# RESPONDING TO DISCOVERY REQUESTS FOR YOUR ELECTRONIC RECORDS: WHY YOU CAN'T WAIT TO "CROSS THAT BRIDGE WHEN YOU COME TO IT

ROBERT H. HAWN, JR., ESQUIRE COZEN AND O'CONNOR 1900 Market Street Philadelphia, PA 19103 (215) 665-2000 rhawn@cozen.com

Atlanta, GA
Charlotte, NC
Cherry Hill, NJ
Chicago, IL
Columbia, SC
Dallas, TX
Los Angeles, CA
New York, NY
Newark, NJ
Philadelphia, PA
San Diego, CA
San Francisco, CA
Seattle, WA
W. Conshohocken, PA

The views expressed herein are those of the author and do not necessarily represent the views or opinions of any current or former client of Cozen and O'Connor. These materials are not intended to provide legal advice. Readers should not act or rely on this material without seeking specific legal advice on matters which concern them.

Copyright (c) 2000 Cozen and O'Connor ALL RIGHTS RESERVED

1

"The electronic information revolution is...as profound as the printing press revolution in its potential impact on cultural and social patterns for creating and using information." H. Perritt, Jr., *Electronic Records Management and Archives*, 53 U. Pitt. L. Rev. 963, 980-81 (1992).

"[T]oday it is black letter law that computerized data is discoverable if relevant." **Anti-Monopoly, Inc. v. Hasbro, Inc.**, 94 Civ. 2120, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995).

"It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the rules,..."

Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985).

# I. Background

## A. Electronic Records?

For our purposes, the term "**electronic records**" is used interchangeably with "**electronic data**" and "**electronic information**". "**Data**" is defined as "an item of information". The definition of "**information**" is "the meaning of data as it is intended to be interpreted by people". "**Records**" means "a data structure that is a collection of fields (elements), each with its own name and type". <u>The Computer Dictionary (Fourth Edition)</u>; Microsoft Press 1999.

It is the data (information) that is processed and stored as records on computers, which is the subject of this discussion. A "**computer**" is defined as "any device capable of processing information to produce a desired result". *Id.* Again, for our purposes, "computer" is generally limited to mean the hardware ("the physical components of a computer system", *id.*) and software ("computer programs; instructions that make the computer work", *id.*) that typically comprise the electronic computer systems on which most of us rely every business day.

## B. Why All the Excitement Now?

One explanation for the increasing attention now being given to the discovery of electronic data may lie with the fact that until relatively recently, few people and certainly very few lawyers or judges had acquired any meaningful experience or skill in using computers. This shared ignorance might easily have discouraged all but the most adventurous litigants and their counsel from exploring the foreboding frontier of electronic data discovery. However, today, as one court observed: "From the largest corporations to the smallest families, people are using

computers to cut costs, improve production, enhance communication, store countless data and improve capabilities in every aspect of human and technological development." **Bills v. Kennecott Corp.**, *supra* at 462. See generally G. Johnson, *Emerging Technologies and the Law: A practitioner's Overview of Digital Discovery*, 33 Gonz. L. Rev. 347, 348 (1997). Like everyone else, members of the corporate and legal communities have become more sophisticated in their understanding and use of computers and computer data. Still, for the most part, the restraint among litigants regarding the discovery of an adversary's electronic records has long continued. Perhaps intimidation engendered by ignorance has been supplanted by reluctance spawned from a common sense of "mutual assured destruction", considering the potentially enormous expense of engaging in reciprocal electronic data discovery. Yet, despite the chill of reciprocation, a growing number of litigants are emboldened to engage in electronic data discovery by an increasingly irresistible allure: electronic mail.

#### C. E-Mail!

In 1997, Americans were estimated to spend 200 million hours per day using computers. See G. Lardner, Jr., *Panel Urges U.S. to Power Up Cyber Security*, Washington Post, Sept. 6, 1997. That same year, Time Magazine estimated that 2.6 trillion electronic mail messages passed through U.S.-based computer networks during a twelve-month period. By 2000, the number of annual e-mail messages was expected to climb to an estimated 6.6 trillion. See S. Gwynne and J. Dickerson, *Lost in the E-mail*, Time, April 21, 1997, at 88.

"In 1991, according to the Electronic Messaging Association, an industry trade group that helps corporations establish e-mail policies, 8 million Americans had access to e-mail. In 1997, the number grew to 67 million. Now, 96 million Americans use e-mail. By next year, that number is expected to increase to 108 million, with office workers exchanging 25.2 billion messages daily." D. Bennahum, *Daemon Seed*, Wired 7.05, May 1999.

## D. Why Worry?

"Most sophisticated business persons have been trained not to put damaging things on paper, but I don't think the culture's gotten there on e-mail, because people don't think of them as documents. People think of them a lot like telephone conversations." John Willems, litigation partner at White & Case, New York City, as quoted in *Electronic Discovery Proves Effective Legal Weapon*, The New York Times, March 31, 1997.

John Jessen, President and CEO of Electronic Evidence Discovery, Inc. has characterized electronic mail as a "time bomb that will come back to hurt companies whose employees don't know how to use it properly...." As quoted by

J. Temes, *E-Mail's Dark Side*, CFO: The Magazine For Senior Financial Executives, March 1993, at 13.

Examples cited by Jessen, as quoted in Daemon Seed, supra:

- 1. "Yes, I know we shipped 100 barrels of [deleted], but on our end, steps have been taken to ensure that no record exists. Therefore, it doesn't exist. If you know what I mean. Remember, you owe me a golf game next time I'm in town."
- 2. "Did you see what Dr. [deleted] did today? If that patient survives it will be a miracle."
- 3. "HI DAVID, PLEASE DESTROY THE EVIDENCE ON THE [litigation] YOU AND I TALKED ABOUT TODAY. THX LAURA"

  (Response) "\*\*\*EVIDENCE DESTROYED\*\*\* HI LAURA ACK YR MSG. AND TAKEN CARE OF. ALOHA DAVID"

And another example from Jessen, as quoted during his interview on CBS Television's 60 Minutes broadcast of June 16, 1996 in a segment entitled *For Your Eyes Only?*:

"Eric, the papers have been signed and [deleted] bank is now the owner of Parcel 15. We've made it through the whole process without alerting them to the old waste site on the Northwest Side"

#### II. A Few Points of Law

## A. *In The Beginning* - The Basic Authority.

In 1970, Fed. R. Civ. P. 34(a), pertaining to the scope of document production, was amended to include not only writings, but "data compilations from which information can be obtained [and] translated, if necessary, by the respondent through detection devices into [a] reasonably usable form." Regarding the amendment, the Fed. R. Civ. P. 34 Advisory Committee cited the need for a broader description of "documents" to accommodate changing technology. According to the Committee Note, the amendment clearly applies to electronically stored information and, in many instances, requires a respondent to produce at least a printout of computer data. See L. Youst & H. Koh, *Management and Discovery of Electronically Stored Information*, Computer L. Rev. and Tech. J. (Summer 1997). Similar amendments have been made to Fed. R. Civ. P.26(a)(1). Cf. Fed. R. Evid. 1001(1) & 1001(3), both of which have also been amended.

#### B. Caselaw to Ponder.

1. It has been held that a discovery respondent is required to produce data in digital format, although this may require the respondent to create a costly new electronic record and despite the respondent's prior production of the

requested data in "hard copy" format. See National Union Electric Corp. v. Matsushita Electric Industrial Co., 494 F. Supp. 1257 (E.D. Pa. 1980). In part, the NUE Court based its decision to compel the production of data in digital form on the Fed. R. Civ. P. 34 provision requiring requested information to be produced in a "reasonably useable form". *Id.* at 1262. See also Anti-Monopoly, Inc. v. Hasbro, Inc., supra. In this context, it's significant that experts have estimated thirty percent (30%) of electronic data never appears on paper and would not be discovered through the production of paper records, including "hard copies" of electronic data. J. Jessen & K. Shear, The Impact of Electronic Data Discovery on the Corporation, Presentation at the National Conference of the American Corporate Counsel Association in May 1994.

- 2. Similarly, it has been held that a discovery respondent must extract and produce relevant data from its computer databases, although this may require the respondent to create a new program to retrieve the data. See <a href="Oppenheimer Fund, Inc. v. Sanders">Oppenheimer Fund, Inc. v. Sanders</a>, 437 U.S. 340 (1978). Likewise, a respondent has been required to produce data sets stored on computer tapes sequentially, just as a respondent might normally organize files when producing paper documents. See <a href="Daewoo Electronis Co. v. United States">Daewoo Electronis Co. v. United States</a>, 650 F. Supp. 1003 (Ct. Int'l Trade 1986). "The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship." *Id.* at 1006.
- 3. In circumstances involving the deletion of relevant data by a discovery respondent's employee, a requesting party has been permitted to enter the respondent's premises and copy the respondent's computer hard drives in order to obtain all deleted data not yet overwritten by the respondent's computer operations. See <u>Gates Rubber Co. v. Bando Chemical Industries</u>, <u>Ltd.</u>, 167 F.R.D. 90, 100 (D. Colo. 1996) (regarding the "Site Inspection Order").

#### C. Consequences to Ponder.

"Sanctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information." **National Ass'n of Radiation Survivors v. Turnage**, 115 F.R.D. 543, 556 (N.D. Cal. 1987) (citations omitted).

This power [to sanction] is broader and more flexible than the authority to sanction found in the Federal Rules of Civil Procedure. ... The Supreme Court has described the inherent powers of the federal courts as those which "are necessary to the exercise of all others."... Deeply rooted in the common law

tradition is the power of any court to manage its affairs, "which necessarily includes the authority to impose reasonable and appropriate sanctions upon errant lawyers practicing before it."...In particular, the courts have the inherent power to enter a default judgment as punishment for a defendant's destruction of documents.

<u>Telectron, Inc. v. Overhead Door Corp.</u>, 116 F.R.D. 107, 126 (S.D. Fla. 1987) (citations omitted).

- 1. Three dangerous myths regarding the discoverability of electronic information:
  - i. So long as there is no paper copy, an opponent won't be capable of finding electronic information.
  - ii. Should opposing counsel seek discovery of electronic information, the computer has stored the most sensitive data in secure files that no one will be capable of finding.
  - iii. The technology involving the storage of data in computers allows sensitive information to be quickly and easily erased.

See P. Grady, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More Than Necessary?*, 14 J. Marshall J. Computer & Info. L. 523, 527 at n.11 (Spring 1996) (citing J. Frazier, *Electronic Sleuthing*, Law PC, August 15, 1993).

- 2. <u>Criminal Indictment</u>: <u>United States v. Lundwall</u>, 1 F. Supp. 2d 249 (S.D.N.Y. 1998). In a highly publicized case, top Texaco executives, including Lundwall, were charged with obstruction of justice and conspiracy following the discovery of audio tapes on which the executives could be heard discussing plans to destroy evidence relevant to a class action filed against Texaco alleging employment discrimination. Although the executives were subsequently acquitted of the charges by a jury, this case represents one of the very few instances in which individuals have been criminally charged with destroying records to avoid producing them in civil discovery proceedings. See R. Ziegler & S. Stuhl, *Spoliation Issues Arise In Digital Era*, The National Law Journal at B09 (February 16, 1998).
- 3. <u>Dismissal with Prejudice or Default Judgment</u>: <u>Crown Life Ins. Co. v. Craig</u>, 995 F. 2d 1376 (7<sup>th</sup> Cir. 1993). Craig sought discovery from Crown Life of all written documents relating to the calculation of commissions owed to Craig by Crown Life. Eventually, Crown Life was compelled by magistrate's order to produce all responsive documentation, which the insurer, by affidavit, affirmed it had done. Thus, Craig received only summary documentation of his commissions in the belief that no supporting data existed. At trial, evidence revealed that Crown Life maintained a database containing raw data underlying the summaries, all of which data were retrievable, but none of which was produced to Craig. Pursuant to Craig's motion, the trial court

imposed sanctions that were tantamount to a default judgment against Crown Life, when the court learned that Crown Life witnesses studied information from the database while preparing for trial. Crown Life appealed the severe sanction, contending the database's data was never specifically requested in discovery. Further, Crown Life argued that the raw data stored in the database where not "documents", because the data never existed in "hard copy" format. The Seventh Circuit was not persuaded, noting that Fed. R. Civ. P. 34 included computer data in its description of documents. *Id.* at 1383. Accordingly, the appellate court affirmed the trial court's imposition of sanctions. See also **American Bankers Ins. Co. v. Caruth**, 786 S.W. 2d 427 (Tex. Ct. App. 1990) (affirming a default judgment against a party that failed to produce requested information in discovery, allegedly because 30,000 boxes of documents had to be searched to obtain the information, thereby constituting an undue burden, although the party also maintained the information in a computer database, which was easily retrievable.)

- 4. Imposition of fines, attorney fees and costs: See Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 631-2 (D. Utah 1998) (wherein monetary sanctions were imposed against a corporation that failed to search or preserve electronic mail communications involving key employees who were previously identified as having relevant information). See also Capellupo v. FMC Corp., 126 F.R.D. 545, 551 (D. Minn. 1989) (wherein monetary sanctions were imposed against a party that engaged in intentional, systematic destruction of electronic evidence). See also Applied Telematics, Inc. v. Sprint Communications Co., 94-4603, 1996 U.S. Dist. Lexis 14053 (E.D. Pa. Sept. 17, 1996) (wherein monetary sanctions were imposed against a party that failed to prevent relevant data from being overwritten on back-up tapes, which in the normal course of business were recycled weekly).
- 5. Adverse Inference: This common law doctrine provides that a factfinder may draw an unfavorable inference against a party who has destroyed relevant evidence, because the party is assumed to have been motivated by the desire to conceal damaging evidence. Thus, when a party has failed to produce requested information, courts have imposed a sanction, based on this doctrine, in the form of an "adverse inference" jury instruction. See Fed. Jury Prac. & Instr. 12.05 (1997 Supp). See generally Nation-Wide Check Corp., Inc. v. Forest Hills Distrib., Inc., 692 F.2d 214 (1st Cir. 1982) (affirming a trial court's imposition of sanctions involving an adverse inference instruction). To this end, a court may instruct the jury that if they believe it to be appropriate, they may assume evidence made unavailable by the acts of a party or its agents would have been unfavorable to that party. See M. Bester A Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence, 6 CommLaw Conspectus 75 (Winter1998) at 83 n.123. But see **Turner v. Hudson Transit** Lines, Inc., 142 F.R.D. 68, 74-7 (S.D.N.Y. 1991) (wherein the court acknowledged the appropriateness of imposing an adverse inference sanction when negligent destruction of evidence has occurred, but only if extrinsic

evidence tends to show that the destroyed evidence would have been unfavorable to the responsible party).

## III. Responding to Discovery Requests for Electronic Records

# A. Discovery Requests, The Likes of Which Have Never Before Been Seen!

Effective discovery of electronic data will include initial comprehensive requests for information regarding the respondent's entire electronic information systems profile. These requests, propounded in the nature of document requests or a deposition of a knowledgeable party representative, should cover in detail the features of the respondent's general systems, networks, desktop and laptop computers, backup and archiving systems, electronic mail and other messaging systems, document management systems, database management systems, applications and system auditing functions. In this way, the requesting party may focus further inquiries on areas more likely to contain relevant information. A respondent's failure to adequately search all of its systems for relevant data and respond appropriately to proper electronic data discovery requests is counterproductive and risky. In addition to the sanctions previously described, a court may permit the requesting party to enter the respondent's premises and conduct its own search of the respondent's computer systems. See Gates Rubber Co. v. Bando Chemical Industries, Ltd., supra. See also J. Howie, Jr. Electronic Media Discovery: What You Can't See Can Help (or Hurt) You, Trial (January 1993) at 70.

## B. What About The Costs Involved?

"Courts have increasingly required the responding party to bear the cost of producing electronic data." Youst & Koh, *supra* at 82 [quoting C. Lovell & R. Holmes, *The Dangers of E-mail: The Need for Electronic Data Retention Policies*, 44 R.I.B.J. 7, 9 (1995)]. In **Bills v. Kennecott Corp.**, *supra*, a discovery respondent asked the court to shift to the requesting party the costs of retrieving electronic data from the respondent's computers. In denying the respondent's motion, the **Bills** Court considered four factors:

- 1. Whether the amount of money involved is not excessive or inordinate;
- 2. Whether the relative expense and burden in obtaining the data would be substantially greater to the requesting party as compared with the responding party;
- 3. Whether the amount of money required to obtain the data as set forth by the responding party would be a substantial burden to the requesting party; and
- 4. Whether the responding party is benefited in its case to some degree by producing the data in question.

Bills v. Kennecott Corp., 108 F.R.D. at 464. In reaching its decision, the court observed: "...that information stored in computers should be as freely discoverable as information not stored in computers...the party responding [to discovery requests] is usually in the best and most economical position to call up its own computer stored data." Id. See also In re Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526 (N.D. Ill. 1995), wherein the court held that a discovery respondent must bear the estimated \$50,000 to \$70,000 cost to compile, format, search and retrieve responsive data from approximately 30 million pages of e-mail data stored on its back-up tapes. In so ruling, the court concluded the respondent alone should bear the extraordinary costs of the production, reasoning: "...if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk". Further, the court observed that the requesting party had no control over the respondent's record-keeping scheme. See generally Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999)(courts seek to balance the equities of the circumstances, in determining which party must bear the costs of producing electronic data). But see e.g. **Anti-Monopoly, Inc. v. Hasbro, Inc.**, supra, wherein the requesting party was ordered to bear some of the costs associated with discovery of electronic information.

# C. <u>Preserving Electronic Data - When To Begin.</u>

While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.

William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443, 1455\_(C.D. Cal. 1984) (citations omitted and emphasis supplied). In this case, the court entered a default judgment against G.N.C. when it determined that G.N.C. destroyed records, including electronic data, after service of the complaint, but before discovery requests were propounded. See In re Prudential Ins. Co. Sales Practices Litig., 169 F.R.D. 598 (D. N.J. 1997), wherein the court ordered Prudential to preserve all documents relevant to a class action brought by policyholders. Although Prudential directed its employees to preserve information pursuant to the court order, some relevant information was nevertheless negligently destroyed due to Prudential's "haphazard and uncoordinated approach to document retention". *Id.* at 615. Consequently, the court sanctioned Prudential by imposing a \$1 million fine, ordering the payment of plaintiffs' attorney fees, and further ordering Prudential to promulgate a formal, company-wide document retention policy. *Id.* at 607-12 and 616-17.

## IV. Coping With the Risks and Burdens of Electronic Evidence Discovery

#### A. Records Retention Programs.

"The best way to avoid any appearance that documents have been destroyed in order to avoid production in litigation is to establish a document retention program that is designed for the selective retention and destruction of documents." Youst & Koh, *supra* at 86.

- 1. Document retention programs have been described as procedures for the systematic review, retention and destruction of documents received or created in the course of business. See, C. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 Iowa J. Corp. l. 417, 419 (1999). This description applies to electronic data retention programs, as well.
- 2. "The vast majority of large business enterprises now have some formal document management program. Nevertheless, some companies still approach document retention and destruction in an *ad hoc* manner." L. Solum & S. Marzen, *Truth and Uncertainty: Legal Control of the Destruction of Evidence*, 36 Emory L. J. 1085, 1185 (1987) (footnote omitted). "While most clients have document retention policies, few clients apply those policies to electronic information." Committee on Federal Courts, *Discovery of Electronic Evidence: Considerations for Practitioners and Clients*, 53 The Record 656, 667 (Sept./Oct. 1998).
- 3. Advantages and Disadvantages of a Written Document Retention Program. J. Fedders & L. Guttenplan, *Document Retention and Destruction: Practical, Legal and Ethical Considerations* 56 Notre Dame Law. 5, 13 (1980):

#### Four advantages-

- [t]he elimination of the onerous expense of storage of irrelevant and obsolete documents;
- a reduction in the burden and cost of retrieval of documents in response to business requests, government investigations or litigation;
- a substantial reduction of legal risks flowing from documents, particularly those which are hastily drafted, erroneous or misleading; and
- the avoidance of an adverse inference from the non-production of documents in litigation.

#### Six disadvantages-

- the expense of establishing and administering a program, including the commitment of human and capital resources needed to assure compliance;
- the inability to prove a fact affirmatively, because documents have been destroyed;
- a diminished flexibility of response to formal and informal requests for documents;
- the adverse inferences arising from incomplete compliance with the retention program;

- the adverse inferences arising from selective destruction outside the boundaries of the program (selective destruction appearing less corrupt without a program); and
- other adverse legal effects, including the discoverability of the program.

## B. A Slight Conceptual Problem!

In <u>Carlucci v. Piper Aircraft Corp.</u>, 102 F.R.D. 472 (S.D. Fla. 1984), the trial court sanctioned Piper by entering a default judgment against the defendant after determining that Piper employees systematically reviewed and destroyed potentially harmful documents. <u>Remarkable</u>, in the court's opinion, was the fact that Piper's practice of destroying documents occurred pursuant to a policy, which had a stated purpose of destroying records that might be harmful to the company in litigation. *Id.* at 485-6. Yet, the judge noted: "I am not holding that the good faith disposal of documents pursuant to a *bona fide*, consistent and reasonable document retention policy can not be a valid justification for a failure to produce documents in discovery." *Id.* at 486.

# C. And Two Key Mistakes Worth Avoiding.

There are two serious mistakes that can be made when instituting [a document retention] program. First, conducting the program on an *ad hoc* basis and second, conducting it on a selective destruction basis. An *ad hoc* approach may take place, for example, when additional space is needed or when files are very old. This approach is typically disorganized and may not destroy all copies of the desired documents, or it may destroy documents that must, by law, be retained. A selective destruction is usually triggered by some event, such as an investigation or lawsuit....embarking on this type of program can be very dangerous due to the exposure of the party destroying the documents to potential civil and criminal liability.

Youst & Koh, *supra* at 86-7.

## D. Fundamental Components of a Valid Records Retention Program.

- 1. Systematically develop the records retention program.
- 2. Address all your records in the records retention schedules, including reproductions.
- 3. Address all media in the records retention schedules, including microfilm and machine-readable computer records.
- 4. Obtain written approvals for the records retention schedules and the program procedures.
- 5. Systematically destroy records when permitted by the records retention program.
- 6. Control and manage the operation of the records retention program.

- 7. Stop destroying records, even when permitted by the records retention program, when litigation, government investigation or audit is pending or imminent.
- 8. Maintain documentation supporting the development and implementation of the records retention program, including records retention schedules, procedures, changes in procedures, approvals, legal research and listing of records destroyed.

# See D. Skupsky, **Recordkeeping Requirements**, §2-10 (1991).

#### E. Guidelines for the Development of a Records Retention Policy.

The policy to be formulated should incorporate the following requirements:

- 1. that documents maintained in accordance with applicable laws and regulations be preserved for as long as necessary, but in any event for a term not to exceed a specified number of years;
- 2. that documents required for the conduct of business be filed in a systematic manner and be accessible whenever necessary;
- 3. that documents relevant to foreseeable or pending litigation and other judicial or governmental investigations or proceedings be identified and preserved;
- 4. that documents required to be permanently maintained are catalogued and reduced to electronic media for convenient and economical storage and access;
- 5. that all other documents be destroyed;
- 6. that audits of all electronic data be regularly conducted to assure compliance with the retention policy provisions;
- 7. that a mechanism be established which assures the immediate suspension of data destruction occurring pursuant to provisions of the retention policy; and
- 8. as a guiding principle, that the retention policy assures any uncertainty as to its application be always resolved in favor of retention.

See W.F. Reinke, Limiting the Scope of Discovery: The Use of Protective Orders and Document Retention Programs in Patent Litigation, 2 Alb. L. J. Sci. & Tech. 175 (1992).

## F. Tasks Specifically Relating to the Management of Computer-Stored Data.

- 1. Profiling the company's computer systems to determine how they work in an operational context. This profile needs to include a review of the hardware and software in use, an inventory of the electronic media available, such as computer tapes and disks, and an analysis of the accumulated or stored information.
- 2. Creating an electronic information database that indexes electronic media and details the file sets contained in that media.

- 3. Developing and implementing policies and procedures regarding information creation and retention.
- 4. Periodic review and audit of the information systems.

K. Shear, *Electronic Evidence; It's Not 'Cutting Edge' Anymore. Disregard it at Your Peri*", Law. PC at 2, (August 1, 1994).

# G. "Reasonableness" Standard for Records Retention Programs.

In Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988), Remington appealed a jury verdict of liability for injuries sustained by Lewy resulting from an accidental discharge of a shotgun. Specifically, Remington argued that the following jury instruction was inappropriate: "If a party fails to produce evidence which is under his control and reasonably available to him and not reasonably available to the adverse party, then you may infer that the evidence is unfavorable to the party who could have produced it, but did not." Id. at 1111. Lewy sought and obtained this jury instruction, because Remington had been unable to produce documents, which were destroyed pursuant to Remington's document retention policy. Remington contended that the documents were destroyed according to routine procedures and should not, therefore, give rise to an adverse inference. Id. The Eighth Circuit reversed and remanded the case, setting forth several factors to be considered by district courts in determining whether or not sanctions are appropriate when a party is unable to produce evidence, because the evidence was destroyed pursuant to a document retention program. *Id.* at 1112. First, the trial court must determine whether [the delinquent party's] record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents: "For example, the court should determine whether a three year retention policy is reasonable given the particular document. [It] may be sufficient for documents such as appointment books, but inadequate for documents such as customer complaints". Id. Then, the court must consider the extent to which the destroyed documents were relevant to pending or probable lawsuits: "In making this determination, the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints and the magnitude of the complaints.". Id. Finally, the court must consider whether the document retention policy was instituted in bad faith: "In cases where a document retention policy is instituted in order to limit damaging evidence available to potential plaintiffs, it may be proper to give an instruction similar to the one requested by [Lewy]". Id.

## H. One Final, Troubling Thought.

Significantly, in <u>Lewy</u>, the Eighth Circuit observed that the retention of certain documents might be compelled by circumstances, despite the existence of a document retention program: "[I]f the corporation knew or should have known that the documents would become material at some point in the future, then such documents should have been preserved.... [A] corporation cannot blindly destroy

documents and expect to be shielded by a seemingly innocuous document retention policy." *Id*.

#### V. Conclusion

If you've responded to electronic data discovery requests, then you know well the enormous amount of time and expense involved in responding to them. If you haven't yet encountered these discovery requests, then the trend may soon overtake you. In either circumstance, you company's ability to respond efficiently and effectively to the next set of electronic data discovery requests it confronts depends largely on what preparations your company makes now. In both legal and practical terms, acting later is simply acting too late.

Consider for a moment: Is your company able to identify all of its electronic data and locate every place where its data is stored? Can your company retrieve any of its data, regardless of the data format or the type of media on which the data is stored? Does your company have an electronic records retention policy? Does your company apply and enforce the policy uniformly and consistently? Do employees always use your company's e-mail system appropriately and responsibly? Can all messages generated on your company's system be characterized as correct and businesslike in form and content? A negative response to any of these questions is a warning worth heeding. Well-crafted electronic data discovery requests could expose embarrassing, perhaps legally compromising information buried deep within your company's electronic records. They could also trigger extremely costly searches and legal analyses of your company's unnecessarily comprehensive electronic databases, archives and back-up tape depositories.

Clearly, you simply can't wait to "cross that bridge when you come to it". In today's litigious environment, you and your company are already there.

These seminar materials are intended to generally educate the participants on current legal issues. They are not intended to provide legal advice. Accordingly, these materials should not be relied upon without seeking specific legal advice on matters discussed herein. Copyright © 2000 Cozen and O'Connor. ALL RIGHTS RESERVED.