



The Art of War

Thoughts on a Strategic Approach to Addressing Electronic Discovery

**By Samuel H. Solomon
February 2007**

DOAR
170 Earle Avenue
Lynbrook, NY 11563

sam@doar.com

Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.

Sun Tzu (The Art of War)

Abstract:

Electronic evidence transcends traditional discovery techniques to a whole new appreciation of your firms and your opponent's information resources and their value to understanding business and litigation risk management. The author addresses critical planning issues and new developments in this expanding litigation arena. This paper presents the issues from a corporate management as well as a litigator's perspective.

Overview:

With over 90 percent of all business records being originated in electronic form and at least 30 percent of corporate records kept *only* in electronic form¹, the entire field of electronic evidence and discovery is rapidly becoming the focal point of interest and concern among corporations and their counsel. A simple search using www.google.com (in itself a great tool for on-line research during discovery) reveals that the words "electronic evidence" provide for over one million "hits". This result reflects the extraordinary growth of interest and resources devoted to this burgeoning field. If one adds the word "discovery" to narrow the search, we still produce over 182,000 hits for further investigation.

Electronic evidence, as might be theorized by the ancient Chinese philosopher, Sun Tzu, is either your enemy or your friend and this choice has everything to do with the "attitude" of the combatants. Two millenniums ago he stated: *"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."* In other words, the true Art of War (which is the title of his classic treatise), as articulated by Sun Tzu and practiced by corporate and military strategists world-wide, is to identify and utilize your enemies weaknesses as your strengths. Nowhere is this truer then in today's information economy where the competitive advantage between firms is as much in the knowledge as the product one produces. Knowledge springs from information and experience, and information is the source of your opponents' true strengths and weaknesses. In fact, if the truth were known, it is the source of your core strengths and critical weaknesses, as well.

What is fascinating is that knowledge and insight into your information resources is the real source of strength not just the information itself. This is a significant shift in thinking by corporations who thought that its company data was its natural resource – only now realizing that knowing what they have is just as important. This is analogous to a general in the army who realizes that his strength is not just in having arms and people to execute a military objective. Instead, his strength is in understanding the quality, quantity and location of the resources as his disposal. It is with this in mind that our article explores three fundamental strategies that are critical to probing and addressing your opponents' weaknesses as you assess and "take ownership of" your own resilience and frailty.

If you don't have a competitive advantage, don't compete.

The new Federal Rules of Civil Procedure that were just adopted codifies this need for knowledge as the critical success factor in this new art form. Meet and confer, sampling and safe harbor all point to the need to know what you have in your corporate infrastructure before proceeding to either make demands for production or in response to the demanding party. The overarching goal is to preserve broadly and produce narrowly – but this can only be accomplished if you can negotiate from a position of knowledge of what you have or what you need. Overall broad, poorly documented or articulated requests are being viewed by most courts as a negative stigma on the party who engages in this type of behavior. Exaggerated claims of undue burden and cost are just as damaging given the increased sophistication of today's judges and special masters. Accurate assessment of what a corporate client has along with a determination of the opponent's capabilities is the defining characteristic of success in today's discovery environment. And under FRCP, this knowledge is to be ascertained and shared early in the litigation process. Sun Tzu could have easily been a commentator to the FRCP rules committee!

Let us focus on three key developments that make the cogent argument for attorneys and in-house counsel to craft an approach beyond tactical or technical plans in order to address the long-term threats and opportunities that the field of electronic evidence offers. These central strategic issues *are corporate buy-in, reflective risk assessment and discovery scope*. These strategic issues transcend any particular concern regarding technical considerations such as file formats, electronic mail systems or “locking down” hard drives; though as tactics they are important and will be addressed in a future article. The entire discipline begs for a strategic vision and an overriding business approach to electronic information discovery and, in this paper, we will outline appropriate core business concepts to be considered prior to discovery; in fact, even prior to filing suit.

Corporate Buy-in

Attack where they are not prepared, go out to where they do not expect.

Electronic discovery may be a corporate opportunity. Why do we say this? With all the panic encouraged by industry pundits, players and vendors, how can we say there are long-term opportunities and not just threats to the explosion of interest in electronic evidence discovery? This seems inconsistent with the popular literature that typically focuses on disasters looming on the horizon for those who ignore electronic evidence issues². No doubt the threats are real, however, to paraphrase an old expression: *one firm's threat is another firm's opportunity*.

In many ways, one's attitude regarding electronic evidence reflects how one sees competition or any other “threat” to one's business – some firm cultures are defensive to a competitive threat and some are responsive, ingenious and proactive. For example, companies have formed “competitive intelligence working groups” that engage in legal gathering activities and integrate the results into their product and marketing plans. In some cases, this group reports to very high levels within the organization. Firms advocating this approach see competition as a healthy and

necessary part of their business planning strategy and operate accordingly. *It is our belief that a similar attitude is necessary in order to deal with electronic information gathering as it relates to a firm's involvement in any form of legal practice or litigation risk assessment.* It is the author's suggestion that an "electronic evidence working group" be initiated within corporate counsel to create an interdisciplinary team of attorneys (in-house and outside), information technology professionals and senior policy makers for the firm in an effort to treat electronic information as an internal resource and corporate opportunity. With some firms, this may even be a natural outgrowth of strategies meant to understand and enhance firm-wide Information Resource Management (IRM) and planning.

Let's step this up a notch. Since electronic discovery has transformed a company's information resources into a risk management challenge, these risks and associated controls must become part of the assessment of outside directors, especially those on the audit committee as well as the senior financial executives of the firm. Though Sarbanes-Oxley is now being hotly debated, the bottom line is that senior executives are being held liability in civil and criminal proceedings for their failure to establish and oversee effective internal controls that potentially generate a material risk for the corporation. Corporate buy-in is essential for an appropriate level of insight and monitoring.

A discovery production request should not come as a surprise to either in-house counsel or the law firm supporting them. In fact, part of the working group's responsibility would be to audit outside counsels skills in addressing such requests. Once served with a production request, it is really a "deer in headlights" situation unless the law firm has specific expertise in this area. From a law firms perspective, expertise in electronic evidence strategies is a significant marketing tool in developing and working with their clients. In other words, with corporations already cognizant of their information resources issues, these prospects or clients would appreciate a law firm with sensitivity to their needs as it pertains to electronic information and discovery.

The current and appropriate concern by in-house counsel is to the escalating and unacceptable costs in responding to discovery requests both in terms of production processing and legal services. As long as law firms employ traditional approaches to address a completely redefined set of problems presented by electronic discovery, outside counsel will be out of synch with the needs of the corporation. With the FRCP and resulting court rulings, new policies and technologies will be required to alter the way law firms manage the scale of corporate information resources. This shift will also demand from in-house that the focus of their efforts will be strategic and not just about tactical issues surrounding production and costs.

A poorly designed and integrated strategic plan has a significant potential penalty as it may lead to charges of spoliation. Recent and highly publicized, though not necessarily unique matters, such as Zubelake and Morgan Stanley demonstrate that spoliation has an enormous impact on the course of legal proceedings and ultimately, trial. The National Law Journal, in a recent article focused on this topic, states: "The vast majority of jurisdictions in the United States have long followed the common law rule that 'the trier of fact may draw an inference from the intentional spoliation of evidence that the destroyed evidence would have been unfavorable to the party that destroyed it.'" *Beers v. Vayliner Marine Corp*, 236 Conn. 769, 775 (1996). Or, put another way by the Connecticut Supreme Court: 'omnia praesumuntur contra spoliatores' – all things are

presumed against the despoiler.”³ The courts have been very stern with firms accused of spoliation with penalties ranging from sanctions and striking of pleadings to ominous jury charges. In addition, the courts are unreceptive to the presumption that destroyed evidence is not relevant to the matter. In *Sage Realty Corp v. Proskauer Rose LLP*, 713 N.Y.S.2d. 155 (2000), the court refers to the relevance claim and states: “The sheer effrontery of this claim...is amazing.”

The key to spoliation, however, is that there be “an obligation to preserve [evidence] at the time it was destroyed” and also a culpable state of mind (*Byrne v. Town of Cromwell Public Schools*, 243 F.3d 93 (2d Cir 2001)). The decision left to the individual court is the definition of “culpable state of mind”, with the spoliator having a potential burden of acting intentionally, in bad faith or, with a lower burden, gross negligence. Under the gross negligence standard, if the party knew or should have known the retention policy for these documents at the time they were destroyed, it would be construed as a culpable state of mind. Finally, there are documents that have clear retention statuses, such as tax information and then there is the retention of general business records that is based upon customary industry practice. Here the court has enormous leeway in defining whether or not a gross negligence standard applies.

Where this leaves us is to better understand the process by which electronic documents could be destroyed. In the old world of paper and paper archival, destroying these physical records “accidentally” would be difficult since retention policies are well known (for example, a seven-year rule for IRS related financial documents) and the process of destruction would raise eyebrows at the minimum. Besides having clearer rules for document retention, the other protection is that someone who is familiar with corporate retention policies as well as the statutory standards typically manages and controls this hardcopy archive.

In contrast, electronic information, for which there may not even be a hardcopy backup, suffers from a number of key deficiencies that requires diligence on the part of the corporate policy makers. The first is that retention policies on electronic backups are more ambiguous and, worse, are set by IT professionals without the expertise in legal retention issues. IT professionals may be very familiar with technical backup policies, such as tape “rotation cycles”, since that is the focus of most back-up applications: to ensure that if computer storage “crashes” there is a copy of the information. Backing-up drives for contingency purposes is not related to the retention policies needed to observe Federal and State preservation statuses or legal evidentiary requirements for business records. Backup and retention are completely different issues – yet they are often confused. Standard procedures are to backup storage everyday and to rotate (in other words, overwrite the backup tapes) every 30 to 90 days. From an IT perspective, this is fine backup policy, however, under this scenario, we would have a guaranteed spoliation issue if these business records had statutory retention requirements and the corporation “should have known”, therefore was grossly negligent. For ordinary business records the gross negligence risk may be just as serious.

Confusing backup versus retention becomes the battleground between the potential threat and the possible opportunity. As a threat, it is incumbent that the “electronic evidence working group” collaborate with the team responsible for traditional records retention, to review IT’s tape retention policy⁴ and either: change the rotation cycles to comply with the record retention rules;

or, create digital copies specifically for the purpose of retention, not backup. This policy must extend beyond mainframe information systems (such as personnel and accounting data) to the information stored on the numerous servers within a company, and in some cases, individual computers of employees with access to, or the authority to develop, electronic information in need of retention.

Just as in physical document discovery, the courts are careful not to allow an unreasonable burden of discovery by an overly broad discovery request. It is important that electronic evidence requests be broad enough to get at the evidence and yet focused so as not to be stricken for their broadness. One would also ask the court to interpret the burden as a gross negligence standard. The best chance of finding defective retention implementations is on departmental servers as well as individual personal computers and laptops since policies and procedures may be relaxed or even ignored.

Spoliation aside, corporate adoption and buy-in is not just about risk and costs, it also makes good business sense. And it is very hard to move to the other points in this article without a good basis in one's business environment. Part of the problem is that it is quite unlikely that being successful in this area will lead one on the path of one day attaining the CEO mantle at a firm. That should not negate, however, the need for the Board of Directors to take special note of the business opportunities, risks and exposure reflected in this emerging area of corporate asset management.

Reflective Risk Assessment

If you know the enemy and know yourself, your victory will not stand in doubt.

Reflective Risk Assessment is a new and critical discipline of "introspection" that should be part of the overall decision whether or not to pursue litigation or in anticipation of a lawsuit. With electronic evidence one is presented with a unique opportunity not affordable or efficient in the world of hardcopy documents. For Sun Tzu, knowing yourself is as important as knowing your enemy -- combined you are superior in battle. This can best be explained by example. In patent litigation where the aggrieved party is about to engage in a lawsuit to protect its rights, implementing Reflective Risk Assessment on their own electronic information resources would be utilized to determine landmines and "bad docs" that would be part of the potential discovery population. By utilizing advanced clustering and analytical tools, a very "rough cut" of potentially harmful documents from the suing party's own electronic files are highlighted for review and risk assessment.

A number of decisions may result from this assessment:

1. Understanding the risk exposure of important trade secrets or damaging documents that significantly helps the defense, thereby making this litigation too risky or expensive.
2. That the claims should be refined to avoid potential pitfalls during the discovery process.
3. In some cases, *the devil you know is better than the devil you don't*. Knowing the

potential damaging electronic information and messages already puts you in a superior position when it comes to dealing with this during depositions and trial.

The key to making this a practical and economical analysis is to follow the basic rule that this is a “screening” process rather than a detailed investigation. Search engine tools exist that understand complex relationships between concepts and word clusters far beyond simple word searches. For example, the word “violation” in itself may be benign if that word is used in technical documentation to explain an incorrectly wired circuit. It takes on an entirely different meaning when it is coupled with the word “standard” and “industry” and where one of the addressees of the memo is the head of safety for the manufacturing organization. “Data mining” experts (no different than people who know how to “look” for gold buried deep in the desert) utilize advanced software tools that create reports outlining the offending documents and their relationship within the organization as well as the document universe.⁵

Utilizing this “twenty thousand foot view” of the potential risk, the documents are reviewed in a number of ways, including checking “high probability” offending documents based upon an analysis of the probability of “bad content”, an analysis and statistical distribution of bad language occurrences, or a listing of the offending language with a specified number of sentences displayed before and after the offending language. In addition, the software may print out communicating relationships between parties that may lead to further investigation, such as subject material being exchanged between the CEO and head of research.

Of course, this very summary view of the content can also be utilized as a first pass analysis of documents being produced by the other side in order to determine “parallel” disclosures to what was uncovered in your firm’s material. Finally, in reviewing the other side’s material, one could use statistical analysis to demonstrate to the court the need for future electronic discovery due to “footprints” of potential offensive documents in the summary analysis.

A recent article written by Anne Kershaw, Esq., “When Less is More”⁶ suggests that new tools, the FRCP and thinking about what a company has produced a fundamental change in one’s negotiation strategy by coming equipped to discuss meaningful approaches to discovery based upon a very narrowing of the request. The contention is that this demand to narrow scope can only be accomplished if one investigates very early on what the company really has and to point opposing counsel to the most relevant and accessible information resources. The thought on our part is counsel’s entire approach to discovery needs to be reconsidered in the light of electronic stored information and the FRCP. Traditional subterfuge and misdirection of opposing counsel regarding discovery is now a (really) bad practice. Investigation and communication with opposing counsel is how one narrows discovery and reduces the cost and intrusion of litigation.

Discovery Scope

Don't attack walled cities.

What is really out there to be “discovered”? Are we flying blind or is there a real understanding as to the scope of the information resources of the other side’s IT infrastructure? How do we craft discovery requests that will stand up to the judicial standard of *proportionality* and not be construed as prohibitively expensive or too broad? This leads us to our last strategic issue that of

defining scope as early as possible during the discovery process. As Sun Tzu observed, one should know what one is attacking thereby avoiding unnecessary difficulties or even refraining from the attack altogether.

Defining scope requires knowledge and understanding along a number of dimensions:

1. What is the scope of electronic information processing and storage systems within the target company?
2. What types of information structures that capture and store information should we be investigating?
3. What does the nature of the specific litigation engagement require in terms of information that may be important?

“Meet and confer,” though always a good practice by litigators, has taken on a more strident and critical role in discovery. It is to be performed early and with an eye towards authentic and accurate disclosure. Though there will be gamesmanship in this process, the ground rules are becoming clear: you need to be incredibly prepared with the knowledge of what you have before you enter that room. Footnoted is just one example of the questions being requested by parties to this discovery meeting.⁷

Each of these concepts is important to elucidate. The first relates to investing in an early investigation of the target’s information technology infrastructure. This may be accomplished at the summary level via Internet searches, review of annual reports, and even speeches and publications of IT professionals from the firm (this can be found often on the web or even a company PR publication!). Sometimes companies such as IDC and The Gartner Group have profiled the IT structure of this particular firm. The next step, however, is more critical and that is to conduct 30(b)(6) depositions of senior IT representatives with knowledge of their systems at the corporate and departmental level. For example, it may be necessary to depose both the corporate IT guru and the divisional/departmental IT manager to gain a full appreciation of where the information you need resides.⁸ This is a new direction for investigation not typically encountered in the non-electronic discovery era.

The second and third items are somewhat related. Once there is an understanding of the technology employed by the firm, one needs to consider, depending upon the type of case, where the information would most likely reside. This does not mean you should not ask for the world, but you want to make sure that the real “stuff” is detailed enough to survive judicial review. For example, if the case involves invoices, then you know that the accounting system and its department components are most critical. If it is a product design issue, then CAD/CAM drawings may be very important. This is where you should then focus your investigation. At the end of this article, the author outlines various forms of electronic data; engaging an electronic information expert in a review of the litigation claims will help determine where and how one should focus the production.

Scoping has other strategic values for the firm seeking the information. For example, it is common for the target company to assert some form of privilege. However, if the information is “generally available” without secured access – such as being accessible via a web browser or a

departmental server in an unsecured room, then privilege may have been effectively waived. One needs to be probing the privilege issue early and many times the IT professionals being deposed will not be attuned to this and will offer important information to be later presented to the court during a hearing that will deal with privilege.

The best way to understand the scoping process is to engage in such an assessment of your own IT organization. This inward perspective is important to better understand your technology landscape for risk management as well as educating relevant parties as to the issues surrounding scope and exposure. It is common to engage an outside professional to assist in defining the scoping interviews and analysis since it is, frankly, hard to be objective in this type of endeavor when one is personally involved.

Conclusion

Electronic information discovery is a strategic as well as tactical issue for corporations and the law firms that represent them. It does not have to create panic, however, since there is a real opportunity for those firms that have a culture to invest in “competitive” initiatives. Creating a working group to deal with these issues is the first step. It needs to be at a high enough level within the company to get the attention and accountability it requires for success. Understanding your retention policies, being introspective as to your information risks and investigating the scope of your firm’s information resources are great places to start along the path of education and awareness. New analytical software is being created to address the problems associated with the internet and messaging technologies, such as email, which have forever altered the face of corporate communications. The author is certain that over time, attention to this area of information resources within the firm will be a significant corporate advantage -- not just as a protective measure against lawsuits, but to be used for legitimate proactive business litigation and protection of the valuable information assets. In today’s “information economy” what could be more appropriate?

Overview of Electronic Evidence

Nor can one march through a country without knowing its mountains and forests, all the dangers and difficulties of the route and marshes. Sun Tzu

Author's Note: The following overview is reprinted with permission from "Discovery of Electronic Data: Basics, Burdens, and Costs"; Written and presented by Charles R. Kellner, Electronic Evidence Discovery, Inc., kellner@eedinc.com.; at the forty ninth annual meeting of the Seventh Circuit Bar Association; May 2, 2000. © 2000 Electronic Evidence Discovery, Inc

I. THE BASICS

A. Paper v. Electronic Data

There are notable differences between discovering paper and electronic data. Significant among them are:

The electronic version of data is qualitatively different and richer than its paper representation.⁹ It may contain multiple drafts and versions, and information about the author of each. It may disclose relationships and formulae which paper cannot. The electronic version of e-mail discloses information about transmission and distribution more precisely than paper prints. With proper planning or support, a party can full-text search and analyze large volumes of electronic data much more effectively than a similar volume of paper. Even where paper summaries or prints are available, a requesting party may be entitled to underlying electronic data for manipulation, search, and analysis.¹⁰

In many business organizations, between 20% and 80% of documents have never been printed.¹¹ Without electronic discovery, a requesting party will miss documents important to its case, particularly drafts, databases, and e-mail discussions. Without a thorough search of its electronic data, a party cannot accurately comply with duties to disclose or respond.

E-mail, in particular, holds a particularly rich chronological and contextual history in ways that paper prints and reports do not. Because of its casual and conversational origin and its misperceived veil of privacy, it has particular credibility as an author's true impression.

B. Commonly Requested Electronic Data

Databases: Databases often hold the core knowledge of a business organization. They contain information about customers, production, performance, transactions, prices, competition, and proprietary internal processes or formulae. These include financial and accounting system databases. They may be transactional and ever-changing or, as

knowledge management tools, incrementally recording growth and progress. The hardest-fought discovery battles usually involve databases that reside on large servers with complex software and operating systems. Many can be copied and produced outright, but parties usually agree to “dump” or “report” various relevant portions in a way that a discovering party can use. Despite the real or apparent complexity, courts often require the production of whole databases, or large portions of them, as the only useful source of financial, transactional, or historical data.¹³

Electronic Mail: Rich in content, context, and chronological detail, e-mail is the most widely requested form of electronic discovery. Finding and producing it presents challenges to corporate IT departments. First, most e-mail systems have some kind of proprietary format that combines messages and attachments into a format not widely usable outside the native software. Second, e-mail systems often combine mail from dozens or hundreds of users into large “post office” databases. These databases require extra steps to extract individual users’ mail from backup tapes. Third, many service bureaus routinely restore, convert, or search e-mail. Most corporate IT departments, while technically capable of doing the same, are scaled for ongoing operations and rare disaster recovery incidents. They have few available resources or computers for litigation e-mail projects.

Word Processing and Presentation Files: Most often created by individual users or small groups, these are very targetable and useful to discovering parties. They contain edit, control, and version histories not found in paper. They may be easily searched with full-text search engines. They can often make shorter work in review than their paper counterparts. Along with spreadsheets, they are consistently among the easiest formats to identify copy and produce from desktops, disks, servers and backup tapes.

Spreadsheets: Spreadsheets may be the output of a single user or work group, or they may be a complex “data dump” or formatted report from a financial or transactional database. They differ substantially from their paper counterparts in that the electronic versions reveal the formulae of their computations. They may also reveal direct electronic links to the underlying raw data. Printed spreadsheets may contain “hidden” columns or other data outside a specified print range.

CAD / CAM / CAE and Graphics: Business use of computer-assisted design and engineering software has eclipsed reliance on printed blueprints and specifications. Highly relevant in construction, manufacturing, chemical and electronic engineering, these electronic files, in their many versions and iterations, are rarely printed except in circumstances of final or approved designs. They are usually problematic to restore or operate without the specific software and graphics utilities used to create them.

Personnel Records: Corporate HR managers usually keep paper files of official records. However, word processing copies and drafts tend to abound on desktops, laptops, servers, backup tapes, and attached to e-mail. As such, they provide rich context to the final or official paper record.

Policy and Procedure Manuals: Formerly relegated to binders on credenzas and filing cabinets, manuals of all kinds are more widely available for common use on servers, Internet and intranet sites, and on CD disks. They are most often in word processing, HTML, or PDF image format, and as such, are amenable to full-text search and comparison to previous versions.

Software and Source Code: Among the most valuable proprietary information or intellectual property, these electronic files are among the most sensitive for litigants to disclose or produce. Software and source code may apply to website design, software or hardware product, or proprietary process. It may be reasonable for attorneys to agree to inspect, with experts if necessary, for sensitive or relevant materials, and then determine the scope of production.¹⁴

Internet and Intranet Content: These items consist of the words, graphics, and parts of the source code behind internal and publicly accessible web sites. They are often created in text, HTML and simple graphic formats, and are relatively easy to copy, produce and analyze.

Internet Service Providers: ISPs provide Internet access, e-mail service, message storage, web site hosting, chat, and other real-time communications services. With appropriate process, usually as a non-party respondent, an ISP may provide copies of messages, chat, discussion threads, or web site content stored on its servers. It may be able to produce logs of Internet activity. However, because of volume and transaction speeds, most ISPs save activity logs for a very short duration, perhaps only hours.

Fax Servers: Most faxes begin as word processing documents. The fax machine converts the word processing file or paper document to a graphic format for printing by the intended recipient. In high-volume fax operations, the graphic may be stored on a server, waiting for an open line. It may also be backed up to tape. A stored fax and its associated log often contains information about sender, recipient, date and time.

Personal Digital Assistants (PDA): Hand-held devices create documents, store databases, manage calendars and contacts, send and receive e-mail, and access the Internet. For purposes of discovery, these capabilities put PDAs into the same category as desktops and laptops. Their space and memory are limited, and their file formats are usually proprietary. With appropriate utilities, however, they can “dump” or “report” their contents.

Telephone, Security, and Network Activity Systems: Litigants seek data from telephone and security systems most often to establish a chronology. Who spoke to whom, and at what time? Who entered or left what area at what time? These may correlate to other “electronic” activities that may be detectable and relevant, such as transmission of e-mail, copy of a proprietary file, or print of a particular list.

Cell Phones, Pagers, and Service Providers: As with the above telephone, network, PDA, and ISP services, these devices, networks, and service providers may store and supply relevant data not available elsewhere.

Voice and Video Mail: As voice mail has converted from analog to digital format, many business organizations have found themselves with hundreds of hours of voice mail stored on servers, and even backed up to tape. Servers and tape similarly record and store the contents of video mail and conferences.

C. Common Sources of Electronic Data

The following identifies sources of electronic data created by computer users, exclusive of software or other files which are present to make the devices operate.

Business or home desktop or laptop computer: Files created by users are stored on hard drives. For most up-to-date computers and hard drives, a technician can copy user files to a network or backup device in anywhere from a few minutes to an hour or two.

“Deleted” Files and “Slack Space”: When a user deletes a file or message, only the file or message listing disappears. The content of the file or message usually remains on the hard drive until overwritten by new data.

Deleted files and file fragments are recoverable in a number of ways. Computer forensic experts usually make a bit-by-bit “disk image”, an exact replica of every bit of information on a hard drive. To preserve the integrity of the computer in question, they restore the image to a fresh computer to search the areas not occupied by active files.

“Slack space” refers to an area of a disk that is reserved by a file but not actually used for storing its data. Slack space may contain data from deleted files which has not been overwritten. Slack space and the data within it often “travels” with a file as it is copied from hard drive to disk to server to tape. A forensic expert often finds old, presumably deleted data in the slack space of files on new computers.

Proper disk imaging of an up-to-date computer may take several hours to a day. Restoration and analysis may take another day or longer, depending on the computer and the search requirements.

Business or personal diskettes, backup zip, jaz, and tape drives. These inexpensive storage media are sometimes fragile and time consuming, but not particularly difficult to read or copy

Network or departmental server, enterprise server, mail server, or proxy server. Servers may contain the collective contents and activity logs of dozens or hundreds of users. Depending on size and operating system, backup tape, and backup software, they may require a few hours to copy or backup to tape, and for some, several hours or a half day to restore a tape.

For purposes of discovery, active user files can be copied to tape in an attended process. A full server backup is rarely useful or required. Some backup tapes and systems require full restoration to examine contents. Some can be read and selectively restored more quickly.

Backup tape repository and recycling: By tradition over the last decade or so, most businesses back up their computer systems on an interval schedule, e.g., daily for a week, weekly for a month, monthly for a year, and then preserve annual tapes. They may store these tapes on site, or with off site service providers. Some percentages of the tapes themselves are always scheduled to be overwritten with newer backups.

The tapes in these libraries, each usually containing combination of desktop files, e-mail post offices, databases, and software, present a huge resources and risks for parties in litigation. The libraries may consist of hundreds or thousands of tapes, with or without external logs. They may contain files for which the business no longer owns systems or software. They contain the history of the organization, and as such, in near term likely contain information potentially relevant in litigation.

Many organizations now seek to reduce their tape stores only to that required for actual disaster recovery, and for compliance, litigation and business requirements. These programs are established within detailed and comprehensive paper document and electronic data records retention policies.

II. PRESERVATION, BURDEN, AND COST

While courts are encouraging parties to resolve discovery disputes on their own,¹⁵ parties are using electronic discovery to strategic and tactical advantage. Experienced counsel knows that a targeted and comprehensive electronic discovery request, with a preservation notice or order, will create an emergency with opposing counsel and clients.

A. Duty to Preserve:

The duty to preserve arises when the party possessing evidence has notice of its relevance. Spoliation, or failure to preserve, may result in sanctions, an adverse inference as to the contents of the evidence, or default judgment.¹⁶

Normal business backup and tape rotation procedures wipe out large volumes of data from previous weeks or months. Average users routinely delete drafts and empty their “recycle bins” on a daily basis. Just booting a normal Windows-based computer overwrites information from the previous day. Each of these activities results in the loss of data. At what point is it spoliation? At what point is the request to preserve tantamount to a request for TRO or injunction?

Responding parties are wise to act quickly with counsel, business managers, IT directors, opposing counsel, and the courts. The action required is

Swiftly to assess what electronic data is relevant, where it is, and what users are or may be affected, and

Reasonably to propose how to preserve data that the discovering party may require, while maintaining reasonably normal business and computer operations.

B. Burden of Preservation and Production

Litigants differing in financial wherewithal and intensity of use of computers may be required to shoulder proportional burden of cost and effort.¹⁷ The mere fact that the production of computerized data will result in a substantial expense is not a sufficient justification for imposing the costs of production on the requesting party. In addition to considering the amount of money involved, the courts may consider whether:

The expense and burden is greater to the requesting or responding party.
The responding party will benefit to some degree in producing the data
The technology required to effect production requires special cost or development.
The risk of having to use or make such technology is ordinary and foreseeable.¹⁸

The responding party is required to produce the data in a form that is usable and useful to the discovering party, either with or without sharing of cost.¹⁹ The law is clear that data in computerized form is discoverable even if paper hard copies of the information have been produced, and that the producing party can be required to design a computer program to extract the data from its computerized business records, subject to the court's discretion as to the allocation of costs.²⁰

Some courts have denied discovery in cases where the electronic information sought is highly duplicative of data otherwise available, even though inconvenient.²¹ Most cases turn on balancing the need of one party for the data in its requested form versus the hardship to the other to produce it.²²

<p>The author suggests that you also investigate The Sedona Working Group information on Electronic Discovery for contemporary information in this area: www.thesedonaconference.org</p>

FOOTNOTES

¹ Digital Discovery & e-Evidence , Pike and Fischer, December 2001.
http://www.pf.com/law_internet_digitaldisc.asp .

² As an example, see the online article: “Electronic Discovery: Introduction”, by Professor Charles Nesson, The Berkman Center for Internet and Society at The Harvard Law School, October 10, 2000. http://cyber.law.harvard.edu/digitaldiscovery/digdisc_library_10.html . Here is just one excerpt on the “threats”:

The Threat From a Company Viewpoint

A completely electronically networked company with all of its past and current data accessible online approaches the ideal of complete transparency in electronic discovery....This specter of near transparency to discovery is frightening to companies for several reasons. First, companies fear that they will be obliged by courts to expend the effort and pay the costs of making their data accessible, a task that is potentially overwhelming. Beyond the expense of locating and indexing their data, companies confront huge expense in making their data readable...Second; companies fear the decision of who will be allowed to do the discovery searches. If, as in traditional discovery process, the company’s lawyers do the search, the time and expense could be overwhelming. One could imagine a respondent company being required to open its system to the other side, inviting its litigation opponent to jack into its data world and search at their time and expense. For understandable reasons, no company of which I am aware has been willing to take this step, undoubtedly because giving a hostile litigant open access to a company’s entire information system would mean disclosure of current business plans, trade secrets, loss of attorney client privilege and invasions of privacy.

...Realistically companies will resist any surrender of control in the digital discovery process. If searches through their data are to be conducted, they will want to conduct them themselves, or have their agents conduct them. This means they must look to the courts to set limits on the scope and cost of what they can be required to do. The legal problem companies face is that there seem to be no definite bounds on digital discovery, no limits of subject, type, time, or expense. All forms of digital data are potentially discoverable, including any data compilations, according to the Federal Rules, “from which information can be obtained, translated if necessary by respondent through detection devices into reasonable readable form.” The fact, for example, that the senders or receivers of email may have “deleted” them, far from insulating them from discovery, may give reason to think that these email messages are a particularly important source to mine for admissible evidence. The fact that a computer may be used for personal as well as company business may give reason for care in conducting a discovery search but does not necessarily limit the scope of what can be searched.

³ “Spoliation by Oversight” by Michael Starr and Jordan Lippner, *The National Law Journal*, November 12, 2001.

⁴ For an excellent treatment of FRCP, I suggest Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167 (2006).

⁵ One such product is *Inference*. It employs advanced pattern matching technology (non-linear adaptive digital signal processing) to extract a document's digital essence and determine the characteristics that give the text meaning. Once identified and encoded the unique "signature" of the key concepts, Concept Agents are created to seek out similar ideas in websites, news feeds, email archives and other documents. Because it does not rely on key words, it can work with any language. The software architecture combines high-performance pattern-matching algorithms with sophisticated contextual analysis and concept extraction to automate the categorization and cross-referencing of information, improve the efficiency of information retrieval and enable the dynamic personalization of digital content. For more information, please refer to the website www.inferencedata.com and a demonstration of its data mining features may be found at <http://www.inferencedata.com/online-demo.htm>

⁶ Anne Kershaw, Esq., *When Less Becomes More: Making the Case for a Discovery Strategy*, *Digital Discovery & E-Evidence*, Pike & Fischer, Vol. 7, No. 1, January 2007.

⁷ Sample request in anticipation of a Meet & Confer:

Dear Counsel:

In anticipation of the requested meet and confer regarding electronic discovery and at the request of some of defense counsel, I have compiled a list of questions that we would seek to have answered about your electronic data production, specifically:

- (1) Regarding data collection, who is responsible for compiling the data for production and what is their function or role within your organization? Who is responsible for your data retention policies? Have you preserved all backup tapes since the commencement of litigation, and is there an inventory of such tapes? After the data is collected, how will it be stored and who maintains the chain of custody?
- (2) Identify each and every source from which the data will be collected. Specifically, will the data be collected from all possible sources, including but not limited to, network servers, shared drives, email servers, network share, hard drives, PCs, laptops, employees home computers, back-up tapes and PDA's?
- (3) How many network servers exist at your organization? For each server, please identify its physical location and function or role. Will each server be searched in connection with your organization's collection of data? If not, please identify the servers that will not be searched and explain why such servers were not included in the search.
- (4) Identify what system your organization and any subsidiary or affiliate organizations, utilize for email. Additionally, if your organization, or any subsidiary or affiliate organizations, use different email systems, please identify and correlate each email system with the proper entity, or divisions within the entity, that utilize each program.
- (5) Identify the email domain name for each Defendant.
- (6) List the most likely custodians of relevant electronic materials, including a brief description of each person's title and responsibilities.
- (7) Will your organization include the materials for each file collected?
- (8) Describe in detail your organization's electronic data back-up policy or protocol, the type of

media on which any such back-up information is stored, whether your organization utilizes full back-ups or an incremental back-up and the schedule that exists for your organization's back-ups. How and where is your organization's back-up media stored, and does your organization re-use said back-up media or otherwise recycle said back-up media?

(9) What is your organization's retention destruction policy for electronic documents and data, including, but not limited to, email files, electronic calendars, contact files, and any other electronic documents or data?

(10) Do you have reason to believe that any of your electronic documents are of limited accessibility (e.g, created or used by electronic media no longer in use or maintained in redundant electronic storage media)? What provisions have you made for collecting such materials?

(11) Do you reasonably anticipate any unique issues with respect to your electronic discovery?

Defendants have also proposed a set of search terms to utilize in their search for responsive documents and data, and have requested that Plaintiff comment on the same, and if necessary add to or supplement Defendants' list. While Plaintiff is willing to assist in focusing Defendants in their search, any such search terms proposed by either Defendants or Plaintiffs shall not constitute a waiver of any of Plaintiff's rights to request additional search terms, searches or discovery.

Additionally, we request that you provide samples prior to commencing the entire production in order that they may evaluate the format and compatibility of your electronic production. Finally, if your organization plans to produce any of the requested materials in a hard copy format, there is no reason to delay the production of such documents while your electronic production is underway, and as such I would request that you produce any hard copy documents as soon as practicable.

Should you have any questions regarding the above referenced information, please do not hesitate to contact me.

⁸ The author as developed an outline of questions to be asked during a 30(b)(6) deposition. You may contact him at sam@doar.com to discuss this further.

⁹ *Armstrong v. Executive Office of the President*, 821 F.Supp. 761 (D.D.C. 1993).

¹⁰ *Crown Life Insurance Company v. Craig*, 995 F.2d 1376 (7th Cir. 1993); *US v. Microsoft; New York v. Microsoft*, 1998 WL 699028 (D.D.C. 1998)

¹¹ This estimate is based on the writer's experience with paper and electronic data identified with the same specifications on the same cases. Note that the collection of paper is also dramatically on the rise, even as exclusively electronic data makes an increasingly greater percentage of the whole. Among many estimates, between 1996 and 2001, volume of office copy and laser print paper will increase from 1.5 trillion to 2.3 trillion. Between 1995 and 2005, percentages of documents printed will descend from 90% to 30%. "*Network, Screen and Page: The Future of*

Reading in a Digital Age” Electronic Document Systems Foundation, 1997. *Xerox Corp. 10-K*, December 31, 1998, <http://www.sec.gov/Archives/edgar/data/108772/0000108772-99-000009.txt>. “*Content Management Fact Book*”, International Data Corp., 1999.

¹² *Knox v. State of Indiana*, 93 F. 3d 1327 (7th Cir. 1996).

¹³ *Dunn v. Midwestern Indemnity* 88 F.R.D. 191 (S.D. Ohio 1980), where non-class plaintiff sought the insurer’s actuarial underwriting database as a potential source of identifying patterns of discrimination.

¹⁴ *Rates Technology, Inc. v. Elcotel* 118 F.R.D. 133 (M.D. Fla. 1987)

¹⁵ E.g., Local Rule 37 ND Ill. To curtail undue delay and expense in the administration of justice, this court shall hereafter refuse to hear any and all motions for discovery and production of documents under Rules 26 through 37 of the Federal Rules of Civil Procedure, unless the motion includes a statement (1) that after consultation in person or by telephone and good faith attempts to resolve differences they are unable to reach an accord, or (2) counsel's attempts to engage in such consultation were unsuccessful due to no fault of counsel's. Where the consultation occurred, this statement shall recite, in addition, the date, time, and place of such conference, and the names of all parties participating therein. Where counsel was unsuccessful in engaging in such consultation, the statement shall recite the efforts made by counsel to engage in consultation.

¹⁶ *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F.Supp. 1443 (C.D. Ca. 1984); *Applied Telematics Inc. v. Sprint*, 94-4603, 1996 Lexis 14053 (E.D. Pa. 1996)

¹⁷ *Sanders v. Levy, et al.* 558 F.2d 636 (2d Cir. 1976); op.cit. *Dunn v. Midwestern Indemnity*

¹⁸ *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526 (N.D. Ill. 1995); *Bills v. Kennecott Corp.* 108 F.R.D. 459 (D. Utah 1985)

¹⁹ *National Union Electric Corp. v. Matsushita Electric Industrial Co., Ltd.*, 494 F.Supp. 1257 (E.D. Pa. 1980); *Daewoo Electronics Co. v. United States*, 650 F.Supp. 1003 (C.I.T. 1986); *In re Air Crash Disaster*, 130 F.R.D. 634 (E.D.Mich. 1989)

²⁰ *Anti-Monopoly Inc. v. Hasbro*, 1995 WL 649934 (S.D.N.Y)

²¹ *Williams v. Owens-Illinois, Inc.*, 665 F. 2d 918 (9th Cir. 1982), cert. denied, 459 U.S. 971 (1982); *Torrington Co. v. United States*, 1992 WL 40699 (C.I.T.)

²² *Timken v. United States*, 11 C.I.T. 267, 659 F.Supp. 239 (1987) op. cit. *Daewoo; National Union*.