



The Impact of Electronic Data Discovery on the Corporation

By John H. Jessen and Kenneth R. Shear, Esquire

Electronic evidence has become a key focus of discovery in litigation in U.S. courts, and this development presents enormous problems for corporate counsel. Moreover, with changing discovery rules, rapid accumulation of electronic data, the growing and uncontrolled use of electronic mail and the increased use of sophisticated backup and archive systems, the problem will only intensify in the coming years.

Indeed, we are in the midst of a dramatic change in the discovery process, and those corporate counsels who are prepared to meet this challenge will find ways to turn this transition to their advantage. Those who ignore it do so at the risk of expensive, embarrassing and unproductive litigation experiences — not to mention the distinct possibility of devastating verdicts.

The Door Opens to Electronic Data Discovery

Only a few years ago, the majority of corporate data was stored and processed on large, expensive mainframe computers. The cost of obtaining processing time and expertise to deal with data from such systems was prohibitive in most litigation — or at least that was the perception. As a result of this and other factors discussed below, paper documents remained the preferred source of discovery by plaintiff's lawyers, who could rely on persistence, dedication and quick wits to cull useful information from the mountains of paper that were often produced.

This situation has changed dramatically in the past few years. The power of the personal computer has substantially increased, causing most corporations to downsize their mainframe operations onto networks of personal computers, and networked microcomputers within corporations now perform varied and important electronic data processing operations. Correspondingly, plaintiff's lawyers are beginning to realize that they, or specialized computer consultants, now have the power to process types and quantities of electronic data that were formerly unapproachable. The intimidating prospect of learning about, and gathering information from, a complex mainframe computer is greatly reduced today, as much corporate data processing is done on computers that are virtually identical to those used in the lawyer's office. Once their foot is in the door, plaintiff's

counsel often find that it is a much shorter and simpler step to an organization's electronic data than they may have thought while looking in from the outside. The downsizing of complex computer systems and the widespread distribution of personal computers is leading to serious discovery in the electronic data area.

Recognition is growing among both the Bar and clients that lawyers who handle discovery the old fashioned way — ignoring electronic mail and other types of electronic data sets —are missing evidence that could be critical in the litigation. One might make an analogy to the early, post-world war II period when radar became widely available as a civilian navigation tool. There were some fine, experienced captains who had learned to navigate without any electronic aids and who stuck to their tried-and-true ways rather than trusting their fate to a 'new' technology. This lasted until the courts began to impose liability on those ships that did not use radar when it was determined that the collision or accident could have been avoided by using such technology. Those decisions cost the ship owners large amounts of money and no doubt put a premature end to some careers.

Litigation lawyers who do not attend to electronic evidence — in an age when electronic mail and other kinds of electronic data are often the sole source of critical evidence — are soon going to be in the same boat as those captains of old. A transformation of the discovery process has begun, and it promises to be a disaster for those corporations that are not prepared. Any corporation that does not prepare proper litigation response mechanisms in advance of litigation will be at a strategic disadvantage and may not be able to respond in accordance with prescribed rules of discovery.

Electronic Data Gets Its Day in Court

The courts have also begun to recognize that the discovery of electronic data means more than obtaining a printout of computer files. As an example of the increased attention being given to electronic evidence, review the following excerpt from a federal court decision, holding that electronic copies of electronic mail under the IBM PROFS system are not the same as paper printouts:

First, these systems give recipients [of electronic mail] the option of storing notes in their personal electronic "log." After receiving a message, a user may instruct the computer to delete the note; otherwise, it will be stored in her log for later use. Second, both the recipient and the author of a note can print out a "hard copy" of the electronic message containing essentially all the information displayed on the computer screen. That paper

rendering will not, however, necessarily include all the information held in the computer memory as part of the electronic document. Directories, distribution lists, acknowledgments of receipts and similar materials do not appear on the computer screen--and thus are not reproduced when users print out the information that appears on the screen. Without this "non-screen" information, a later reader may not be able to glean from the hard copy such basic facts as who sent or received a particular message or when it was received. For example, if a note is sent to individuals on a distribution list already in the computer, the hard copy may well include only a generic reference to the distribution list (e.g., "List A"), not the names of the individuals on the list who received the document. Consequently, if only the hard copy is preserved in such situations, essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish. A final relevant fact here is that the individual note logs are not the only electronic repositories for information on the electronic mail system. The [system operators] periodically create backup tapes -- snapshots of all the material stored on these electronic communications systems at a given time -- that can be used later for retrieval purposes. [Armstrong v. Executive Office of the President, 1 F.3rd 1274, 1280 (D.C. Cir. 1993)]

Not only is all of this additional information available in electronic form and not on paper, but the information is more useful in electronic form because it is easier to search and manipulate. Courts have therefore required parties to litigation to turn over electronic copies of their information, in some cases even where the information has already been turned over in paper and where some additional computer processing work is needed to generate the electronic file. See, e.g., National Union Electric Corp. v. Matsushita Electric Industrial Co., 494 F.Supp. 1257 (E.D. Pa. 1980).

The Federal Rules of Civil Procedure: A Growing Role for Electronic Data

In December, 1993, the Federal Rules of Civil Procedure were revised, including the creation of a new Federal Rule of Civil Procedure 26(a), requiring that a litigant turn over to the other side a list of relevant electronic data compilations — as well as paper documents — early in litigation. While the new rule had an "opt-out" provision, that has now been revoked. Even if not directly invoked, the explicit mention of electronic data in Fed.R.Civ.P. 26(a) and 34(a) make it clear that electronic data is going to play a significant role in discovery. Even without these new rules, however, plaintiffs will force production by aggressively targeting electronic data.

Many corporations, required to produce a list of their relevant electronic data after litigation commences, will simply be unable to do so. If the court can be persuaded that the corporation really does not have an understanding of its own electronic data, monetary sanctions may be avoided. There may still be costs, however, in the form of:

- the corporation being forced into a defensive posture from the very outset of the litigation;
- the disclosure of a weakness in the corporation's armor, on which the smart plaintiff lawyer will surely focus; and,
- potential public embarrassment in the form of the corporation being identified as an organization that does not even know what data it has.

It may sound far fetched to suggest that aggressive plaintiffs may be permitted by the court to access a corporation's computer system and search the data on it, but Federal Rules of Civil Procedure envision such a procedure "if the discovering party needs to check the electronic source itself" Fed.R.Civ.P. 34(a), Official Comment to 1970 Amendment. If the corporation cannot reliably state what potentially relevant electronic data is contained on its system or in data storage, the plaintiff may have an argument under this rule for direct inspection.

A failure to fulfill the requirements of Fed.R.Civ.P. 26(a) early in the litigation can affect the proceeding all the way through trial. Any evidence turned up later may be subject to attack as fabricated, and a delay or failure to produce information can be disclosed to a jury. Fed.R.Civ.P. 37(c)(1). If substantial discovery has taken place without the evidence being produced as required under the rule — or an early discovery request — it may lead to the exclusion of the evidence or the corporation being forced to pay for re-doing discovery. Id.

If evidence harmful to the corporation is divulged later in the litigation, it opens up charges of a "cover up." Worse still, if all of the pertinent evidence is not identified early in the litigation, it opens the door to such evidence being overwritten or erased during the normal operation of the computer system or the rotation of backup media. Whenever evidence is destroyed after the commencement of litigation, the line blurs between inadvertent loss and purposeful destruction. The situation is even more dangerous when the destruction occurs after a discovery request for the evidence has been received or a court rule imposes a duty on a party to produce evidence. Unless the pertinent evidence has been identified prior to litigation, some will be lost while the litigation is pending, and the potential results range from default judgments to monetary sanctions to huge legal bills in fighting off charges of evidence destruction.

On top of all this, there is the requirement of Federal Rule of Civil Procedure 26(g) that “the lawyer has made a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand,” and many states have similar rules. Few corporations are in a position to make such an assurance when it comes to electronic data. Yet, under the definition of documents in Federal Rule of Civil Procedure 34(a), and under the standard definition of documents used by most litigants, the request for documents is explicitly framed to include all types of electronic data.

As the general counsel of one of the author’s corporate clients stated, he gets more uncomfortable with every discovery response that goes out because the company simply does not have the means to search its electronic data, even if it were attempted. In most organizations, the combination of factors outlined above has permitted this state of affairs to persist, in effect creating a situation where the plaintiff’s attorneys failure to go after electronic data is all that stands between the corporation and some very unpleasant litigation experiences. The organization’s credibility in litigation and its public image are hanging on the expectation that plaintiffs’ lawyers will not exercise their right to aggressively pursue electronic data.

Sanctions for Failing to Produce Electronic Data: Crown Life Insurance Co. v. Craig

The plaintiff requests all of the relevant “written documents.” Your company produces the paper documents but does not search for electronic data because it was not specifically requested. Then, at trial, the plaintiff learns of electronic data and, dismayed at her own failure to ask for such pertinent data, lashes out at the most convenient target, accusing your company of stonewalling and hiding evidence.

If you are the counsel for Crown Insurance Company, this scenario ends with your corporation being, in effect, found in default and required to pay damages according to the plaintiff’s calculations. Your opportunity for rebuttal was canceled as a sanction for discovery abuse. See *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993). The pertinent part of the case involved a claim for renewal commissions by a terminated insurance agent subsequent to the termination. In discovery, the agent sought “documents” relating to the calculation of commissions. The company produced all paper documents and affirmed full production in affidavits responding to a series of motions to compel. At trial, the company’s attorney sought to introduce testimony based on evidence in a computer database in order to rebut the agent’s valuation of commissions. This move earned the company severe sanctions for willful discovery

misconduct, with the trial court precluding it from putting on any evidence that contravened the agent's valuation. The federal court of appeals upheld this ruling, recognizing that it was tantamount to a default judgment.

Crown Life Insurance Co. should set off several alarms for companies regarding possible consequences in the way in which electronic evidence has traditionally been handled. A defendant corporation was, in effect, placed in default for failing to produce electronic data, even though the plaintiff had limited his discovery requests to written documents. The court of appeals held that the data was a written document, because the trial court's discovery orders had made clear that it was the kind of information that the company was required to turn over to the plaintiff. The duty to turn this information over arose in the case, although the company had no printout of the data at the time of the plaintiff's request for production and although the court observed that "it may be true that [the company] could not access the data at the time of the request." Nevertheless, the court explicitly held that the company had a duty to create such printouts of data responsive to the request for production. The court based its holding on the official comment to the 1970 amendment to Federal Rule of Civil Procedure 34, explaining why documents had been defined in the rule to include "data compilations, translated, if necessary, by the respondent through detection devices into reasonably usable form":

It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form [Fed.R.Civ.P. 34(a) and Official Comment to 1970 Amendment to Fed.R.Civ.P. 34(a).]

In other words, a corporation that is asked for written documents may be required to produce electronic data directly in an electronic format useable by the plaintiff, or face a potential default based on willful violations of discovery orders.

The result in the Crown Life Insurance case cannot be chalked up to bad tactics, although it was obviously a risky course to withhold a database containing relevant information during discovery and then attempt to use it at trial. Sophisticated plaintiff's lawyers often will find relevant electronic data at some point in the litigation. If it was not produced by the defendant in response to requests for production of "documents," charges of hiding evidence will be made — and sometimes be successful. In today's litigation environment, the appearance that a party is hiding

something can overwhelm the merits in a case. Only those organizations prepared to deal with electronic evidence in discovery will avoid disasters of this kind.

The “Gentleman’s Agreement” to Overlook Electronic Data: A Thing of the Past

In the Crown Insurance Company case, the corporation may have been lulled into a false sense of security by adhering to what an in-house corporate attorney recently described to the authors as “a gentleman’s agreement that has allowed us to get by without producing electronic data.” While the definition of ‘documents’ in standard discovery requests is usually broad enough to encompass electronic data, there are typically no questions asked that specifically seek its production. The definition section of the discovery request is simply overlooked, and there is very seldom any follow up effort made at obtaining such data. Accordingly, neither attorney is required to traverse the unfamiliar and forbidding terrain of the corporate computer system. While this arrangement may be comfortable for the attorneys, it is no longer in the best interest of their clients and may set the corporation up for a Crown Life Insurance scenario.

There are several reasons why electronic data has not been properly utilized in discovery. First, and perhaps most importantly, is that many attorneys lack the comprehensive knowledge of computer hardware, software and systems layout that is required to understand the technical aspects of creating, modifying and storing data. Without such an understanding, it is difficult to write the proper interrogatories and requests for production to elicit desired information, let alone attempt to actually discover and/or recover such information. Furthermore, some technical expertise may be needed to understand any answers that come back, to compile the pertinent information contained therein, and to then place that information into the context of the case.

Second, if any electronic data is produced, the logistical problems in converting, storing, reading and analyzing it may be beyond the capabilities of a normal law office computer system. Over the years, attorneys and their support staff have developed extensive policies, procedures and methodologies for incorporating paper-based data into their case preparation process. To date, the same levels of sophistication for handling electronic documents have not been developed.

Third, electronic data can be overwhelming in terms of its sheer volume and organization. While paper documents normally get filed into fixed storage areas — file folders, file cabinets, file rooms — with descriptive tags and in somewhat manageable quantities, electronic document files are

typically commingled in one or more electronic storage areas with little or no descriptive information about their contents provided in the names that they are given. Additionally, while paper documents are often subjected to retention policies designed to inhibit excessive accumulation, electronic files are often allowed to accumulate with no retention oversight whatsoever. The authors are currently involved in a litigation in which over three hundred million electronic data files have been identified for possible production. None of these files would still be in existence if the company would have had a reasonable electronic data retention policy in effect.

Fourth, attorneys tend to stick with tried and true approaches, especially in litigation where a new focus can lead to unanticipated results. As a group, lawyers have historically tended to be technology-averse. Indeed, a significant number of lawyers report that they were attracted to the profession specifically because it is one of the few kinds of intellectual work that permitted them to avoid technological issues. As the personal computer continues to become a standard business tool in virtually all professions, this situation is quickly changing.

Whatever arrangements worked in the past are now crumbling as practitioners learn of the value of professionally, specifically and aggressively targeting electronic data sets. In many, if not most, corporations, the computer has become the primary repository of corporate data. While most of this information may get partially printed to paper and found by traditional discovery methods, there remains in the computer a substantial amount of data that never gets printed and therefore never gets found. This electronic information has proven to be so substantial and so beneficial in litigation that it simply cannot continue to be overlooked.

Electronic Data Management — Its Impact on the Bottom Line

For each disaster awaiting those corporations unprepared to deal with electronic data discovery is an opportunity for those who do prepare themselves for such an eventuality. Given current trends, it is only a matter of time until the discovery of electronic data in litigation becomes the primary type of discovery. In the transition period, those who are ahead of the game will reap substantial benefits; those who are unprepared will pay. And pay. And pay.

Forward thinking corporations will take steps to develop an electronic evidence management plan that will prepare them for reviewing, evaluating and retrieving electronic data for production. Several benefits accrue from developing such a plan outside of the pressure and constraints of the discovery phase of a particular litigation.

Reduced litigation expenses.

It is very expensive to deal with large amounts of disorganized computer data at the last minute. The response will require effort by in-house information services or outside consultants. If done in-house, a major search and analysis of data for litigation will usually divert computer resources from profit-making activity and will distract information services personnel. If done by outside consultants, such intense, last minute efforts will be billed at a premium and result in higher expenses. By contrast, a corporation that addresses the electronic evidence issue prior to litigation has the time to explore cost effective approaches.

Maintaining a position of strength and confidence.

A key aspect of electronic evidence management is to prepare the corporation to meet deadlines for mandatory disclosure and to respond in a timely and accurate manner to discovery requests. A corporation that competently handles electronic data in a planned manner, rather than being put on the defensive, will present a better litigation posture and, in many cases, defuse a weapon its adversary was depending on. When the corporation wishes to, it can demonstrate that requests for electronic data will involve little difficulty or cost, that the corporation has reviewed and evaluated the electronic data sets, and that the plaintiff or adversary will need to expend a great deal of time, effort and money to catch up. A corporate image of good faith, competency and readiness will be projected.

Identifying strengths and vulnerabilities.

The ability to assemble the relevant electronic mail and other electronic records early in litigation will assist counsel in identifying strengths and vulnerabilities. Additionally, the ability to use electronic evidence will not be lost because of a failure to timely disclose it in response to discovery requests or mandatory disclosure rules.

Avoiding ambushes.

Without the early identification and review of electronic mail and other electronic data, corporate witnesses may be required to give deposition testimony without the benefit of reviewing such material. When materials such as contemporaneous electronic mail messages are found by later discovery efforts, they may provide a rich source of impeachment material over details that otherwise may not have been important. An effective electronic data management plan will permit counsel to make an informed decision as to when and how to use electronic data as discovery unfolds.

Maintaining a consistent corporate position.

Large corporations always face the danger that discovery responses in one case will be treated differently than in others. For various reasons, one litigation counsel may take a more restrictive

approach to discovery than another and produce different types and/or quantities of response material to similar requests. Inconsistent discovery responses can lead to problems if plaintiffs communicate with one another. Electronic evidence should be managed to avoid such problems insofar as possible.

The bottom line benefit of addressing electronic evidence in advance will be even greater for corporations in business litigation. A corporation that has an effective program for retrieving and evaluating its own data will be at a tremendous advantage in business disputes, as opposed to a corporation that has failed to address this issue. The corporation prepared to deal with its own data is also better prepared to probe its adversary's computer system and electronic data sets. In many cases, this will mean that the unprepared party is faced with substantial litigation costs that do not exist for the other side and that the unprepared party will be on the defensive throughout the litigation and will not be able to make as effective a presentation at trial.

Another advantage that will accrue to those corporations that address the electronic evidence issues in advance of litigation is the ability to address problems in a preventative way. Data backup and archiving procedures can be reevaluated and adjusted to make it easier to identify, evaluate and retrieve data in connection with litigation. Inadvertent accumulation of information with no business purpose can be minimized. Procedures can be developed to reduce abuses of electronic mail, such as inappropriate comments and the like. Such steps can reduce the misuse of the computer system, thereby reducing the underlying causes of lawsuits and liabilities.

A Case Study of an Unprepared Corporation

A recent case handled by the authors' company, Electronic Evidence Discovery Incorporated, or EED, highlights the pitfalls that await the unprepared. EED was retained by a lawyer representing the new employer of an individual who had been fired by a medium-sized company. The plaintiff's story: He was fired, despite good job performance, after he began dating the ex-wife of an important customer. After being fired, his former employer tried to prevent him from working for a competitor. The employer's story: Although the customer did complain about the relationship between his ex-wife and the employee, the firing happened much later, after some incidents of poor performance by the plaintiff. It was only after these incidents that the plaintiff's supervisor flew from headquarters to the branch office where the employee worked and fired him. A suit was brought approximately a year after the termination.

The plaintiff believed that there would be useful information in the corporate electronic mail system. His lawyer made a request for production several months after the lawsuit commenced. By the time of the discovery request, the company attorney ascertained that the computer department had "purged" from the computer system the electronic mail from the time of the firing. The company's attorney rather blithely wrote to plaintiff's lawyer that the pertinent electronic mail no longer existed. At that point, Electronic Evidence Discovery was engaged.

It was apparent to EED that further discovery was likely to be fruitful. The word "purged" as used in the computer world does not necessarily mean destroyed. Rather, purging data normally means taking it off of the system's on-line storage and putting it onto an archive media where it will be saved for some defined time period. A deposition of the head of information services (the computer department) was scheduled. The question of purging was clarified in this deposition and we further learned that there was a rotation policy for such archive tapes under which electronic mail messages would be kept for about a year before the tapes were reused and overwritten with new information. It was determined that, by the time of the deposition, the electronic mail tapes in question were scheduled for rotation and in fact had been "scratched," that is, had been removed from archive status and, literally, placed on a shelf for reuse. At this point in the life cycle, the computer department regards the tape as discarded and the information as having been destroyed. It is not uncommon, however, for 'scratch tapes' to queue up for some time before reuse, and we asked that the scratch tapes be checked for the electronic mail. After a break in the deposition, it was reported that the electronic mail tapes in question were indeed found on the scratch rack.

The company attempted to keep control of the situation by printing out the electronic mail messages that they considered to be relevant. Given the circumstances, however, the company was not in a position to resist the plaintiff's demand that the electronic mail be produced for the plaintiff's own review. After all, up until the deposition of the information services manager, the company's attorney had insisted that the tapes containing the electronic mail did not exist at all. Perhaps this was not evasiveness, but, because of his unfamiliarity with the computer jargon and procedures within the company, merely the attorney's misunderstanding of the term "purged." However, it is a dangerous and uncomfortable litigation posture for a corporation to tell a judge or jury that it refused to produce the most relevant information in the case because it was just overlooked or because its own attorney misunderstood the computer department. In such circumstances, it is very difficult to credibly claim that the plaintiff should rely upon the company's assertion that it has culled out the relevant data.

As a result, over 750,000 electronic mail messages were produced on a number of 9-track magnetic tapes. Only a few years ago, processing and analyzing this data would have taken a mainframe computer, some custom programming, perhaps two or three weeks and a substantial budget. EED was able to design and implement a review process that was completed in a few days and which located some 6,000 relevant electronic mail messages. Many of these messages gave a running account of the relationship between the employee and management and presented a contemporaneous record that was inconsistent with the company's claim of poor performance. Even more damaging to the company's position was an Electronic mail message that the plaintiff's supervisor had completed scheduling airplane reservations for the trip that was specially made to fire the plaintiff. This electronic mail message was dated the same day that he had learned of the plaintiff dating the customer's ex-wife and approximately a month prior to the alleged misconduct that the company claimed initiated the plaintiff's firing. This evidence was in direct opposition to sworn testimony from the supervisor and other company representatives.

Perhaps even more striking was the electronic mail message that turned up that, although not directly related to this case, proved to be damaging to the company. This message read: "*****EVIDENCE DESTROYED***** Ack[nowledged] your message and have destroyed the records." EED then located the first message that requested the destruction of these records. Although the plaintiff claimed that these messages were evidence of a corporate culture, we were informed that a motion in limine succeeded on grounds that the messages were not related closely enough to the case at hand to be admissible. Nevertheless, authenticated proof of corporate management destroying evidence is not the kind of image that most corporations want to project either in a court of law or in the public arena.

Because they were unprepared, this corporation set itself up for a legal and public relations disaster. The company's attorney did not understand the computer system and made no effort to examine the electronic data set at the commencement of litigation. As a result, managers who were key witnesses were permitted to give deposition testimony without reviewing the electronic mail that gave a contemporaneous account of their thought processes and actions. The company set itself up to be ambushed if the plaintiff found out about the electronic mail. Given the poor communication between the company's attorney and its information services department, it is doubtful that efforts to prepare would have been successful anyway. Counsel appears to have lacked basic understanding of computer technology, and the information services department, as it often is in these situations, was reluctant to devote scarce resources and time to what may have appeared from their perspective to be a distraction from their mission.

Because the company had not properly addressed its electronic data set, it tainted itself with the appearance of hiding evidence and it set up its own witnesses by letting them testify without reviewing the record. Embarrassing messages that may otherwise have been protected from discovery were placed on the public record and had to be explained to the court. Costs to the corporation of all this are difficult to calculate, but include increased damages, bad public relations and an undermining of the trust and morale within the corporation itself.

Developing an Electronic Data Management Structure

When you talk about a management plan for electronic data, it is important to make sure that all of the parties to be involved in the development have a clear understanding of what the project is all about. This is an area where semantics can dramatically alter perceptions. Electronic file management will mean one thing to the computer department and something entirely different to the corporate legal department. In the context of this article, management of electronic data refers to the development and implementation of various policies and procedures designed to (1) organize electronic data so that it can be found and retrieved efficiently for litigation and in such a manner that it does not invite wholesale discovery beyond what is relevant; (2) identify and preserve necessary business documents while keeping the number of unnecessary documents to a minimum; (3) to identify preventative measures for reducing abuse of electronic mail and other computer systems; and (4) to define and implement retention policies that both support the goals above and that keep the necessary business documents from accumulating past their useful lives. Usually, an ongoing auditing procedure is needed to maintain the level of preparedness.

We are concerned at this point with the content of the documents and not with how efficiently they are being processed or stored by the computer system. For this reason, it is usually critical for either in-house or outside counsel to take the lead in developing such a plan. The traditional computer department sees a file as an item to be managed and processed, regardless of its content. This management plan, however, revolves around the content of the file, whether or not it should exist in the computer system at all, and, if so, for how long. Basically, we are concerned about the efficient maintenance of information and the associated liability of either not managing it or in not having proper retention schedules.

Once the goal of the project is made clear, the first step in developing an electronic data retention and management plan is to develop an overall profile of the organization's electronic data processing system. This overall profile should address the structure of the system in terms of hardware, software and policies and procedures and should locate and identify the source, content and location of all electronic data sets.

The information gathered should be general enough in nature so as to allow completion of the audit in a reasonable time, but specific enough to understand the nature and type of electronic activity taking place. This macro profile should be reviewed to identify possible areas of vulnerability in terms of data accumulation and liability problems. Specific departments, platforms or functional areas that exhibit problems or vulnerabilities, or that tend to be targets of litigation, should be identified for specific, detailed, electronic data audits.

These specific audits should address in detail the structure of the computer system in use in that area in terms of hardware, software and policies and procedures and should locate and identify the source, content, location and ownership of all electronic data sets.

The information gathered above should be very specific so as to allow a detailed review of the nature and type of electronic activity taking place. From this review, specific data retention and management policies and procedures can be developed and implemented for the given target area.

Once all high-risk, targeted areas have been reviewed in detail, a general set of electronic data retention and management policies can be derived and implemented throughout the organization.

One temptation for many institutions when they first address the electronic data issue is to destroy anything that is not operationally needed in an immediate way. This could be a strategy that backfires later on. Any destruction of data that could ultimately be relevant in a lawsuit is a dangerous matter, both because of appearances and because of the potential for misunderstanding by a court. What is needed is a hard look at how the electronic data system is used, the purposes of maintaining electronic data sets from a business perspective, and how policies and procedures and adjustments can be made to the system to meet those needs most effectively. From a litigation perspective, the key is to know what information exists and to be able to find what is relevant in a timely and cost-effective manner. Being able to do so goes a long way toward defusing the electronic evidence time-bomb in litigation.

Accessing helpful data will improve an institution's position in a lawsuit, and forthrightly producing all relevant data, even if adverse, will maximize the ability to deal with a case realistically and in time to develop helpful defenses. The dangers of destroying electronic data are every bit as serious as the dangers of destroying paper documents that are relevant to a lawsuit. Useless data

should not be maintained, but destruction of data for the purpose of making it unavailable for litigation may be a formula for disaster.

In order to prepare for addressing electronic evidence in the litigation context, a substantial effort will be required for most corporations. The task will involve integrating functions that are dissimilar in style and approach. Involvement is usually needed from information services, internal audit, records management, and appropriate representatives from affected operational functions. A substantial investment of time, effort and money may be required. This investment, in our view, will pay off in several ways: lower litigation costs, in some cases improved settlement posture or trial presentation, better public relations and less interference by lawsuits into profit making activities. Counsel can protect and benefit their corporations by addressing these issues in a timely manner.

Authored by

John H. Jessen | Chief Executive Officer

John H. Jessen is the Founder and CEO of Electronic Evidence Discovery, Inc. Recognized internationally as the pioneer in the field of electronic discovery, Mr. Jessen is a frequent author of articles on the subject and has presented numerous lectures and seminars nationally on legal and electronic data issues.

Mr. Jessen and his company have been profiled in *The Wall Street Journal*, *Forbes*, the *Chicago Tribune*, the *Los Angeles Times*, the *Boston Globe*, *Wired*, and many other publications. He has been featured on CNN, CNBC, and CBS' *60 Minutes*, *20/20*, *The Oprah Winfrey Show*, and has been called the "Best of the Breed" by the *American Bar Association Journal* and "*The nation's foremost authority on sniffing out secret or deleted computer files*" by *Entrepreneur Magazine*. Mr. Jessen and his firm assist attorneys in utilizing electronic data in litigation and organizations in developing electronic data retention and management policies.

Kenneth Shear | formerly Vice President of Technology & Law | Electronic Evidence Discovery, Inc.

Conditions for Distribution:

This document may be freely distributed, so long as (a) it is copied and distributed in full without redaction; (b) all notices of copyright are contained on each copy distributed; (c) authorship is attributed as on this document; and (d) the address, telephone number, and URL of Electronic Evidence Discovery, Inc. are included.

Electronic Evidence Discovery, Inc.

Worldwide Headquarters
Plaza at Yarrow Bay, Suite 200
3933 Lake Washington Blvd. NE
Kirkland, WA 98033
Phone: (206) 343-0131
Fax: (206) 343-0172

www.eedinc.com