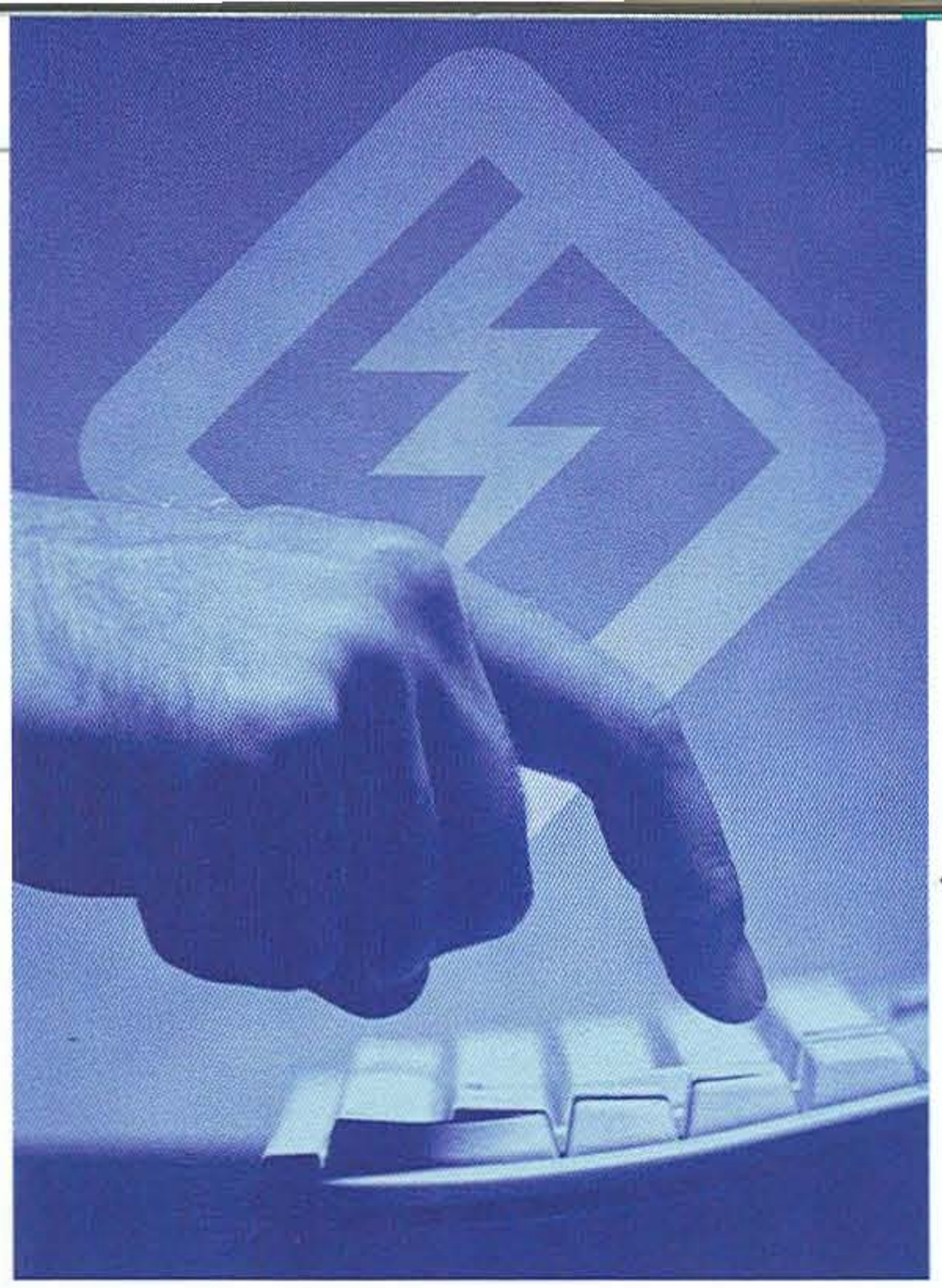
If Your Computer Could Talk...

Electronic data should be retained and destroyed based on company policy that is compliant with laws governing the company's industry.

By Khristi Doss Driver and Kelly J. Todd



THE TECHNOLOGY YOU PROVIDE TO YOUR customers is cutting edge, but are you on top of what the technology being used inside your company can do to you? Are documents on your computer systems lying in wait to destroy your profitability? Today's increasingly technological workplace presents unique legal responsibilities and pitfalls related to retaining and destroying electronically stored information, also known as ESI. Any information can be stored electronically, and almost all new information is being created and stored exclusively in electronic format.

Development and implementation of an electronic document/e-mail retention policy is crucial to protecting your business from the pitfalls of ESI, while maintaining proper records for your type of industry. While many companies have such a policy in an employee handbook or other policy manuals, few have updated the policy to keep up with current legal trends and even fewer are implementing their own policy.

Imagine how it appears to a juror when a business destroys documents potentially key to a particular case, but other documents from the same time period are retained. In fact, courts can and have instructed juries in such cases that they may assume the destroyed information would have been detrimental to the business' position in the case. Not surprisingly, several such cases have resulted in large jury verdicts or monetary sanctions against parties who failed to preserve or produce key information.

The gut reaction to the potential dangers may be to save everything. Of course, in a business context, where thousands if not millions of e-mails and other electronic documents are created each year, the costs of storing ESI can become astronomical. Not only is storing all ESI expensive and impractical, it is unnecessary. Moreover, keeping information you no longer need for a business purpose, and are no longer required to keep by the laws governing your industry, only subjects you to potential legal liabilities.

The term "retention policy" is somewhat a misnomer. Retention policies actually provide a schedule for "deletion and destruction" of information. Recently passed amendments to rules regarding court procedure specifically set out that ESI is discoverable in the context of civil litigation. Those amendments provide a safe harbor for destruction of potential evidence, as long as the destruction was in good faith and pursuant to the action of a bona fide document retention policy. In the litigation context, a business may be charged with preserving and producing existing evidence, even if the information is located only in hidden or deleted files on a computer system or on backup tapes. While there are a plethora of legal arguments about what should be preserved and when, businesses must ensure on the front end that they have an up to date retention policy and that it is used consistently. Do not wait until you are facing potential litigation to attend to your retention policy.

Your business should be asking:

- Do we have a retention policy that covers electronic documents/e-mails?
- Has that policy been updated since the Federal Rules of Civil Procedure were amended in December 2006?
- If so, what are we doing to ensure that our IT department is actually implementing the policy as written?
- Do we know what to do when we get sued or believe we may be sued?

Whether these questions loom overwhelmingly because you have yet to implement a retention policy or whether you have taken a "don't ask, don't tell" approach to your long outdated policy, there are several best practices from a technology perspective that should be employed in an effective electronic document retention policy:

Identify an IT Leader — The IT leader is a critical member of the team developed to implement a document retention policy. One or more individuals from within your IT staff should be selected who will be responsible for maintaining the framework of your computer systems. It is not necessary that the individual come from the senior ranks of the IT department. The ideal candidate should be intimately aware of the day-to-day logistics of where and how your company's data is stored.

Inventory — The storage of electronic documents is vastly different than that of paper. Electronic documents thought to be deleted or lost can often be recovered or found intact on other devices, such as backup tapes.

Additionally, background information called metadata (inherent with electronic data) can turn up skeletons you had no idea existed. Knowledge of the location of data, storage methods and document types is critical. The inventory should include the location and storage formats of electronic data. One thing is certain with ESI: What you do not know will inevitably haunt you. Any information stored and/or used by computer technology is considered to be electronic evidence discoverable in litigation. Relevant information may exist in a variety of locations and various forms. Be careful not to overlook basic categories of data, including:

ACTIVE DATA – Information readily available and accessible to users. Active data include the files listed in a directory listing and can easily be viewed through file manager programs.

AUTOMATICALLY STORED DATA – Automatic backup features commonly create and save copies of the file being worked on in order to help users recover data lost due to a computer malfunction. On most networked systems, file copies are saved to the user's hard drive rather than to the network file server. As a result, a document (or some version of it) that was purged from the file server may exist as a file copy on the user's hard drive.

"GHOST" OR RESIDUAL DATA – Residual data are information that are still recoverable from the computer system, but does not appear as accessible data when performing a list file or directory command. Residual data include deleted files or file fragments, file slack and unallocated space.

DELETED FILES – "Deleted" does not mean destroyed. The process of deleting a file merely indicates to the computer that the physical space belonging to the deleted file is available. All or part of the deleted file may be recoverable.

SLACK SPACE – Because computer hard drives cannot contain any space that is truly empty, any leftover space or "slack space" is automatically packed with random data, including remnants of deleted files and files viewed that the user never intended to save. Think of it as "digital packaging material" similar to the old newspapers used to stuff the empty space of a box of goods ready for storage in the attic. Years later it is often the old newspapers that are far more interesting that the items that were packaged.

BACKUP DATA – Network backups that capture data saved on the network server (typically excluding user drives) can provide valuable ESI, though restoring and locating relevant data can be expensive and time-consuming.

ALL TYPES OF HARDWARE AND SOFTWARE USED – Be sure to include laptops, handheld devices, removable storage devices, cell phones, etc. Often overlooked, removable storage devices often contain information long believed to be purged from the network or other hard drive.

METHODS BY WHICH DATA CAN BE TRANSFERRED INTO AND OUT OF THE COMPANY – Be careful not to neglect sources of electronic data that may reside or operate independently of the standard corporate IT environment, including instant messaging, voicemail, online storage repositories and/or Web-based e-mail.

RETENTION/DESTRUCTION SCHEDULE – Define how, where and how long to store electronic records, and develop document destruction schedules based on document type, legal requirements and business needs. As e-mail retention policies have long been a challenge for companies, consider the automatic destruction of e-mail unless the recipient or author consciously stores the message as a business record. Once developed, be sure to consistently follow your retention/destruction schedule.

RESPONSE PLAN – Implement procedures for ensuring that document destruction can be quickly suspended should the need arise. A litigation response plan that sets forth a road map to quickly identify the types and locations of records that might be potentially relevant to pending or threatened litigation is a critical part of your retention policy. To be effective, your litigation response plan should include the steps for identifying, capturing and preserving potentially relevant data, preferably in its native format.

Once you have your newly crafted or recently updated electronic document retention policy, be careful not to leave it unattended for too long. The electronic world of document retention is nothing short of a moving target. Be proactive and conduct periodic audits of your policy. Make adjustments as necessary.

KHRISTI DOSS DRIVER is a litigation attorney with Haskell Slaughter Young & Rediker, LLC. Her practice is focused on civil trials and appeals. She has represented insurers and insureds in a wide variety of matters, including products liability, insurance coverage matters, property and casualty claims, fraud, bad faith and punitive damages claims and employment discrimination cases. She also has extensive expertise in electronic data discovery and regularly advises clients on electronic data retention policies. She can be reached at 205.251.1000 or kdd@hsy.com.

KELLY J. TODD, CPA/ABV is a shareholder with Forensic/Strategic Solutions, PC. Her work as a forensic accountant and fraud examiner includes work for defense and plaintiff attorneys, audit committees, corporate boards and government inspector generals. Todd testifies as an expert witness in federal and state courts on matters involving complicated financial transactions and economic damages. She is a frequent lecturer on various forensic accounting matters throughout the country, including electronic evidence and discovery, data mining, employee embezzlement, occupational fraud and abuse and financial statement fraud. She can be reached at 205.397.2122 or Kelly@forensicstrategic.com.