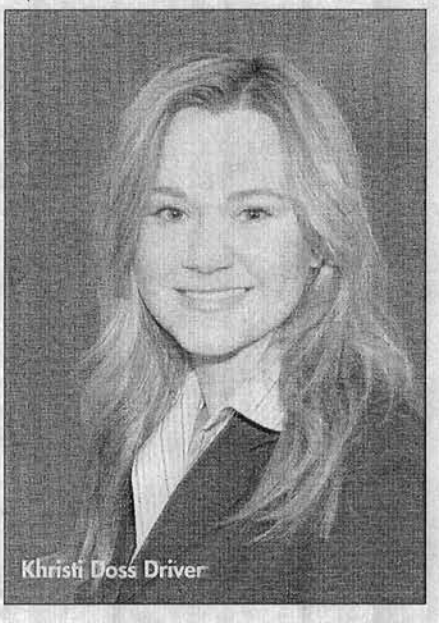
ERASING THE PAST

Document retention and destruction should be planned out, with an exception for documents that have the potential to be requested in cases of litigation.

BY KHRISTI DOSS DRIVER AND KELLY J. TODD


Khristi Doss Driver


Kelly J. Todd

Your employee is getting a divorce and his office e-mail and internet records are subpoenaed by his spouse's attorney, who suspects your employee was having an affair and used his office computer to communicate with his paramour. Your former employee alleges she was subject to gender discrimination at your workplace and claims that electronic records on your office computer systems will prove her case. You manufacture a product that a consumer claims is defective and dangerous, and there are spreadsheets, memos and e-mails on your company computers that show you may have had notice of the problem. Your partner stole valuable customer lists and proprietary information from your company computer systems before leaving you to join a competitor. Each of these scenarios is a distinct possibility in a modern business environment.

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 was 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 documents and e-mails 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 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

TODAY'S INCREASINGLY TECHNOLOGICAL WORKPLACE PRESENTS UNIQUE LEGAL RESPONSIBILITIES AND PITFALLS RELATED TO RETAINING AND DESTROYING ELECTRONICALLY STORED INFORMATION, ALSO KNOWN AS ESI.

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.

Businesses 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?

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 that should be employed in an effective electronic document retention policy:

Assemble the Team. Establishing the right team to undertake the process can save valuable time and resources. Seek input from legal, business and technical expertise.

Identify an IT Leader. Select one or more individuals from within your IT staff 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. Be mindful that the storage of electronic documents is vastly different than that of paper. Knowledge of the location of data, storage methods and document types is critical. The inventory should include:

- All types of hardware and software used. Be sure to include laptops, handheld devices, cell phones, removable storage devices, etc.
- The location and storage formats of electronic data. Be careful not to overlook 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.
- Methods by which data can be transferred into and out of the company.

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.

Be aware of electronic footprints — understand that delete does not always mean delete. 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.

Once developed, be sure to consistently follow your retention/destruction schedule.

Records Custodian. Designate a records custodian. A large company may best be served by one organization-wide records custodian who delegates preservation responsibilities among different departments within the company.

Educate. Educate all employees on the company's retention and destruction policies. It is important that the employees understand not only the policy, but also the implications of not following it. Monitor adherence to the policy and re-educate annually.

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.

Now that 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 by conducting periodic audits of your policy. Make adjustments as necessary.•

BE AWARE OF ELECTRONIC FOOTPRINTS — UNDERSTAND THAT DELETE DOES NOT ALWAYS MEAN DELETE. 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.

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 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. As a forensic accountant and fraud examiner, she works with 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 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.