If the Slate Is Wiped Clean

Spoliation: What It Can Mean For Your Case

By Randolph A. Kahn and Kristi L. Vaiden

"The next information revolution is underway.
It is not a revolution in technology, machinery, techniques, software or speed.
It is a revolution in concepts."
Peter Drucker

This article, co-authored by one of my associates, details a very significant conceptual revolution that is occuring in our legal system; specifically, courts are redefining their traditional perspectives about destruction of evidence - spoliation - when the evidence is electronic records. In an era of ever-increasing growth in litigation and the exponential expansion in the volume of electronic records, this conceptual revolution regarding spoliation and electronic records must be both understood and proactively addressed to avoid this new and emerging legal problem in the future.

Robert Williams, President
Cohasset Associates, Inc.

This article originally appeared in the American Bar Association Publication, *Business Law Today,* May/June 1999 edition and is reprinted by Cohasset Associates, Inc. with ABA permission.

Government lawyers cross-examine witnesses with "smoking gun" e-mail messages unearthed from the deep recesses of a storage tape. A company summarily fires two senior employees for distributing revealing pictures over the company intranet. A claim for spoliation is successfully advanced against a litigant for merely failing to stop the "recycling" of computer tapes containing potentially relevant information.

As the dust begins to settle from the rush to apply technology to most business processes, what has become clear is that the application of such technologies can be a source of liability.

The vast majority of corporations keep electronic records, but few manage them effectively. Ineffective records management exposes a company to significant risks. It frustrates business operations, wastes resources and creates litigation minefields.

Failure to produce electronic records in litigation could open the door to discovery sanctions and a spoliation claim. Something as simple as recycling back-up tapes of electronic data, that effectively erases information requested in discovery, can spell trouble in the courtroom and result in hostile headlines for a company competing in the electronic age.

This article briefly reviews the evolution of the tort of spoliation and explores how the haphazard and inefficient management of a company's records could translate into potential liability. It also suggests some concrete steps for management of electronic records to protect a company's interests and to minimize its exposure to risks of spoliation claims.

The potential for spoliation liability arises under the discovery rules. These require production of not just paper records, but also relevant electronic records. Rule 26(B) of the Federal Rules of Civil Procedure defines electronic records as "data compilations," that broadly encompass "any means of storing information other than the conventional words and figures in written or documentary form and includes electronic computer storage." Under this rule, discoverable material can include not only internal e-mail messages, but also Internet communications, computer graphic images, digitized photo files and any "data compilation" stored on magnetic disks, optical disks, hard disks, back-up tapes and other electronic storage media.

Statutes that define record-keeping requirements for tax and other regulatory purposes are more narrow in scope than the federal discovery rules. In other words, companies may be compelled in litigation to produce broader categories of data used by their business, if they exist, even though they had no legal obligation to keep the data in the first place.

When adversaries aggressively seek broad categories of electronic records, some of the data may not be accessible or in a usable form. In Sanders v. Levy, 558 F.2d 636, 649 (2nd Cir.1982), the court required a new program to be created to extract the requested data and to translate them into usable form, all at the producing company's expense. The court explained:

> *Computers, which in general make information more readily available, may occasionally make information more difficult to discover. Even where a party adapts his computer software strictly in accordance with legitimate business purposes, complex electronic processes may be required to extract information which might have been obtainable through a minimum of effort had different systems been used. If the information demanded is such as*

the respondent might reasonably have expected to be required to make available for public examination or for use in the judicial process, it seems not unfair to require production of the information albeit necessitating special programming.

The expense of special programming can be shifted to the discovering party where the production would impose an undue burden or expense. The court in Sanders nonetheless followed the general rule, leaving the responding party to bear the expense. The court's ruling embraces the notion that "you created the data, now produce it at your cost."

If evidence is not available, the court may direct a jury to infer that the requested data is unavailable because it supports claims against the offending party. All or part of the offending party's pleadings may be struck and monetary sanctions imposed. If the unavailability of the data precludes a plaintiff from putting on a case, some courts are willing to recognize an independent tort of spoliation.

When files are destroyed, be sure to follow a set policy.

Despite some courts' view that a separate tort of spoliation is unnecessary; the variety of circumstances that have been recognized to support a claim for spoliation reflect a worsening risk for companies. Typically a claim requires knowledge of pending litigation, an intentional action to destroy evidence, and damages resulting from the destruction. See *Willard v. Caterpillar,* 40 Cal. App.4th 892, 48 Cal. Rptr.2d 607 (1995).

Some courts have entertained spoliation claims based on something less than intentional misconduct. Sanctions have been imposed where records were simply unavailable. Poor record keeping and inadequate organization of records are no excuse. Ineffective records management is viewed by some courts as the functional equivalent of destroying records. *Velasco v. Commercial Bldg. Maintenance Co.,* 169 Cal. App.3d 874, 215 Cal. Rptr. 504 (1985).

The progeny of spoliation claims based on mere negligence are particularly troublesome as companies store more and more of their corporate memory in electronic form. The inherent nature of electronic data and storage media contributes to the ease with which records can be altered, deleted, misplaced or rendered inaccessible. Storing a massive volume of data on media that requires a computer to see it compounds the difficulties in finding and retrieving electronic records. The result is that companies may inadvertently expose themselves to a spoliation claim if their failure to maintain an effective electronic-management system frustrates the timely production of evidence.

In assessing the degree to which spoliation has impaired the administration or disposition of an action, courts look to:

- the evidence destroyed,
- when it was destroyed,
- who destroyed it, and
- how it was destroyed.

This framework has been set forth in the context of the destruction of paper and other physical records. Applying the framework to electronic records raises difficult questions.

Errant keystrokes are common to most computer users. Is it reasonable to expect that some electronic records are inadvertently deleted? Would the result differ if huge volumes of data were inadvertently deleted as the result of one errant keystroke? Will the migration of electronic data from one system to another in the ordinary course of business be viewed as reasonable, even if it allows data to evaporate from the storage media? Will imaged records, whose insufficient indexing makes their access virtually impossible, give rise to a spoliation claim? Will improper storage of electronic records, which makes it uncertain whether all the needed data has been stored, expose a company to a spoliation claim?

Despite the quagmire of questions, there is hope. While even some mistaken conduct may give rise to a spoliation claim, established record-keeping practices may help to minimize any sanction meted out by the

court. This trend can be seen in *Koch v. Koch Industries,* 1997 WL 447822 (D.Kan. 1997), in which the court declined to reopen discovery where destruction of documents was part of an established record-keeping policy.

An effective record-keeping policy must mandate that regular record-keeping practices be suspended when litigation begins or is foreseeable. That was the precise issue in *Applied Telematics v. Sprint,* 1996 U.S. Dist. LEXIS 14053 (D. Pa.). Sprint saw no operational need to retain electronic tapes of computer transactions that routed telephone calls. Applied Telematics requested the tapes, alleging they were relevant to the assessment of damages in a patent-infringement case. Sprint produced certain tapes in response to the initial discovery request. Because Applied Telematics did not follow up with additional requests, Sprint followed its routine practice of reusing the tapes, which effectively destroyed the transactional information contained in tapes not previously produced.

Like old paper files, electronic records need periodic destruction.

The court found that Sprint "knew or should have known that this information was relevant." As sanctions, the court required Sprint to pay the cost of obtaining comparable information from other sources. The court's ruling cautions that, where the medium used to store electronic records is erased in the ordinary course of business, procedures need to be in place that ensure appropriate treatment of evidence needed in pending or foreseeable litigation.

Litigants review the content of documents to determine their relevance to underlying claims. Because content will be critical in the discovery process, effective management of electronic records would require knowing the content of data tapes, disks and other electronic media before destruction. The courts have yet to deal with such issues in the private sector.

Two rulings in the governmental context are worth noting, which although not precedential, may provide insights into factors that courts might consider in approaching such issues. In *Armstrong V. Executive Office of the President,* 1Fed. 3d 1274 (D.C. Cir. 1993) the court required that e-mail messages be dealt with like all other records of similar content, from a records-management perspective. In *Public Citizen v. John Carlin,* 1997 U.S. Dist. LEXIS 16993 (D.D.C. 1997) the court held that the government's practice of allowing wholesale destruction of electronic records without knowing their content was in violation of the Federal Records Act, which, among other things, delineates federal agency procedures for records retention. Recognizing the uncertainties of a pending appeal of the *Carlin* ruling, the National Archives and Records Administration is re-evaluating its records-retention policies related to the disposition of electronic records.

The implication for the private sector is that a company should reexamine how its records-retention policies are being applied to electronic records. Simply because new technologies enable different ways of keeping and destroying records does not mean that electronic records can be purged without regard to their content.

That does not mean that all e-mail messages must be retained indefinitely. Just like out-of-date paper records, electronic records should be scheduled for periodic destruction. Susan Gindin in *Guide to E-Mail and the Internet in the Workplace* (Bureau of National Affairs, 1999), gives the example of a company that deploys emil programs with a built-in scavenger feature that deletes out-of-date material every month. The same company erases back-up tapes after six months where documents have outlived their business usefulness.

Using the most current or most expensive optical-imaging equipment does not necessarily ensure that newly imaged records will be "good" evidence or acceptable as replacements of "original" records. Recently stated federal agency positions (IRS, SEC, Department of Labor, etc.) on the retention of records

on electronic media require procedural safeguards to ensure the thoroughness, clarity and accessibility of the records, among other things. These new rules make clear that good optical imaging requires something more than pushing paper through a scanner.

For any record, reliability and trustworthiness require that the records be complete .

Imaged records may need to be reviewed for completeness as part of the image-capture process. The equipment may need to be set to specific "dots per inch" tolerances or risk not capturing all of the document. Developing and implementing procedures to make acceptable records is not self-evident and not all companies currently storing records on optical media may have the requisite expertise.

While a federal agency may never challenge your imaged records, if any are successfully attacked, then all records similarly stored may be open to attack. This is compounded by the fact that once records are imaged and the originals are destroyed, there may be no simple way to correct the problem since there may be no way to recreate acceptable originals. Having the systems and the method for imaging independently reviewed may provide some comfort that imaging was properly done and that your imaged records will be acceptable.

In the electronic context, "what is the complete record" is not a simple question.

Electronic records are often not nearly as rugged and durable as their paper counterparts. The following factors affect their life expectancy :

- quality of the medium,
- the number of times the medium was viewed,
- the care in handling,
- the storage temperature and humidity level,
- the cleanliness of the storage environment, and
- the quality of the recorder used to write to the media.

Even under the best environmental conditions, however, certain magnetic storage media may have a limited life, which can be much shorter than paper or microfilm. Unless information is moved from one tape to another periodically, part or all of the information contained on the tape or disk can be lost forever.

For any record, reliability and trustworthiness require that the record be complete. Computers make changing or altering the content or structure of a record (with no apparent sign of tampering on the readable version) an easy proposition, which undermines a record's reliability and integrity. A record's trustworthiness is at the heart of its usability for evidentiary purposes. In the electronic context, "what is the complete record" is not a simple question.

Interpreting the records-retention and disposal requirements imposed on the federal government, the courts in *Armstrong and Carlin* found that a complete electronic record is made up of more than the actual text of the record. Specifically the "meta-data" (electronic identification of the sender, recipient and date of transmission, etc.) are integral to the record's completeness for purposes of governmental records-retention requirements.

While companies are not subject to the same records-retention requirements that are imposed on the federal government, preservation of meta-data may be a necessary and integral part of sound records management. Because meta-data contains contextual information about the creation of a record, it may need to be identified and captured in conjunction with the record itself. The meta-data should also be maintained for as long as the record, through successive upgrades of the hardware and software, in such a way as to retain the integrity and value of the "complete" record.

When a company needs "complete" electronic

records, system administrators may cry that the volume of data will clog the company's systems. To address space limitations, effective records-management policies and complementing retention schedules become critical to winnow important records from unneeded electronic data. For example, redundant and back-up copies, including the extra copies that exist in storage, might be purged routinely in accordance with the company's policy. Archival copies might be stored, with an appropriate retrieval system, on separate systems or off-site.

The winnowing process should include reference to the company's retention policies for purging non-record material. For example, weather reports, competitive airfares and other public information downloaded from the Internet used in planning a business trip might not be considered a "record" for purposes of a company's retention policy. Similarly, drafts of spreadsheets and graphs developed by an individual in preparing budget-support documents might be discarded if the company's retention policy considers only final versions to be "records."

Once in place, the company's retention policies should be enforced.

Proper indexing is essential in managing electronic records. Electronic storage does not place records physically in a row, in alphabetical order or otherwise in connected folders on a storage device. Therefore, retrieval requires the development of an indexing "key" to gain access. The keys are most effective if done at about the time the records are being scanned. Without proper indexing, records may not be retrievable.

The software and hardware used to create an electronic record may be replaced over time. New generations of hardware or software may frustrate finding older records or change the look or format when reproduced. In other words, it may not be enough to move the information from tape to tape or disk to disk. Depending on the nature of the records, likelihood of their pertinence to pending or foreseeable litigation, and other relevant factors, it may also be prudent to:

- ensure that the new computer systems can read the storage media,
- retain the older models as well as the key personnel and documentation needed to maintain them, or
- arrange for a third-party service to ensure the readability of the records.

Advanced technologies enable information to be created, transported, manipulated, stored, retrieved and purged virtually anywhere and at any time. In this electronic environment, company records can be found on mainframes, floppy disks, magnetic tapes, CD-ROMs, personal computer hard drives and other media. The media typically are used by dispersed staff, who work in the field, at the office, on a customer's site or at home. The diversities of staff, locations and technologies further contribute to the complexity of managing electronic records. An effective training and continuing education program is critical to ensure that records will be accessible in a readable and usable form.

Exposure to discovery sanctions, tort claims and other liabilities for spoliation are diminished if records are maintained and disposed of in conformity with a formal records-retention policy. The policy should be tailored to achieve the company's legitimate corporate goals. In addition to addressing legal and regulatory requirements, it should reflect:

- cost-effective management to support continuing business activities;
- protection of vital electronic records needed in the event of disaster;
- security of private, confidential and proprietary information;
- preservation of records having long-term and historical value;
- accessibility of records relevant in judicial, regulatory, congressional and other legal actions; and
- procedures for proper disposition of non-records and records beyond their retention periods.

Once in place, the company's retention policies should be enforced. For example, if the policy requires

records to be purged after a defined number of years, then purging should be performed on schedule and documented using a form developed for just that purpose. Thereafter, if a question is raised about when, where or under what circumstances the destruction took place, the disposition form can show that it took place in compliance with the retention policy.

The judicial imposition of sanctions for spoliation emphasizes the need for a company to assess its practices in managing electronic records. The group performing such an assessment should include the company's leaders to ensure that records are being maintained in accordance with corporate goals. Management involved with these issues should include technical experts who understand not only the company's current computing and communications environment, but also its future directions. Legal personnel are also critical to help the company to recognize the potential risks involved in its conduct.

The framework for the assessment should be tailored to the nature of the company's business, the status of any pending and anticipated litigation, and such other factors as identified by the leadership team. Steps within the framework might include:

- establishing and updating an inventory of the advanced technologies deployed by the company (e-mail, hardware, software and other electronic systems);
- maintaining a system for tracking the locations in which electronic data are stored (hard drives on mainframes and personal computers, magnetic tapes, disks, CD's and other media);
- providing for off-site storage of the records needed for disaster recovery;
- ensuring that contracts with consultants, services providers and other third parties require compliance with the company's record policies and permit periodic audits;
- documenting policies and procedures for creating, storing and indexing different types of information;
- ensuring that similar records are treated similarly whether paper or electronic;
- requiring authorized procedures to be followed in purging electronic records;
- developing a procedure to suspend the disposition of records once a lawsuit is filed or is imminent.
- documenting that policies and procedures have been followed in retaining and disposing of electronic records;
- educating employees and other personnel authorized to use the company's advanced technologies about the company's records-retention policies;
- conducting periodic audits to ensure compliance with the company's records-retention policies;
- identifying persons responsible for compliance with records programs; and
- providing review of the framework to adapt to changing technology, evolving company directions and emerging judicial and regulatory trends.

In addition to anticipating where litigation and discovery issues may arise, managing electronic records contributes to many business objectives including minimizing expenses of storing everything forever, making information accessible to support continuing business activities and preserving the corporate memory needed for future operations.

Electronic records are rapidly becoming the mainstay of business and as such comprise the new corporate memory. This presents significant technological and legal challenges. An aware management, however, can significantly reduce the risk of using electronic records and the company can enjoy the economic benefits of efficient control of its critical corporate information.

Randolph Kahn is a lawyer and Senior Consultant with Cohasset Associates Inc., a records, information and technology management-consulting firm based in Chicago.

Kristi Vaiden is Assistant General Counsel with The Prudential Insurance Company of America, in Newark, N.J.

Cohasset Associates, Inc. is recognized as one of the nation's foremost management consulting firms specializing in document-based information management. Now in its third decade of serving clients throughout the United States, Cohasset's experienced consultants specialize in resolving information storage and retrieval problems. The professional services of Cohasset range from preparing retention schedules and the development of e-mail policies, to defining the legal and business requirements for electronic records management initiatives, and performing records and information risk management analysis.

Cohasset is also the publisher of Authentic Electronic Records: Strategies for Long-Term Access *as well as* Legality of Microfilm, Legality of Optical Storage *and* Legality of Magnetic Storage.

Cohasset Associates, Inc.
3806 Lake Point Tower
505 North Lake Shore Drive
Chicago, Illinois 60611
312-527-1550
www.cohasset.com