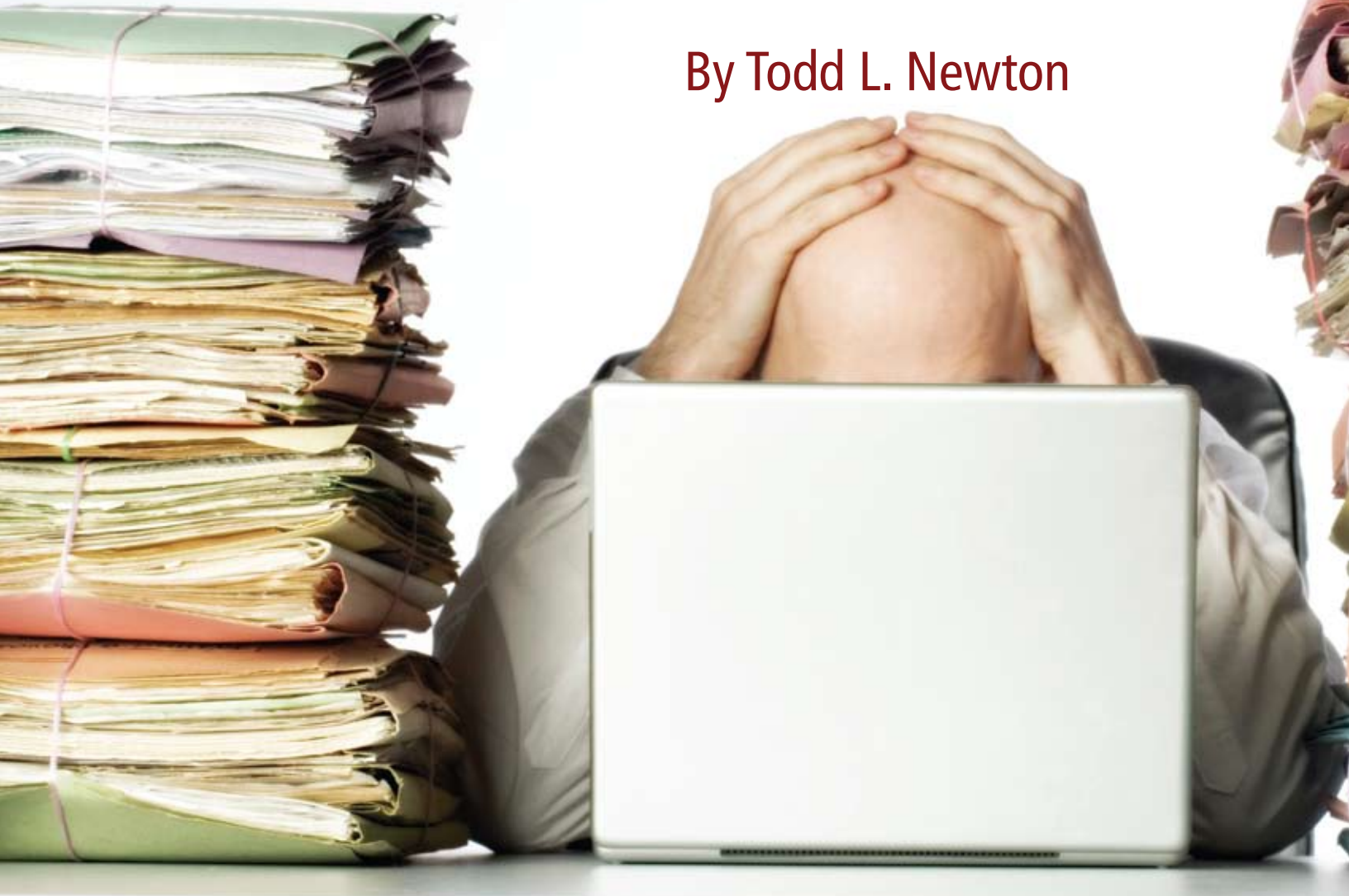


E-Discovery and Record Retention: When Two Worlds Collide

By Todd L. Newton



It's been over a year since the amendments to the Federal Rules of Civil Procedure governing electronic discovery went into effect. By now, we're all somewhat familiar (or at least should be) with the amendments and one key fact: the confirmation that electronic evidence is subject to the rules of discovery just like any other type of evidence. Thus, it must be preserved and produced in a timely fashion upon request. That sounds simple enough, right? Perhaps not, given the fact that electronic records can be (and usually are) far more voluminous than traditional paper records, thus complicating the task of searching for and producing them in the heat of a discovery battle. Scott Dodson's article in this issue provides an excellent summary of some of the complexities that electronic evidence adds to the mix. The goal of this article is to demonstrate how the e-discovery amendments require more planning in advance, beginning with the record retention policies of the client, in order to avoid the risk of spoliation and all of the potential consequences that follow. Indeed, the amendments themselves provide some good clues about what clients need to consider regarding their own record retention policies, including what they keep, where they keep it, and how they can produce it.



“From these rules, it is clear that the path to being prepared for ‘E-Day’ consists of three things: knowing what your clients have; knowing where they have it (and whether it’s ‘reasonably accessible’); and knowing how to preserve and produce it when required to do so.”

The Amendments: The Starting Point for Effective Record Retention

By reviewing some of the amendments, we can begin to see the types of things that clients will need to consider (and their attorneys will need to understand) about what records they keep, where they keep them, and how they can produce them. **Rule 16(b)(5)** and **(6)** requires the court’s scheduling order to include provisions regarding the disclosure of electronically stored information (ESI). That sets the stage for the first consideration: what information does the client keep in electronic format? When most people think about electronic discovery, one word comes to mind: email.



Todd Newton is counsel for Mitchell Williams in Little Rock. He serves as team leader of the firm’s Information Management and Security practice.

There's good reason for that given the fact that most people in the business world, including our own, use email on a daily basis to conduct at least some portion of their business, potentially giving rise to the "smoking gun" pertaining to a potential future lawsuit. However, electronic discovery covers more than just email because there is a wide variety of information that is stored electronically: instant messages, text messages, faxes, spreadsheets, letters, drafts, memos, voicemail, and the list goes on and on. So, from the outset, clients must know the various types of electronically stored information they keep – which will simplify the attorney's responsibilities under the next rule.

Rule 26(a)(1)(B) requires the parties to provide other parties with a copy "or a description by category and location" of ESI without waiting for the other parties to request it. Similarly, **Rule 26(b)(2)(B)** provides that only ESI that is "reasonably accessible" must be initially produced, while providing the means for the requesting party to establish good cause why ESI that is not reasonably accessible should still be produced. These amendments demonstrate yet another factor that attorneys and clients alike must consider. Besides knowing *what* ESI exists, the client must know and the attorney must disclose *where* such information exists. If ESI is reasonably accessible, it must be disclosed. If, however, ESI is retained only on backup tapes that are kept for business continuity purposes, then there may be an argument that such information is not reasonably accessible and does not have to be initially produced. Given the speed with which discovery commences, the answers to these questions must be known sooner rather than later, and waiting until the lawsuit is filed is simply too late.

Rule 26(f)(3) and **(4)** requires the parties to discuss ESI during their initial conference. Specifically, the rule requires the parties to discuss the form of production, preservation obligations, and the procedures for dealing with inadvertent disclosures of potentially privileged information. **Local Rule 26.1(4)** of the United States District Court, Eastern District of Arkansas, expands on these provisions by requiring the parties to include in their Rule 26(f) report the following: whether disclosure of ESI will be limited to that which is "reasonably available" in the ordinary course of business; the anticipated scope, cost, and time required for the disclosure or production of data that is not reasonably available; the format of production and the procedures for production; whether reasonable steps have been taken to preserve potentially discoverable data from alteration or destruction; and other problems that the parties anticipate may arise in connection with the discovery of ESI. These rules further demonstrate that clients need to know *what* they have, *where* they have it, and *what form* it's in before the discovery process even begins.

From these rules, it is clear that the path to being prepared for "E-Day" consists of three things: knowing *what* your clients have; knowing *where* they have it (and whether it's "reasonably accessible"); and knowing *how* to preserve and produce it when required to do so. The remainder of this article will focus on knowing what your clients have or, more importantly, making sure your clients know what they have. By knowing what is being retained, clients are in a much better position to respond to a request for electronic evidence and to halt the destruction of electronic evidence that might otherwise be destroyed. This is where an effective record retention plan can save the day.

Even before the e-discovery amendments took effect, it was clear that courts took a dim view of companies that failed to preserve evidence and even those that could not locate pertinent evidence because of the manner in which it was stored. In response to one company's argument that responding to a discovery request would impose an undue burden because its records were not retained in such a fashion to facilitate recovery, one court was critical of the company's "opaque data storage system," particularly when the company could expect frequent litigation due to the nature of its business. *Zurich American Insurance Co. v. Ace American Reinsurance Co.*, No. 05 Civ. 1970 (RMB) (JCF), 2006 U.S. Dist. LEXIS 92958, at * 5 (S.D.N.Y. Dec. 22, 2006). Moreover, with the safe harbor provision in Fed. R. Civ. P. 37(f), clients will clearly benefit from having (and enforcing) a record retention plan because it can limit their exposure to potential sanctions in the event that ESI is "lost as a result of the routine, good-faith operation of an electronic information system." By having a record retention plan in place, the client will be in a position to operate more efficiently by knowing what records it keeps and where those records are located, and it will be able to produce those records much more quickly when litigation commences or the threat of litigation arises.

So what records must the client keep and how long should it keep them? The answer to both questions is the same and is the one that most, if not all, clients hate to hear: it depends. Specifically, it depends on the nature of the client's business and the laws and regulations that govern that type of business. In other words, there is no such thing as a "one-size-fits-all" record retention policy because every business is different. The health care provider maintains different types of records than the financial institution. While there are certain types of records that all businesses maintain (personnel files, bank statements, etc.), each business is different. Some businesses may keep different records than other businesses in the same industry, depending on the needs of the individual business. The result, then, is that attorneys must ensure that their clients have effective record retention policies in place that are tailored to their clients' businesses and that those policies are enforced.

Steps to Developing An Effective Record Retention Policy

While the following steps do not comprise all of the factors that should be considered when formulating a record retention policy, they will hopefully provide a good starting point. First, the client should establish goals for the record retention policy. For any business, this simply means that the policy will strive to establish that its records will be kept in such a way that they can be retrieved when needed (whether for business purposes or in response to litigation or investigation) and destroyed when no longer needed. Unfortunately, most companies find it much easier to keep electronic information much longer than necessary than destroy it when they no longer need it because the storage capacity of today's computer systems and storage devices is monstrous. Even the little flash drives that fit on a key ring can hold several gigabytes of data. While that capability is extremely useful, it also creates the equivalent of a digital junk drawer: we save electronic information with the notion that one day we'll get rid of it. The reality, however, is that too much information is being saved on networks, hard drives, and other storage media all

E-discovery continued on page 40

E-discovery continued from page 18

over the country that is rarely, if ever, being accessed again. If you don't believe me, take a look at your computer folders or, even better, your email Inbox. An effective record retention policy will ensure that pertinent records are being kept so long as there is a business need or legal obligation to do so.

Second, for any record retention plan to succeed, it must be supported by management. A policy that is not supported and enforced by management is a policy that is doomed to fail. Even worse, an unenforced policy could subject a client to potential sanctions if it appears that the client violated its own policy in handling records subject to discovery. With management "buy-in," a client can ensure that the record retention policy it creates will be enforced.

Third, assemble a team of individuals from different departments such as IT, human resources, accounting, and legal to assist in the creation of the record retention policy. While we attorneys generally believe that we are capable of crafting policies to cover just about any conceivable scenario, the reality is that a policy may be legally sound but practically impossible to carry out. An impractical policy that does not take into account the different needs of different departments is also doomed to fail.

Fourth, conduct an inventory of records maintained both electronically and on paper and the location in which such records are maintained. Records maintained in filing cabinets are the easy ones; those maintained only on computers of certain individuals or on laptops, flash drives, or home computers used for business purposes are a different matter altogether. Thus, interviewing a client's employees to determine what records they produce and where they maintain them is critical because that may be the only way to know all of the types of records, paper and electronic, that are being kept and where they might be located. It will also help determine whether certain types of records possess some historical value that might warrant keeping them for a longer period of time than might otherwise be required.

Fifth, once the inventory is complete, assign retention periods to each category of records based on federal law, state law, industry standards, and potential statutes of limitations that could apply. With respect to federal law, there are numerous statutes and regulations (Sarbanes-Oxley, ERISA, HIPAA, and OSHA regulations, to name a few) that specify retention periods for certain types of records. Similarly, there are also numerous state laws that govern the types of records that businesses must maintain. For example, there are statutes governing the retention of banking records (Ark. Code Ann. § 23-46-511), corporate records (Ark. Code Ann. § 4-27-1601), and employment records (Ark. Code Ann. §§ 11-2-115, 11-4-218). Lastly, statutes of limitations should also be considered. If a business has contracts with various vendors or customers, it is possible that a breach of contract action could arise. Because the statute of limitations in Arkansas for a breach of contract claim is three years after the cause of action accrues, a business should consider retaining a copy of its contracts and any supporting documentation for at least that long, if not longer.

Sixth, an effective record retention policy must include a litigation hold procedure for ensuring that records that are subject to discovery are maintained until the basis for the hold no longer exists. Spence Fricke's article in this issue provides an excellent overview of litigation hold issues, so I won't go into details about litigation hold procedures except to say this: the litigation hold obligation cannot be carried out without the input and assistance of the IT department. Therefore, when devising the procedures for halting the deletion or overwriting



of electronically stored information, members of the IT department must be involved.

Seventh, include destruction procedures in the record retention policy. If that seems a little contradictory, the reality is that records that no longer satisfy a business need or are no longer legally required to be kept should be destroyed in a timely fashion according to the record retention schedule and established procedures. There are numerous reasons for this including preservation of resources. However, there are plenty of horror stories about the "smoking gun" memos or emails that came to light several years down the road that might never have seen the light of day, much less the glare of a courtroom or television cameras, if a record retention policy had been followed. Having said that, one point should be made crystal clear: there is difference between destroying records to obstruct an investigation versus following a valid record retention policy and destroying records at a predetermined time when there is no legal obligation to retain them. As the United States Supreme Court stated in *Arthur Anderson v. United States*, 544 U.S. 696, 704-05 (2005), "Document retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances."

Eighth, review the policy annually and monitor for compliance. A valid record retention policy is not something that is drafted, enacted, and placed behind glass. To the contrary, it is something that should be reviewed annually to ensure that it's workable, that it's being followed, and that records that need to be retained are being retained. An annual review will also provide the opportunity to revise the retention periods in the event the business need for retaining records has changed. Further, an annual review provides a good opportunity to re-educate employees concerning the policy to ensure that it is being followed. After all, if called upon to defend the destruction of records that only later became material to a lawsuit, a company will be in a much better position if it can establish that the records were destroyed pursuant to an enforced policy on which employees were thoroughly trained.

Conclusion

While the amendments to the Federal Rules of Civil Procedure provide a framework for the production of ESI, they also provide the incentive for clients to implement and enforce a record retention policy. It is also clear that the courts are increasingly requiring attorneys to familiarize themselves with their clients' record retention policies in order to ensure full compliance with the amendments. Given the stiff penalties that courts are imposing on parties who fail to preserve and produce ESI, there is no better time than the present to bridge the gap between the requirements of the amendments and the record retention policies of our clients. ■