Recovering and Preserving Public Records in the Age of Electronic Documents

By Robert J. Kerwin

The Legislature long ago established that government records must be preserved, maintained and made available to the public in accordance with state law (M.G.L. Ch. 66, Sect. 8). The state's Supervisor of Public Records, meanwhile, has required municipalities to implement policies governing the backup and archiving of electronic public records (SPR Bulletin No. 1-99). The supervisor has further required municipalities to make "reasonable" efforts to recover any electronic public records that are lost. What constitutes "reasonable" efforts in any given instance is related to the facts in a given situation. The supervisor, however, has not publicly addressed the financial costs involved in the recovery of public records.

Robert J. Kerwin is a former president of the City Solicitors and Town Counsel Association and a shareholder in the Boston firm Tarlow, Breed, Hart & Rodgers, P.C.

With the explosion of electronic documents, most municipal public records are expected to be of an electronic variety within a few years. So the issue of managing and recovering electronic documents is of importance to every municipality. If not properly managed, "personal storage tables" (i.e., files) containing e-mail records may be lost when one simply replaces a hard drive or upgrades software. Given that all municipalities eventually upgrade their computers and software, all municipalities are at risk of losing electronic documents. Complicating matters is the fact that a municipality may not be aware of the loss of records for some time. Where a municipality has many employees, it is not always possible to know when documents are lost.

The effort to recover electronic public records may entail the retention of an outside computer forensic expert. Indeed, in one instance, the supervisor of public records required a municipality to retain an outside computer forensic firm. For the municipality, this cost could be a significant contingent liability that was not budgeted or anticipated. Like other professionals, a computer forensic expert frequently bills by the hour. The hourly cost may vary, depending on whether the expert is being asked to take down a system, obtain a mirror image of the hard drive, or locate specific files. In many cases, these activities must be conducted outside of business hours, and the forensic expert may charge a higher rate for work that must be done at night or in the early morning. It is important, where possible, to establish the expected cost of an activity up front.

Recovering Files

As of five years ago, the average corporate user was sending thirty-four e-mails per day and receiving ninety-nine, or a total of 133 e-mails, according to the Radicati Group's E-mail Archiving Corporate Survey. For 2010, the Radicati Group projects that each user will send and receive a total of 199 e-mails per day, with the number rising to 228 in 2011. Data retention, therefore, is no small task.

Microsoft Outlook is the most popular program for storing e-mail data locally. When one deletes an e-mail, it is sent to the "trash," also known as the "deleted items folder." When a user "empties" the deleted items folder, all the deleted messages ostensibly disappear. The "deleted" items may, however, still be in the user's computer. Depending upon the e-mail system used, the deleted e-mail data will either be in plain text in the unallocated space or may be stored in some binary fashion. If an e-mail repair utility such as Advanced Outlook Repair is used to recover e-mails, one may recover whole and fragmented messages from the unallocated areas of a computer.

Sometimes, it's important to establish that an effort was made to recover e-mails from an individual user's computer. If called upon to produce evidence that demonstrates that searches were made of a computer, it's helpful if the computer forensic expert is able to confirm that the work was performed in an established manner. Indeed, it may be helpful to ensure that the computer forensic expert has a facility in operating Encase or another similar software tool, such as FTK, F-Response or others. In terms of computer forensic qualifications, one should discern whether the forensic professional is schooled in a protocol that provides a systematic manner to undertake the recovery. By way of example, the protocol may be that the hard drive of the computer be forensically imaged and write-blocked to preserve data. A backup copy is made and physically secured in an off-site safe. After the case preparation process (which may include mounting all compound files and recovering references to deleted files that may be missing their parent folders), the forensic expert may run an analysis that may aid in discerning whether document extensions were renamed in an attempt to hide vital evidence. One can also apply a comprehensive e-mail filter to locate any active mail files that reside on the computer.

Frequently, the project may involve working with the municipality to establish a series of searches to discern whether the document may be recovered from the hard drive's unallocated space. Keyword searches are often used to locate missing e-mails. These are beneficial, but could also generate confusion to those reviewing the work being undertaken. For example, a keyword search may generate a number of "hits" in the unallocated space, but these "hits" may include—and often do include—unintelligible sentence fragments. Some observers may confuse "hits" with actual readable e-mails, even though the number of readable e-mails may be substantially less than the number of "hits."

The limitations of keyword searches to recovery are perhaps obvious. The searches require that the public entity undertaking the search recall generally the subject matter or person to whom an e-mail is addressed and identify the users with whom he or she may have communicated. This approach to the recovery of "lost" e-mails may only uncover a limited number of messages. It's also important to keep in mind that unallocated space is constantly being used and overwritten. Since one often cannot discern the full scope of the lost e-mails, the number of searches to be conducted is likewise within the discretion of the municipality. It should be noted that if e-mail has been "double-deleted," the number of hits will vary from the number of readable e-mails. The process of discerning what is readable and what is not readable is a time-intensive activity. As noted, even recoverable e-mails will frequently contain some sections of gibberish. Given the sheer volume of e-mails sent and received over many months, such keyword searches can be daunting, and confirmation of full recovery based on e-mail searches is, in and of itself, difficult. It is therefore not entirely possible to say that all e-mails have been recovered. The reverse is also true: It is difficult to say that all e-mails have not been recovered. When combined with examination of the backup systems and examination of archived e-mails, however, the recovery can be more complete.

System Back-Ups

Most systems have some form of back-up that can aid in the recovery of lost e-mails. Such back-up systems, however, are not as easily accessible as the name suggests. Recovering the back-up for a particular computer may be time-consuming and difficult. It seems counterintuitive, but most back-up systems really are not readily accessible.

A more efficient form of recovery may be the use of an e-discovery tool such as the auto archive system, if installed. Such an archiving system allows one to recover instantly the documents that were ostensibly lost. If there are internal e-mail

archives, such as with an Enterprise Vault System, one can recover lost public records more easily. It will be helpful to use duplication tools, so that one may discern unique mail items from duplicates. The up-front costs of auto-archiving are not small, but given the panoply of public records requests often received by a municipality, this may be the most cost-effective way to go, long-term, to recover lost e-mails and to respond to public record requests.

An effective e-mail retention policy will go a long way toward avoiding the necessity for an extended public document recovery process. Archiving public records on a periodic basis may prove to reduce the necessity of an expensive recovery program. New draft guidelines from the secretary of state's office contemplate training for e-mail users, expanded identification of public records (e.g., Facebook and other social media), and a prohibition on automatic deletion of public records. With the avalanche of electronic documents, however, it is clear that recovery programs, when necessary, will become less costly and more sophisticated as time and technology progress. This is good news for municipalities seeking to preserve and recover public records.

STATE WORKING ON ELECTRONIC RECORDS GUIDELINES

The secretary of state's office, the Records Conservation Board, and the state's Information Technology Division are currently working on guidelines that state agencies will use for electronic records management.

While the guidelines do not apply to municipalities, according to the secretary of state's office, the recommendations may have some advisory value for cities and towns.

A draft of the Electronic Records Management Guidelines was released on April 6. The intent of the guidelines is "to ensure that government electronic records are created, maintained, disseminated and destroyed in a manner consistent with the transparency and accountability requirements" of the public records law and the provisions set by the Records Conservation Board.

"The prevalence of electronic records gives rise to security and retention concerns," the draft guidelines state. "Therefore, it is imperative that government records custodians are mindful of the unique qualities of electronic records."

According to the draft guidelines, "electronic records include, but are not limited to, numeric, graphic, text, audio and voice information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record."

The draft guidelines, which cover fourteen pages, call for state government entities to assign responsibility for developing and implementing "an enterprise-wide program for the management of all records created, received, maintained, used, or stored on electronic media."

The guidelines also call for state agencies to provide training for users of e-mail, websites, social media, and desktop documents on recordkeeping requirements and moving or copying records for inclusion in an agency recordkeeping system. Users should also be trained in the operation, care and handling of the equipment, software, and media that they use.

State agencies will need to develop and maintain up-to-date documentation about all electronic information systems and specify the location, manner, and media in which electronic records will be maintained. They would need to work with the Records Conservation Board to develop appropriate records disposition schedules.

The guidelines outline documentation, recordkeeping requirements, records management responsibilities, and the records disposition process for public entities to manage records created or received on e-mail systems.

Public entities with access to external e-mail systems are advised to ensure that agency records sent or received on these systems are preserved in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the public entity for recordkeeping purposes.

If the e-mail system is not designed to be a recordkeeping system, the guidelines call for public entities to instruct staff on how to copy the public entity's records from the e-mail system to a recordkeeping system.

Public entities that maintain their e-mail records in an electronic format are advised to move or copy them to a separate electronic recordkeeping system, unless their system has specified recordkeeping capabilities. Records from e-mail systems should be retained in an off-line electronic storage format, such as optical disk or magnetic tape.

Public entities that are unable to maintain their electronic records in an electronic format and maintain paper files as their recordkeeping systems should print their e-mail records and any related transmission and receipt data, except for those that they are permitted to delete under the Statewide Records Retention Schedule.

Public entities that create and use desktop documents should ensure that word-processing, spreadsheet, presentation, task list, contact, calendar, and other desktop documents are identified, preserved, and disposed of in a manner consistent with the Statewide Records Retention Schedule. They should also identify and capture desktop documents created and received by their employees in remote locations.

E-mail records identified as "administrative use" may be disposed of once the administrative use of the record has ended. "Administrative use" e-mails would include: communications reminding employees about scheduled meetings or appointments; telephone messages; announcements of office events such as holiday parties or group lunches; and recipient copies of announcements of agency-sponsored events such as exhibits, lectures, workshops, etc. Transitory messages are not intended to formalize or perpetuate knowledge and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.

When a public entity has taken the necessary steps to retain a record in a scheduled recordkeeping system, whether electronic or paper, the identical version that remains on a user's screen or in a user's e-mail box has no continuing value.

Public entities are advised to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems.

– John Ouellette