BROWN & RUPRECHT PC
ATTORNEYS AT LAW

• THE LATEST DEVELOPMENTS IN THE BUSINESS WORLD •

LEGAL UPDATE

911 Main Street, Suite 2300 • Kansas City, Missouri 64105 (816) 292-7000 • www.brlawkc.com

Law Adapts to the Digital World

The Legal Landscape

In December 2006, the federal court system implemented an array of new rules all designed to confront the issue of discovery and production of electronically stored information (ESI). Court decisions interpreting these new rules were slow coming, but it is apparent that they are changing the way lawyers conduct themselves in litigation. More than that, though, the rules signaled to the legal and business communities that companies need to be thinking more about the way information is stored, retained, and deleted.

In the wake of the federal rules changes, the Sedona Conference, a think-tank of businesspeople and lawyers who discuss issues relating to commercial litigation, published a list of principles and comments designed to guide attorneys and their clients in managing information, both in the context of litigation and everyday business practice. In the past, the Sedona Principles, as they have come to be known, have been very influential on courts deciding the appropriateness of business policies and procedures. Doubtless, the new principles on topics like e-mail management will be just as influential.

Court decisions, rule changes, and policy papers like the Sedona Principles all form the landscape of "authorities" that guide and shape business practice.

What Is a "Document" or "Record"?

The starting point for any discussion of management and retention of electronic information is to define the scope of the conversation. In other words, how much and what types of information are we talking about?

Various words are used in an attempt to encompass the entire field of relevant materials: document, record, ESI, etc. None of these terms, however, does any justice. Few people actually realize the extent of what might be covered by retention or preservation policies and rules. In our fast-paced, on-the-go society we create "documents" or "records" in places never before contemplated. Each of these media may be needed on a day-to-day basis by a company; or, in those cases where the company sues or is sued, they likely will be the subject of a subpoena or discovery request. Here is a non-exhaustive list of storage media:

- files on PC hard drives
- local network servers
- removable storage media like disks and USB drives
- backup tapes
- web files
- cell phone text messages
- files on Blackberries and other PDAs
- email and email attachments

The volume of information created by a single person is just as staggering as the list of possible places where that information is stored. For example, the most recent research suggests that the average person in the U.S. generates 75 email messages per day. *In a company with 20 employees, this means that over 500,000 emails are generated in a given year.* And for whatever reason, the vast majority of these emails are being saved, either locally on the user's machine, or on a network drive.

All told, the electronic "documents" or "records" kept by a business, even one with only 20 employees, are voluminous, to say the least. Many organizations are struggling with how best to cope with the explosion of electronically stored information and with competing needs imposed by regulatory, litigation, and day-to-day business needs.

What Is the Harm?

The cost of electronic storage space (hard drives, network drives, etc.) alone is significant, but the natural tendency to keep everything is risky for other reasons. Especially for emails and text messages, the drafter tends to be more casual in his or her remarks. A flippant message that reads, "Is this rep accurate," could be spun very negatively by an outsider if there is later a dispute over the representations and warranties in a merger or asset purchase. We also tend to be more personal in emails and text messages, sometimes making comments about a person's character. As quickly as we are called on to respond to such messages, we often give little thought before forwarding an email conversation to others. Later recipients of a forwarded email would be required to produce that email in its entirety if given a subpoena or discovery request, meaning that communi-

cations that once were only among a few people might very well be expanded to include many more, any of whom could be called upon to turn the email over.

If there is any regulatory investigation or lawsuit, then the stores of information on PCs, network drives, and backup tapes all become subject to discovery. *Without effective retention policies, the costs involved are astronomical.* In the often-cited case of *Rowe Entertainment*, the processing of 8 backup tapes was estimated to be $400,000. Even something as simple as making a copy of a single 40-gig hard drive can cost as much as $4,000—and the costs only increase with the size of the hard drive. Implementing in good faith a policy under which data is routinely deleted can reduce costs all around, both in litigation and in the daily operation of business, and can also serve to decrease the risk of someone reading something they should not be.

What Is a "Litigation Hold"?

Blind application of a retention policy, though, is also not a good idea. "Litigation hold" refers to the court-imposed duty of a party to suspend its retention policies when litigation is reasonably anticipated. *Well-meaning and unwary litigants have found themselves on the receiving end of judicial sanctions for failing to properly implement a litigation hold.* Significantly, a computer system's automatic deletion of old emails (like in Microsoft Outlook) constitutes a retention policy, and that the failure to stop this default feature of the program constitutes a violation of the duty.

Proper implementation aside, the question of when to implement a litigation hold is a matter of some disagreement. Each business is different in its needs and capabilities, and also in the types of risks it is subject to, so a general, hard and fast rule cannot be fashioned. Instead, litigation holds require thoughtful application of the law in the particular jurisdiction to the particular business for which the hold is being implemented. The one thing that is true for all businesses is that the ability to effectively implement a litigation hold is a necessity.

What Should Be in a Retention Policy

First and foremost, retention policies dealing with email and other ESI should be guided by the needs of your particular business. Email conversations about a given contract negotiation might be kept only as long as the contract is being performed. Or, if the contract provides for a certain claims period following the transaction or project, then they might need to be kept longer. If, however, there is no reason to keep emails or other documents, then they should be deleted—and recent trends in the law say it is acceptable to do so. Consultation with in-house or outside counsel can help clarify what "business needs" will drive the policy.

Second, retention policies must conform to statutory and regulatory requirements. To name a few, HIPAA and COBRA have certain retention periods for the health care industry, while Sarbanes-Oxley has different periods for the securities industry. State insurance regulations impose yet another set of requirements for preserving "documents," including email.

Third, the Sedona Principles, mentioned earlier, provide some very insightful guidance about what a retention policy should contain and what questions you should ask when formulating one. For example, one Sedona Principle specifically about email states: "Any technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems." A company is not required to spend a ton of money on a shiny new server so that emails are dealt with in a specific way. Rather, this principle focuses on the current capabilities of the company's information system and teaches that no matter what the vendor thinks is important, ultimately it is the needs of the business that control. The courts have similarly recognized that the technical limitations that a given business might have.

Fourth, the policy must provide for consistent enforcement and application. *Picking and choosing which emails to delete for reasons deemed improper by the law could subject the company to sanctions.* This could happen even for a properly created policy where that policy is not consistently enforced.

Final Thoughts

Electronic information like email will continue to proliferate in size and amount. "Keep everything" is no longer an option; the costs of doing so simply do not allow for it. On the other hand, neither is simply cleaning house. Your company must put some thought into how and under what circumstances it is appropriate to destroy electronic information. Retention policies for ESI are a requirement rather than simply another business policy. To handle this challenge effectively, the policy must evolve as much as the technology.

For more information about the obligations of businesses in dealing with email and other electronic document retention, or to develop your own ESI retention policy, please call Brown & Ruprecht, PC:

Brown & Ruprecht, PC
911 Main Street, Suite 2300
Kansas City, Missouri 64105

Phone: (816) 292-7000
Fax: (816) 292-7050

www.brlawkc.com