The Perils of Email: Navigating the Legal Risks

Wednesday, July 6, 2011

In 2011, the typical corporate user will send and receive more than 110 electronic messages a day (over 40,000 per year), according to the Radicati Group. The number of worldwide email accounts is projected to increase from over 3.1 billion in 2011 to over 3.8 billion by 2014, 25% of which will belong to corporate users. As technology continues to drive growth and expansion for businesses, greater volumes of communication will be handled via email.

Although electronic messaging makes communication easier, faster and less expensive, it also creates an extraordinary set of issues. Identifying these perils and developing procedures to avoid them is critical for every company.

Information Preservation and Hold Notices

Various federal, state and local laws, rules and regulations require corporations to retain electronic communications and other information. For example, Rule 17a-4 of the Securities and Exchange Act requires SEC-regulated companies to retain all communications sent and received for at least three years, the first two in an easily accessible place. NASD Rule 3110 requires members to preserve books, accounts, records, memoranda and correspondence, and under the Sarbanes-Oxley Act, emails can become part of the business records of a company that are to be retained.
But, even when it is not required by law, an email retention policy should be in place. For example, according to a 2008 study by Osterman Research, 66% of the organizations surveyed rely upon email, IM archives or backup tapes to support and defend the organization in litigation. This should come as no surprise. Under the **Federal Rules of Civil Procedure**, a party generally is entitled to any document - in "hard" or "soft" (i.e., electronic) copy - that "appears reasonably calculated to lead to the discovery of admissible evidence." Knowing this, litigation battle lines are often drawn around electronically stored information (ESI) and allegations that evidence has been destroyed (or "spoliated"). Savvy lawyers know that ESI discovery costs can drive settlement negotiations, or at least, distract parties from the real issues in the case. It is important, therefore, to have a sound retention policy to help make retrieving data for both business and legal purposes less painful.

### Information Retention Policies

The adoption and enforcement of a retention policy is the first step to managing ESI. To be worthwhile, retention policies should:

1. reduce the risk of loss of critical and/or confidential business data,
2. alleviate burdens during an investigation or a lawsuit,
3. account for information that needs to be retained to advance the goals of the business units and is legally required to be retained by the administrative and regulatory entities to which the corporation reports. What this means is that information critical for business continuity should be backed-up, retained and stored in a sensible way for retrieval. In developing retention policies, management should consider the importance and usefulness of information that is not legally required to be retained against the potentially high costs of locating and producing the information if required to do so later.

Determining what information to retain should be a collaborative process that includes at least one member of the IT department, the legal department, the affected business unit or units and human resources. That team should appoint a leader, most likely a legal department member, who is charged with mastering all facets of the policy and assuming ultimate responsibility for implementing and supervising all of its requirements. In terms of litigation, one of the requirements should include the process for retrieval, taking into consideration the time, manpower and monetary expense needed to actually assimilate relevant information for review and production.

After the policy is implemented, an ESI task force should schedule periodic reviews to test the retention procedures in order to confirm that the scope of retention adequately meets the over-arching goals, and that record-purging and backup activities are occurring and are documented. Additionally, the task force should ensure that data on all servers, desktops, laptops, PDAs, etc. is accounted for in the regularly scheduled purging cycle. When financially feasible, periodic audits of the policy and the processes, with the assistance of a third party, can verify and enhance reliability and compliance.

A lot of effort goes into formulating an effective retention policy and adequately communicating its importance to all of the persons affected by it. As one analyzes ways to improve and enforce the policy, one should be mindful to consider whether the policy includes certain characteristics as suggested by information management firm Iron Mountain's Records Management Best Practices Guide. These include:

- A sound and defensible record retention schedule that captures and reviews all records created by all business units.
- Electronic records that are migrated into a digital archive equipped with efficient and effective tools for searching, discovery organization and retention management.
- A retention program with components integrated into an internal audit process.
- Appropriate disposal methods, based on the different record classes or media types employed by the end-users of the electronic media.

### Managing the Litigation Hold

Information retention policies that are reasonable outside the litigation context may nevertheless result in the destruction of ESI that would be relevant in litigation and give rise to a claim of spoliation. A proactive
approach to thwart such a claim should require strong lines of communication between management, IT and legal and a keen appreciation for determining the date at which the company may “reasonably anticipate litigation.” Indeed, courts have insisted upon the suspension of routine document retention and destruction policies at the moment a party reasonably anticipates litigation. At that instance, a litigation hold notice should be prepared and distributed to all key personnel.

Obviously, deciding what to retain for purposes of a litigation hold is as equally important as determining when to distribute the litigation hold notice. For this reason, it is recommended that the litigation hold notice be a joint effort between in-house and outside counsel, and include language broad enough to describe categories of information that may be relevant to both the defense and prosecution of any reasonably anticipated claim. The litigation hold notice should also clearly identify one or two people to whom all questions should be directed and describe which ESI storage devices are subject to the hold. In more significant litigation, counsel should also plan to meet and interview key custodians and summarize the efforts undertaken to preserve and collect documents and ESI. While the summary should be privileged, it is an important document that counsel may refer to in defending a claim challenging the integrity of the litigation hold. In short, a well thought out and executed litigation hold plan may save a bundle of money (both in legal fees and possible sanctions) in responding to allegations of spoliation or other nonsensical litigation gamesmanship.

Avoiding Sanctions

Spoliation is “the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.” Courts have broad discretion to impose appropriate sanctions under Rule 37 of the Federal Rules of Civil Procedure when a party spoliates evidence in violation of a court order. However, in the absence of a court order, a party asserting a spoliation motion has the burden to prove spoliation occurred. As a general rule, that party should prove: 1) the party charged with destroying the evidence had an obligation to preserve it; 2) the records were destroyed with a “culpable state of mind”; and 3) the destroyed evidence was relevant to the moving party’s claim or defense.

While evidence of the third point may be under the control of the moving party, proving the first two points will usually require evidence within the possession, custody and control of the party against whom the motion is filed.

As with most prudent plans, the key is to be proactive. The first step to potentially avoid sanctions for spoliation is to initiate the litigation hold as soon as possible. Thereafter, one should immediately identify and modify retention policy features, systems and devices that, in routine operation, would destroy potentially relevant ESI. Then, one should send a notice to all personnel affected by the hold. Purging functions should be disengaged and protocols to overwrite backup media should be suspended. It is also important to be diligent and anticipate what employees will hide, destroy or alter ESI; one should guard against such tactics by interviewing key employees early and monitoring their use of company email and electronic document storage systems for signs of tampering, destruction or other troublesome behavior. An “Electronic Discovery Response Team” composed of management, IT personnel and legal counsel, should be assembled and should secure all storage media containing potentially discoverable data immediately upon receiving a request for production, and document all preservation efforts. In significant matters, consider retaining forensic experts to segregate, image and examine potentially discoverable electronic media both to meet early disclosure deadlines and to be in a better position to avoid abusive fishing expeditions.

Forensic Reviews

No discussion about ESI is complete nowadays without a reference to forensics. According to a November 2007 article in the American Bankruptcy Institute Journal entitled “Digital Forensics 101: Where to Find Critical Evidence,” authors Walt Manning and Michelle Campbell define digital forensics as a practice that “combines elements of law and computer science to collect and analyze electronic data in a way that could
be admissible as evidence." Forensic tools and techniques search every obvious and hidden space for stored data, and usually uncover evidence missed by even a diligent custodian's review. Common places where stored data is overlooked in the data retrieval process can include computer hard drives, telephones, fax machine transaction records, USB "thumb" drives, optical media such as CD-ROM or DVD disks, backup media, online storage services, off-site archival services, shared network drives, external hard drives, cell phones or PDAs capable of containing email or text messages.

Through the use of forensic tools, techniques and experts, it is possible to: 1) recover deleted files or email messages; 2) recover fragments of data, even if a portion of the original has been permanently deleted; 3) identify and capture relevant data saved on external data storage devices; 4) capture and search data from cellular telephones and personal digital assistants; 5) capture and analyze instant messaging traffic; and 6) analyze internet history and recover images of websites visited. Given the particularly aggressive nature of some lawyers, and the evolving procedural guidelines for ESI discovery, effective internal policies should consider the ability to resurrect and unveil deleted and/or "hidden" ESI. The simple, but harsh, truth is that the days of total document destruction (i.e., shredding) are gone. The concept of "shredding electronic data" is a complex, often incomplete, process.

**New Technology, New Threats**

The internet and email have revolutionized the way individuals and businesses communicate with each other. As email and text-messaging increasingly become the primary forms of communication, the continued widespread use of email and texting in the corporate setting creates a whole host of interesting issues for companies and their lawyers. In litigation, for example, emails are an important component of discovery and often contain the proverbial "smoking gun." The best defense is a good offense, which starts with a thoughtful analysis of the threats, backed by sound policies and practices that may ensure the proper use, retention and handling of emails and other ESI.

----------

*Felicia Harris Kyle* is a member of *Sutherland Asbill & Brennan LLP*'s Litigation Practice Group and focuses her practice on complex commercial matters involving energy, employment, contract, trade secret, business tort and product liability issues.

Risk Management Magazine and Risk Management Monitor. Copyright 2020 Risk and Insurance Management Society, Inc. All rights reserved.