APPLIED DISCOVERY WHITE PAPER

Document Retention & Destruction Policies for Digital Data

What You Don't Know *Can* Hurt You

LexisNexis®
Applied Discovery®

Businesses have benefited from the use of computers since the 1970s. Technological advances, including sophisticated email systems and desktop Internet access, have made the use of computers easier and more prevalent than ever. For most businesses, corporate communications—including confidential and sensitive information—occur more frequently in email messages than in memos or letters. Other business documents, including contracts, budgets, and meeting minutes, are frequently created, reviewed, revised, approved, and emailed to numerous recipients without ever being reduced to printed form. The various drafts and versions of these documents, along with corresponding backup copies, may be stored on a company's computers for years.

Many attorneys, including in-house counsel, litigators, and mergers and acquisition specialists, now realize the importance of electronic data in the legal process. While electronic documents are still sometimes printed for production, legal professionals and their clients are confronted more and more with requests for data in its native electronic form. Sensible preparation prior to an electronic discovery request is the best way to minimize the potential for costly surprises.

Electronic Discovery—an Overview

Electronic data has been recognized as discoverable evidence in federal court for more than thirty years. Fed. R. Civ. P. 34, which governs the production of documents between parties, includes electronic data in the description of "documents" that are subject to production. The 1970 Amendments to Rule 34 specifically state that the definition of "documents" shall include "electronic data compilations," even when the electronic data can be obtained only with the use of "detection devices" or from "the electronic source itself."

Though the Federal Rules supported the discovery of electronic data for three decades, practitioners were slow to exploit this opportunity. In recent years, however, electronic discovery requests have increased, and courts routinely hold that a producing party has a duty to provide discoverable electronic data. "Electronic documents are no less subject to disclosure than paper records." *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

Email messages are discoverable and may be introduced into evidence when properly authenticated. *See, e.g., U.S. v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000). Even information never reduced to paper format and stored only in electronic form is discoverable if there is a likelihood that it is relevant to the litigation. *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999)("[B]y requesting 'documents' under Fed. R. Civ. P. 34, Plaintiff also effectively requested production of information stored in electronic form.") *See Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) (defendant required to make computers available to plaintiff's expert so relevant deleted files could be available for discovery); *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622, 632 (D. Utah 1998) (party allowed to perform limited keyword search of opposition's electronic databases), *aff'd in part, rev'd and remanded in part*, 222 F.3d 1262 (10th Cir. 2000), *cert. denied*, 534 U.S. 945 (2001).

Some recipients of electronic discovery requests have attempted to thwart the opposition's efforts to review electronic data in its native form by producing the requested documents in print form. Such responses may be found deficient. Courts have held that reducing such data to paper form does not necessarily relieve a producing party from the duty to provide the information in electronic form. *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 U.S. Dist. LEXIS 16355; 1995-2 Trade Cas. (CCH) P71,218 (S.D.N.Y. 1995). *See also Storch v. Ipco Safety Products Co. of Pennsylvania*, 1997 U.S. Dist. LEXIS 10118, *6; 134 Lab. Cas. (CCH) P33,560 (E.D. Pa. 1997)("[I]n this age of high-technology where much of our information is transmitted by computer and computer disks, it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff.") In *American Brass v. U.S.*, 699 F. Supp. 934, 938 (Ct. Int'l Trade 1988), the court held that the size and complexity of printouts of electronic data warranted additional production of data in more usable electronic form.

The December 1, 2000, "mandatory disclosure" amendments to Rule 26(a)(1) further increased the burden on producing parties to disclose the existence of electronic documents and other information when a lawsuit is commenced. These changes, coupled with the growing body of case law concerning production of electronic data, mandate that businesses prepare in advance for electronic discovery requests.

The Importance of a Document Retention Policy

A competent and consistently enforced document retention policy reduces a company's risk by ensuring that electronic data is handled properly. Some companies operate without any formalized plan for document retention and destruction. Others have policies in place but fail to include electronic data in their protocol. Even the most proactive company with a comprehensive retention policy that includes electronic data may not be enforcing the policy to the extent necessary to avoid legal risk.

Although many companies know they will face increasing discovery demands for electronic documents in the future, most are not prepared to respond. An ABA survey conducted in May 2000 asked litigators whether their clients had an established protocol for handling electronic discovery requests. A staggering eighty-three percent said no. Seventy percent of the same group said they expected electronic discovery to increase "dramatically" in coming years.[1]

[1] As of June 2004, changes to federal rules to account for electronic discovery were under consideration, and federal courts in Delaware, Kansas, New Jersey, Arkansas, Florida, and Wyoming had implemented local rules specific to electronic discovery practice. State courts in states such as California, Texas, Illinois, and Mississippi also have adopted rules relating to electronic discovery.

A document retention policy formalizes a company's protocol for saving and discarding documents received or created in the ordinary course of business. Such a policy may aid a company in litigation when documents were properly destroyed pursuant to the plan in place; conversely, failure to enact a competent policy may undermine a company's position in litigation, and failure to protect information subject to discovery can have dire consequences. *See, e.g., Telectron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107 (S.D. Fla. 1987)(Sanctions available under Fed. R. Civ. P. 37 for discovery abuse include default judgments and dismissal.) While some documents must be retained for a specific period of time pursuant to federal or state law (for example, tax documents or workplace records governed by OSHA or FLSA), many business documents fall outside these mandates. These documents, including email and other electronic data, often contain key evidence sought by an opposing party in litigation. The decision to retain or destroy certain documents may prove critical in a court's eyes.

Electronic documents present more risks than their paper counterparts. Email messages in particular have proven detrimental to numerous companies because they are often perceived by their authors and recipients as casual in nature. Comments once uttered only in person or by telephone are now sent by email and often unintentionally preserved. Unlike paper documents, large amounts of electronic data can be stored in a small space, allowing years of electronic documents to be kept without any outward sign of accumulation. This results in the retention of useless and potentially damaging information.

To complicate matters further, copies of electronic documents usually exist in numerous locations in the company's "electronic filing cabinet." When a document is created or revised, a copy of the document is stored in a temporary file. Another copy of the document is made when the company's system is backed up. Today's mobile workforce presents additional challenges, as copies of documents are frequently saved on laptops, disks, or in various other drives. Still other copies are generated when documents are passed around for review by email, and the email messages themselves reside in the archives of the author and each recipient.

Even when a computer user intends to discard electronic data, the task is much easier said than done. The "delete" key creates a false sense of security for many people. A deleted document may no longer be visible to the user, but copies remain in temporary files, on backup tapes, and in the case of email, in other recipients' in-boxes. An adverse party may discover all these sources and have the advantage of uncovering documents presumed deleted, or multiple drafts of a document intended to be saved only in its final form.

There are numerous situations in which a company may face unnecessary consequences due to inadequate or improperly enforced document retention procedures. Evidence discovered in documents retained far longer than necessary may expose a company to unforeseen liability. A company may also haphazardly destroy documents that should have been retained, making it susceptible to claims of spoliation even when no intentional destruction of documents is alleged. Either situation is dangerous; both can be avoided.

An effective document retention policy reduces the search, retrieval, and production costs of discovery when stored documents must be produced. When electronic data is organized, a company's ability to foresee and react to potential documentation problems is enhanced. A retention policy also highlights problems in the system that must be addressed. Taking simple preventative steps while no document request is pending avoids a potential crisis situation at a later date.

Document Retention Law and the Consequences of Spoliation

Companies operating without valid document retention policies, or failing to follow existing policies, place themselves in a position of unnecessary risk for claims of spoliation. Failure to retain electronic data in the face of litigation may subject a party to monetary sanctions. *See, e.g., Applied Telematics, Inc. v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa. 1996) (defendant's unintentional failure to preserve electronically stored routing plans resulted in order for payment of plaintiffs' costs and attorney fees).

Even before litigation is commenced, companies have a duty to preserve documents that may be relevant to pending or even potential litigation. *Capellupo v. FMC Corp.*, 126 F.R.D. 545, 551 (D. Minn. 1989) (court found willful destruction of documents related to gender discrimination lawsuit and ordered defendant to pay twice the total of plaintiffs' attorney fees and costs incurred in investigating, researching, preparing, arguing, and presenting all motions related to the issue of document destruction, and additional fees for unnecessary consumption of the court's time). Claims of spoliation may also result in jury instructions allowing a "spoliation inference" based on the inability of a party to produce requested documents. *Linnen v. A.H. Robins Co., 1999 Mass. Super. LEXIS 240,* at *11 (Mass. Super. June 16, 1999).

Simply setting a document retention policy is not enough to protect a company from claims of spoliation. The policy must be valid and consistently enforced. Some courts have clearly defined standards for determining whether a company's document retention policy is valid. The Eighth Circuit set out such a standard in *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988). The *Lewy* court reviewed the defendant firearms manufacturer's document retention program on appeal when submission of a "general negative inference" jury instruction was given following the company's inability to produce certain documents—including information concerning customer complaints—that had been destroyed pursuant to its corporate record retention policy. The appellate court remanded the issue to the trial

court for further consideration of the retention policy, setting out the following issues for consideration: (1) whether defendant's policy was reasonable considering the facts and circumstances surrounding the relevant documents (e.g. a three-year retention period may be sufficient for standard documents such as appointment notes or telephone messages, but may not be sufficient for records of customer complaints); (2) whether lawsuits concerning the complaints or related complaints had been filed, the frequency of such complaints, and the magnitude of the complaints; and (3) whether the document retention policy was instituted in bad faith. *Id. at 1112*. The *Lewy* court concluded that some circumstances may compel the retention of certain documents notwithstanding a general retention policy, such as when a corporation knows or should know that the documents would become material at some point in the future. *Id.* A corporation may not blindly destroy documents pursuant to a stated policy and expect to be shielded from liability in all circumstances. *Id.*

If challenged, a company's document retention plan will most likely be held to a reasonableness standard similar to that set out by the Eighth Circuit in *Lewy*. *See, e.g., Wm. T. Thompson Co. v. General Nutrition Corp., Inc.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984) ("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.")

An improper, unreasonable, or unenforceable document retention policy may be just as harmful as no policy at all. *See, e.g., Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984) (default judgment granted against the defendant following destruction of records to eliminate documents that might be detrimental to the defendant in litigation). The lack of a valid and properly enforced retention policy may lead to grave consequences such as the default judgment entered in *Carlucci*.

So how can a company sensibly prepare for electronic discovery requests? The risk of unnecessary liability or sanctions is substantially reduced if a company's electronic documents are properly organized and maintained. Disorganization creates an inability to access documents when they are requested. If the documents are located late in the discovery phase or uncovered from some other source, it may appear that the information was purposefully withheld or fabricated. An effective, consistently enforced document retention policy helps prevent these situations while ridding the business of unnecessary documents altogether.

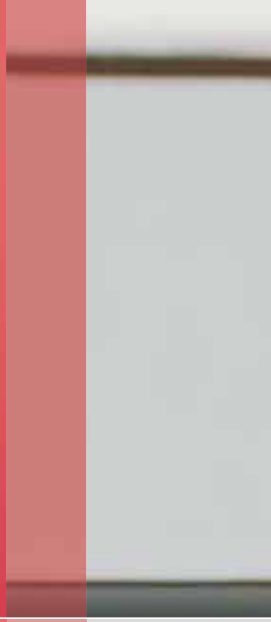
Ten Tips for Avoiding Document Retention Disasters

In light of the increased attention electronic discovery has received in recent years, every company should develop a document retention policy that includes digital data. The following recommendations provide a good starting place for avoiding unnecessary risk:

1. Practice competent pre-litigation planning—develop a policy and enforce it. Know what is being stored, where it is stored, and how long the company must keep it to comply with applicable statutes and court rulings in the subject jurisdiction. Be sure to include electronic data in the policy.
2. Involve the company's technology department in decisions regarding the policy's parameters and methods for enforcement. Remember that the IS or IT department is usually charged with a duty to keep the system from losing any data, and those departments may not realize the implications of keeping too much data for too long.
3. Establish clear accountability for enforcement of the policy. While an executive-level technology employee may be responsible for overall enforcement, be sure the staff handling the daily procedures is educated about the importance of the policy and held accountable for following the guidelines in place. Know in advance who may be called upon to testify about the company's document retention procedures and educate that person in advance of a crisis.
4. Educate all of the company's computer users about the pitfalls of electronic communications. Here is a good rule of thumb for email—before hitting "send," consider whether you would want your employer, your mother, or a jury to read the message. If the answer is no, the message should not be sent. Employees should have no false expectations of privacy in any information on the company's computer system.
5. Teach employees how to manage their electronic data. As a routine matter, decide which business documents must be kept and which can be discarded on a regular basis. Educate employees about these decisions. Advise them about the legal ramifications of deleting information once the company is on notice of a lawsuit or other legal document request.
6. If the policy states that certain unnecessary records will be purged at regular intervals—whether electronic or paper—be sure the policy is consistently followed.
7. Consider segregating business email and personal email by applying different retention standards. A company may even wish to set standards for automatic deletion of email unless the author or recipient makes a conscious decision to store the message as a business record.
8. Immediately reconsider and be prepared to suspend regular retention and destruction procedures when litigation or a legal document request is pending or imminent. Have a plan in place for quickly notifying all necessary staff when this action must be taken.

9. Involve the technology department again when litigation or any form of document request is imminent. Make informed decisions about how best to alter the company's usual retention policy, if necessary.
10. Periodically conduct an internal audit of the company's retention policy. It will be easier to argue the policy is reasonable if it is reexamined and any necessary adjustments are made on a regular basis.

While no document retention policy can provide a fail-safe plan for avoiding liability at the hands of electronic data, an educated, methodical approach to the retention and destruction of electronic documents will fare well in the eyes of most courts.



For updated summaries of electronic discovery case law, visit Applied Discovery's online Law Library at **www.lexisnexis.com/applieddiscovery.**

LexisNexis®
Applied Discovery®