The Electronic Data-management Policy

It's a Good Business Practice — and a Sound Legal Safeguard

By ALEX HOGAN

Businesses can now utilize electronics to efficiently conduct operations, and are able to receive, send, and store data effortlessly. Unburdened by heaps of paper, though, it is easy to lose sight of the data compiled.

And that's why adopting an electronic data-management policy has obvious benefits, such as minimization of electronic storage space and organization of data. Yet there is another important consideration: a business that routinely follows a reasonable electronic data-management policy will be better-situated in the event of litigation.

A legal duty arises to preserve relevant evidence as soon as it can be reasonably anticipated that a dispute may result in litigation. During discovery, parties exchange relevant records, including electronically stored information (ESI). A printout of an e-mail or document is not ESI. A printout is less reliable and might not provide the full history of the data.

Rather, ESI is produced in electronic form (e-discovery) and contains metadata — data behind the data. Metadata in an e-mail may establish the identity of the author; dates when an e-mail was created, mailed, and received; the identity of all recipients; and attachments. Metadata in a word-processing document may include the document name, file-save location, author, editors, and edits to the document.

Some sources of ESI may include e-mail, word-processing documents, spreadsheets and tables, images (e.g., PDFs and JPGs), databases, contact-management data, calendar and diary application data, and files that are incompletely deleted. ESI may be stored in a host of locations, such as network servers, desktop and laptop computers, portable hard drives, flash memory cards, discs, backup tapes, and off-site storage systems.

By now, the reasons to maintain and enforce a policy should be more obvious. If a business has not adopted a policy, relevant ESI may have been deleted, or it may be found in any one, or several, of the sources and locations mentioned above. The challenges during discovery will be locating, identifying, extracting, and interpreting relevant ESI. Most business people do not have the technical knowhow to navigate through this process.

A business that routinely follows a reasonable electronic data-management policy will be better-situated in the event of litigation.

Not surprisingly, an entire industry has been created to aid in the e-discovery process. Both software and computer forensic specialists are available at a significant cost.

On the other hand, if a business adopts a policy but does not routinely follow that policy, once litigation has commenced, it is likely to find that it has destroyed ESI that is relevant to the litigation while retaining irrelevant ESI. This scenario poses significant risks.

Failure to preserve material evidence is known as 'spoliation.' Because spoliation can impair a party's ability to prove or disprove claims, the court may sanction the responsible party. Although sanctions are specific to each case, they may include monetary damages or permitting adverse inferences against the spoliator. A negative inference that a party had something to hide from the court may be more damaging to the spoliator's case than the actual evidence destroyed. Conversely, a party that routinely follows a well-written policy created for legitimate business purposes is more likely to avoid sanctions, because its actions will be viewed as legitimate by the court.

The message is that a business operating without a reasonable policy, or not following the policy, potentially risks spoliation claims and higher costs during the discovery process. A policy should be adopted and enforced before the threat of litigation arises. It should be tailored to the particular business. Although one size does not fit all, there are some universal guidelines.

Specifically, the policy should be written, and its goal must provide for destruction of ESI for bona-fide business reasons only. It should strike a balance between a business's need for retaining necessary ESI and destroying inconsequential ESI on a routine basis.

To consider one example, it may be reasonable for a business to destroy insignificant ESI every 60 days. If the data is significant, the policy should specify a procedure for indexing and storing the data for a designated period of time. The policy must account for laws that impose specific retention periods.

For instance, an employer may be obligated to retain employment records for three years following termination. Once litigation is anticipated, relevant ESI must be retained until the applicable statute-of-limitations period has passed. If litigation is instituted, employees should be notified to ensure that ESI is retained throughout the lawsuit. Employees that use electronics should receive a copy of the policy and training.

Most importantly, though, the policy should be actively maintained and enforced. ■

Alex Hogan is an attorney with Springfield-based Shatz, Schwartz and Fentin, P.C. She concentrates her practice in the areas of business law, business litigation, and bankruptcy law. She was named a Rising Star by Super Lawyers in 2011.