of locating for the information.

### b. Costs of Privilege Review When Data Recovered

Another issue is the cost of reviewing for privileged information, reviewing the data in general, and then producing the information. Due to the volume and nature of electronic discovery attorney-client privilege and proprietary corporate issues come into play such as inadvertent disclosure and the expense of reviewing all documents for privilege. Generally, if a company inadvertently produces privileged information they have waived their attorney-client privilege to that information.[53] Attorneys and their clients often communicate through emails and other electronic devices that may be saved on a company's backup tapes or optical disks. Also, dealing with redundancy and magnitude, the emails may be copied, forwarded and saved several times meaning an enormous amount of the electronic documents could contain privileged information and thus must be reviewed individually for privilege. According to some, privilege screening is emerging as the greatest expense in producing electronic documents because it must be performed manually, not by a computer program which would help lower costs. [54]

Courts have allowed various production options to companies to help lower such mounting costs.[55] For example, courts have given companies two options in the past.[56] One such option was that the requesting party would pay the cost of hiring an expert to recover the company's emails and would perform an initial review to identify those that it considered responsive. The company would then review those designated documents to determine whether any were privileged and then the company could object to the production. The second option would allow the company to review, at its own cost, all the documents recovered by the expert and produce only the responsive, non-privileged documents to the plaintiffs.[57] Regardless of whether the court allows such options for cost reduction, the expense of screening all electronic documents for privilege is still an expensive endeavor. [58]

Actual retrieval of the data is another expensive concern for any company considering most backup data is stored for the purpose of disaster recovery not production for litigation. Some types of data are more easily searched due to their accessible nature, other types of media are not as accessible and therefore more costly to search and retrieve. If using certain types of media like backup tapes, the information must be restored and then searched. The process of restoration often requires the help of outside computer resource companies to restore and search the data. For example, traditional recovery requires: re-creation of the original hardware and software in use at the time the data was created and stored; labor-intensive manual intervention; and the costs of equipment capable of storing the same amount of data as the data that is being recovered. [59] The search terms themselves can also be problematic as the company must determine which search terms will produce documents responsive to the request. [60] Some courts

have required parties to have an electronic discovery conference in which to determine a set of search criteria to search the data for what will produce the most accurate documents.[61] There are also added costs in producing the documents once they are ready to be produced to the requesting party. Once the documents have been located and reviewed generally the documents must be produced in their native format.

**c. Allocation of Cost of Electronic Discovery**

Due to the expensive nature of electronic discovery courts have looked to several different cost-shifting approaches to reduce the burden on the company involved in production. The current Rule provides that each party bears its own cost of discovery.[62] There is a proportionality test which limits discovery when:

> (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 sough; 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. [63]

However, over the years the cost of producing electronic data has increased significantly in part due to the volume but largely as a function of the inaccessibility. [64] Cost-shifting paradigms have been considered in the past but it became apparent such paradigms were not enough and courts began to cultivate their own cost-shifting considerations. The earliest test promulgated has undergone multiple revisions and is now set out in a 7 factor test now referred to as the *Zubulake* factors:

1. The extent to which the request is tailored to discover relevant issues.
2. the availability of the data from other sources;
3. total cost of production, relative to the amount in controversy;

4. total cost of production, relative to resources available each party;
5. the relative ability and incentive for each party to control its own costs;
6. the importance of the issues at stake in the litigation; and
7. the relative benefits to the parties in obtaining the data. [65]

Courts have noted the importance of discussing each of these factors on a case by case basis because each situation is unique to each company.

### d. Rules As Related to a Non-party

The rules on electronic discovery appear not to have changed the procedure and burdens relating to the cost of discovery that exist on companies that are not parties to litigation. The principal difference between electronic discovery from third parties – as compared to electronic discovery from parties – is that third parties enjoy more protection from burdensome and costly discovery than do parties. For example, a third party may in some instances [66] pay all, [67] part, [68] or none [69] of the discovery costs. The rules requires a party or an attorney responsible for the issuance and service of a subpoena on a non party to take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The "expense" for producing documents may include attorney fees for reviewing the subpoenaed documents, including privilege review.[70] The law of third-party electronic discovery is only now beginning to develop.[71]

## V. FAILURE AND CONSEQUENCES

If a company becomes involved in litigation and is unable or unwilling to participate properly in production there are various consequences.

### A. Spoliation

Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable

litigation."[72] When the duty to preserve arises and a company fails to preserve that evidence then a court may impose sanctions on the company for its breach of duty. Spoliation and sanctions are directly related to the duty to preserve as discussed above.

A court has the right and the power to impose sanctions for spoliation but it is "limited to that necessary to redress conduct 'which abuses the judicial process'"[73] An imposed sanction "should be molded to serve the prophylactic, punitive, and remedial rationale underlying the spoliation doctrine."[74] Some courts require the finding of an element of fault in order to impose sanctions,[75] others follow the rule of law "omnia presumuntur contra spoliatorem: that spoliation should not benefit from the wrongdoing whether it was intentional or not."[78]

One example of a sanction for spoliation is cost sanctions for recovering data. A court may require the company at fault to pay the costs for recovering the deleted evidence. The court award for sanctions can require the company failing to obey the order, or the attorney advising that company, or both, to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the court finds that the failure was substantially justified or that other circumstances make an award of expenses unjust." [77] Or the court may increase the amount of data discoverable and require the company to produce even more data.

Often, courts will award remedies in addition to cost sanctions. If the date requested cannot be located and the requesting party is prejudiced or injured in some way then the court will fashion an appropriate remedy for the situation. Examples of some remedies available under the Rule of Discovery include monetary penalties, the exclusion of evidence, adverse jury instructions, dismissal or default judgment, and potential criminal

penalties. [78] Courts have also included monetary sanctions in the form of reasonable fees and costs incurred by reason of a company's discovery failures in addition to an adverse instruction at trial. [79]

Because the imposition of a sanction for discovery abuse can be disastrous for the responding company, courts will often consider factors regarding the company's retention policy to determine whether it was imposed with the intention of destroying documents. For instance, there is a "three-factor test for evaluating documents retention policies: (1) whether the document retention policy is reasonable considering the facts and circumstances surrounding the relevant documents, (2) whether lawsuits related to the documents have been filed, and (3) whether the document retention policy was instituted in bad faith." [80] Many courts have imposed a similar three part test when determining the extent of sanctions which is "(1) whether there existed a duty to preserve the evidence; (2) whether the alleged spoliator breached that duty, either negligently or intentionally; and (3) whether the spoliation prejudiced the nonspoliator." [81] Overall, it is wholly within the discretion of the court whether or not to impose sanctions on the company and generally the court will consider the facts of each case to determine whether the company acted negligently or intentionally and whether the missing discovery will prejudice the requesting party. [82]

Historically, courts dealing with electronic discovery and spoliation were incongruent which led to a lack of uniformity with regard to retention policies and how a company can know how to avoid a spoliation penalty. Overall, without a uniform rule it was up to each court's discretion as to whether the retention policies were reasonable and whether to impose sanctions for spoliation.

The New Federal Rules of Civil Procedure sought to provide more uniformity and congruity within the federal court system by providing rules for spoliation, namely with a new provision which would provide a safe harbor for discovery issues. The new "safe harbor" applies to companies who destroy evidence through routine operation. Essentially the new rule establishes a standard that companies cannot be sanctioned for routine spoliation of material that was not reasonably accessible [83] and provides a requirement that only accessible material be discoverable. [84] This establishes a two-tiered approach to electronic discovery. If no court imposed preservation order was in effect and "(1) the party took reasonable steps to preserve the information after it knew or should have known that the information was discoverable in the action, and (2) the failure resulted from the loss of information because of the routine operation of the party's electronic information system" then the party would not be sanctioned for spoliation.[85] If a court has already entered an order preventing destruction of documents then the safe harbor provision will not apply. Therefore, the safe harbor rule provides protection for companies who conduct spoliation if no protection order was entered and the electronic discovery was reasonably inaccessible.

## VI. SUGGESTIONS

Many companies today have a mixed data environment wherein both paper data and electronic data are commonly used. One issue with document and data management is whether to maintain two separate systems. It is often difficult to know when looking at a hard data file whether there is electronic data located elsewhere within the offices unless a notation is made revealing same. One solution to a mixed data environment would be to use a document imaging system to convert all hard data into an electronic format therefore

maintaining consistency in either location. Unfortunately, if the documents are kept in electronic format then all of the issues in this paper must be considered with regard to retrieval production and destruction. Additionally, converting all of the corporate electronic form is likely to be prohibitively expensive and time consuming. Another option is to convert all electronic data into hard or paper data at the conclusion of a project. While this too is time consuming, it is less expensive on the front end but more expensive with regard to document storage and/or organization.

To set up a document management system, a business should create a document management plan, implement the plan, and enforce the plan. To create a document management plan, a company should identify the type of documents it generates, determine the best method to store those documents, determine how to simplify retrieval of documents, and maintain the integrity and security of the documents. Once these issues are resolved, the company has plan. The next step is to record the plan in a written policy and provide it to the employees for implementation. Any one who has access or use of documents or electronic data within the organization should be required to follow the plan and same should be enforced by periodic review of the process. Two (2) sample document and data retention plans are attached hereto (Addendums A and B) as merely a guideline to assist you in the development of your plan.

Should a company find itself involved in the electronic discovery process, there are several ways to protect itself. First and foremost, contact should be immediately made to legal counsel (whether in house or outside) to assist in identifying the electronic data and/or documents responsive to a subject issue or request. Focus must be turned to preventive maintenance to insure electronic data is not lost or destroyed from the first

notice of inquiry into same, including issuance of a litigation hold letter (Addendum C). A plan should be developed for a production protocol. Be prepared to explain the document and data plan to legal counsel, to identify the key contacts within company to assist counsel in identifying, preserving, reviewing and producing the documents. It would also be helpful to identify an individual within the company who is familiar with the operating systems, software and hardware in use, back up schedules and segregation of data, so that any questions from the lawyers, or from witnesses to whom deposition notices are issued, can be answered quickly and with accuracy.

Attached is a glossary (Addendum F) to assist with terms that may be of importance when preparing the document management plan. Additionally, should the company find itself in a situation where production is necessary, either as a third party or as a party to litigation, there are entities that can assist with document review including privileges screen and duplicate removal. An attachment hereto (Addendum D) lists various entities that are known to provide this service.

Finally, there are software programs that provide scrubbing services such that a document containing metadata cannot accidentally be sent from within the system to a computer outside the system. Specifically, an alert and scrubbing system will identify to the user a document containing Metadata to be sent and will require the user to actively opt to send the document clean or unclean. A list of the programs known is attached hereto as Addendum E.

## VII. CONCLUSION

The law of electronic discovery is only now *beginning* to develop, and will continue to develop for quite some time. As such, it is not only important that professional firms

gain an understanding of electronic information, but must also remain cognizant of the changes that will occur within the area of electronic discovery. Doing so will help relieve some of the tension and expense brought on in the event of litigation, which is an already difficult, stressful, and at times expensive process.

## Sample: Document Retention Policy

The corporate records of ACME, INC. and its subsidiaries (hereafter the "Company") are important assets. Corporate records include essentially all records you produce as an employee, whether paper or electronic. A record may be as obvious as a memorandum, an e-mail, a contract or a case study, or something not as obvious, such as a computerized desk calendar, an appointment book or an expense record.

The law requires the Company to maintain certain types of corporate records, usually for a specified period of time. Failure to retain those records for those minimum periods could subject you and the Company to penalties and fines, cause the loss of rights, obstruct justice, spoil potential evidence in a lawsuit, place the Company in contempt of court, or seriously disadvantage the Company in litigation.

The Company expect all employees to fully comply with any published records retention or destruction policies and schedules, provided that all employees should note the following general exception to any stated destruction schedule: If you believe, or the Company informs you, that Company records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until the Legal Department determines the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that exception may apply, or have any question regarding the possible applicability of that exception, please contact the Legal Department.

From time to time the Company establishes retention or destruction policies or schedules for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management. Several categories of documents that bear special consideration are identified below. While minimum retention periods are suggested, the retention of the documents identified below and of documents not included in the identified categories should be determined primarily by the application of the general guidelines affecting document retention identified above, as well as any other pertinent factors.

(a) Tax Records. Tax records include, but may not be limited to, documents concerning payroll, expenses, proof of deductions, business costs, accounting procedures, and other documents concerning the Company's revenues. Tax records should be retained for at least six years from the date of filing the applicable return.

(b) Employment Records/Personnel Records. State and federal statutes require the Company to keep certain recruitment, employment and

personnel information. The Company should also keep personnel files that reflect performance reviews and any complaints brought against the Company or individual employees under applicable state and federal statutes. The Company should also keep all final memoranda and correspondence reflecting performance reviews and actions taken by or against personnel in the employee's personnel file. Employment and personnel records should be retained for six years.

(c) Board and Board Committee Materials. Meeting minutes should be retained in perpetuity in the Company's minute book. A clean copy of all Board and Board Committee materials should be kept for no less than three years by the Company.

(d) Press Releases/Public Filings. The Company should retain permanent copies of all press releases and publicly filed documents under the theory that the Company should have its own copy to test the accuracy of any document a member of the public can theoretically produce against that Company.

(e) Legal Files. Legal counsel should be consulted to determine the retention period of particular documents, but legal documents should generally be maintained for a period of ten years.

(f) Marketing and Sales Documents. The Company should keep final copies of marketing and sales documents for the same period of time it keeps other corporate files, generally three years. An exception to the three-year policy may be sales invoices, contracts, leases, licenses and other legal documentation. These documents should be kept for least three years beyond the life of the agreement.

(g) Development/Intellectual Property and Trade Secrets. Development documents are often subject to intellectual property protection in their final form (e.g., patents and copyrights). The documents detailing the development process are often also of value to the Company and are protected as a trade secret where the Company:

(i) derives independent economic value from the secrecy of the information; and

(ii) the Company has taken affirmative steps to keep the information confidential.

The Company should keep all documents designated as containing trade secret information for at least the life of the trade secret.

(h) Contracts. Final, execution copies of all contracts entered into by the Company should be retained. The Company should retain copies of the final contracts for at least three years beyond the life of the agreement, and longer in the case of publicly filed contracts.

(i) Electronic Mail. E-mail that needs to be saved should be either:

(i) printed in hard copy and kept in the appropriate file; or
(ii) downloaded to a computer file and kept electronically or on disk as a separate file.

The retention period depends upon the subject matter of the e-mail, as covered elsewhere in this policy.

Failure to comply with this Document Retention Policy may result in punitive action against the employee, including suspension or termination. Questions about this police should be referred to John Doe (555-555-5555; jdoe@acme.com), who is in charge of administering, enforcing and updating this policy.

READ, UNDERSTOOD, AND AGREED:

_____ _____

Employee's Signature Employee's Signature

Date : _____

Excerpt from: The A-B-C's Of E-Data: A Discussion Related to the Issues Raised by Electronic Information, by Jannea S. Rogers, Esq.