

Public Records, Electronic Documents and Traps for the Unwary

By RICHARD T. HOLLAND

Neils Bohr, who won the Nobel Prize in physics in 1922, said it best: “Technology has advanced more in the last thirty years than in the previous two thousand. The exponential increase in advancement will only continue.” And continue it has. Although the operations of government have benefited greatly from advances in computer technology, such benefits come with significant responsibilities regarding the preservation of, and accessibility to, government records.

The following comes from SPR Bulletin 3-96, one of the many bulletins issued by the Massachusetts supervisor of public records: “The computer generally enhances the government’s ability to collect, compile, manipulate and disseminate information. Certainly, as the manner in which government information is maintained evolves, the means of accessing such information must experience a parallel evolution to preserve a meaningful right of access.”

In order to preserve a meaningful right of access to public information, a municipality must not only create records of its operations, policies and procedures, it must also preserve them. SPR Bulletin 9-04 states: “Our government has a fundamental obligation to record information concerning its operation, policies and procedures. It has a duty to preserve, for the public good, the records and publications by which this information is documented.”

Richard T. Holland is an attorney with Kopelman and Paige, P.C.

Public records include, generally, all documentary materials and data, “regardless of physical form or characteristics, made or received by any officer or employee of” a municipality. [M.G.L. Ch. 4, Sec. 7(26) and 950 CMR 32.03] Yes, this includes electronic documents.

No matter where they reside, electronic documents must be preserved just like paper documents. Primary responsibility for this task rests with public records custodians.

Electronic documents are everywhere. They exist on computers (desktops and laptops), cellphones, smartphones, tablet computers, portable storage devices (i.e., “memory sticks”); the municipality’s computer servers; social media websites like Facebook and Twitter; the “cloud” (i.e., third-party servers hosting public documents and data); and private email services like Microsoft Outlook. For municipal employees who work from home, a municipality’s electronic documents may also reside on the employees’ home computers, laptops and portable storage devices.

No matter where they reside, electronic documents must be preserved just like paper documents. Primary responsibility for this task rests with public records custodians. Under Massachusetts regulations (950 CMR 32.03), each “governmental officer or employee who in the normal course of his or her duties has access to or control of public records” is a custodian of such records. And, states SPR Bulletin 2-96, “[e]ach officer in charge of a government office or department is the custodian of the records held by that office or department and has the primary responsibility for ensuring the safety of the records, providing access to those records and ensuring their authenticity.”

Electronic documents must be managed and maintained in accordance with an electronic records management plan. The purpose of such a plan, according to the *Massachusetts Municipal Records Retention Manual* (2011), is to describe how such “records are [to be] logically categorized or arranged for easy retrieval, use, and destruction.” Since many public records begin in electronic form, and many of them are never printed, a management plan is imperative.

Unfortunately, there is no “how to” manual or accepted standards for the development of a municipal electronic records management plan in Massachusetts. However, a guide recently published by the supervisor of public records for state agencies (*Electronic Records Management Guidelines*) provides helpful recommendations that may be applied to municipalities.

According to the guidelines, the management plan should address, at a minimum, the following elements:

1. Administrative management, including the assignment of responsibility to develop and implement a management program for electronic records and the monitoring of compliance with the public records law and applicable regulations, policies and standards
2. Educational elements, such as employee training on the municipality's records management plan
3. Development and maintenance of documentation on, among other things, the municipality's computer systems and equipment, and the location, manner and media in which electronic records will be maintained

Before a municipality can develop an electronic records management plan, it must first identify the following:

- The types of computer equipment used by the municipality to create, receive or store electronic data
- The types of electronic records it makes and receives in the ordinary course of business
- The employees who make and/or receive such records
- The length of time such records must be preserved (based on content, not form)
- The location(s) and accessibility of such records

This will require, at a minimum, a thorough inventory of all municipal computer equipment and the electronic records created and received by each municipal department, and consulting the retention schedules published by the supervisor of public records to determine the retention period for such records. (See *Municipal Records Retention Manual* [2011].)

An electronic records management plan must also address emails—perhaps the most ubiquitous of all electronic documents. According to a 2012 McKinsey & Company report (*The Social Economy: Unlocking Value and Productivity through Social Technologies*), the “knowledge worker” spends 28 percent of his or her time reading, writing or responding to emails. For a municipal “knowledge worker,” that is a lot of public records.



SPR Bulletin 1-99 states that “email messages are subject to the same records management principles as all other records of the office.” The supervisor requires that *each* public official who creates or receives an email review the content of each such email and consult with the retention schedules to ascertain the applicable retention period. The official must also print each email (including attachments) and file it with the municipality's paper records. The printed copy of the email must include “envelope information” (i.e., “the mailing address, date/time stamp, routing instructions and transmission and receipt information”). If it is too large to print, the email must be stored electronically pursuant to an email record-keeping system.

Thus, the supervisor of public records requires that municipalities also prepare, as part of their management plan, written policies for developing an email record-keeping system capable of displaying and preserving emails and their “envelope” information for the periods of time required by the applicable retention schedules. Unfortunately, email systems

like Outlook will *not* qualify as email record-keeping systems; nor will the “back-up tape,” which is typically used to store undifferentiated electronic information temporarily and is erased or overwritten on a regular basis. [See SPR Bulletin 1-99, SPR Bulletin 1-96, and “Recovering and Preserving Public Records in the Age of Electronic Documents,” *Municipal Advocate*, Vol. 25, No. 2.] According to SPR Bulletin 1-96, offline storage of email and other electronic documents must, generally, be to a dedicated disk or tape library.

Developing a records management plan is not enough, however. In its 2008 report on archival records management (*Preserving the Nation's Local Government Archives*), the Council of State Archivists identified the significant challenges for municipalities in managing public records. They included “the absence of funding and other resources,” and the fact that “records management ... is not a priority of local government executives and legislators, who tend to focus on higher-visibility, higher-stakes issues such as taxes, crime, social welfare, education, and other topics.”

Although easier said than done, management of electronic records must be adequately funded and treated as an important municipal initiative. Employees must be regularly trained on a municipality's records management plan. Records management must be woven into the work descriptions and duties of all municipal employees. It must be something that employees think of every day and with every task. Otherwise, a municipality's records management plan, no matter how comprehensive and well written, will sit on a shelf collecting dust.

Third-Party Contracts and "The Cloud"

A municipality with limited resources may, singly or jointly with other communities, contract with a third party to assist with records management. Some municipalities have retained computer companies to host, on private computer servers (i.e., "The Cloud"), electronic data made or received by the municipalities. Others have scanned existing paper records to create digital copies for storage on the cloud in order to free up storage space and ease the burden of searching for records (under the assumption that the new digital records will be easier to search by computer).

Although this sounds appealing, and certainly can, with appropriate precautions, facilitate cost-effective records management, contracting with a third party does not free a municipality from its obligations under the public records law. SPR Bulletin 3-96 states that a "municipality cannot contract away its public duties." In addition, SPR Bulletin 2-96 points out that a custodian's responsibilities to preserve and maintain public records "are inherent in the office and cannot be delegated or contracted to another entity." The bulletin goes on to say that, while "[t]hese records may be in the care of ... a private contractor providing government services, [or] a private information services vendor, ... the entity maintaining the records is acting as an agent of the record custodian, providing only for the physical care of the record, and may not take action with respect to the records without the specific authority of the custodian."

Thus, for example, municipalities that scan paper records to "free up" storage space may not then destroy the paper records, which must continue to be preserved. In fact, "official, original records and publications of enduring value should be recorded on archival

quality, permanent paper," according to SPR Bulletin 9-04. Records may only be destroyed in accordance with the applicable retention schedules published by the supervisor of public records, and even then only with the permission of the supervisor.

If a municipality is not careful, hiring a third party for records management may make compliance with the public records law more difficult, if not impossible. Some third-party contracts, for example, contain provisions limiting or restricting access to the municipal data maintained by the third party. Such provisions are inconsistent with the public records law. Third-party contracts must include language that, among other things, makes the municipal data "available when directed by the records custodian," states SPR Bulletin 2-96. Legal counsel should be consulted to ensure that any such municipal contract is consistent with the public records law and applicable regulations.

Open Meeting Law

Less obvious, perhaps, is that an electronic records management plan may prevent violations of the open meeting law (M.G.L. Ch. 30A, Secs. 18-25). Like the public records law, the open meeting law was enacted to promote transparency in government—or as one court put it, "to eliminate much of the secrecy surrounding deliberations and decisions on which public policy is based." [*Ghiglione v. School Committee of Southbridge*, 376 Mass. 70, 72 (1978)]

The open meeting law requires, generally, that meetings of multi-member public bodies be open to the public. (Specific, narrowly construed exemptions allow for closed meetings called "executive sessions," as contrasted with open meetings or "open sessions.") The law defines a meeting as "a deliberation by a public body with respect to any matter within the body's jurisdiction." [M.G.L. Ch. 30A, Sec. 18] With certain narrowly construed exceptions, a "deliberation" is, in turn, defined as "an oral or written communication through any medium, including electronic mail, between or among a quorum of a public body on any public business within its jurisdiction (a quorum is a 'simple majority' unless otherwise provided by law, G.L. c. 30A, Sec. 18); provided, however, that 'deliberation' shall not include the



distribution of a meeting agenda, scheduling information or distribution of other procedural meeting [sic] or the distribution of reports or documents that may be discussed at a meeting, provided that no opinion of a member is expressed.” An important observation is that a “meeting” is a *communication*, and, as a result, a meeting for the purpose of the open meeting law may (unlawfully) occur even if all the members of the public body are miles apart. (With few exceptions, multi-member bodies are prohibited from deliberating unless a meeting has been advertised forty-eight hours in advance and at least a quorum is physically present at the location of the meeting, which must be accessible to the public. [M.G.L. Ch. 30A, Sec. 20])

Emails and Public Bodies

Members of a public body who exchange emails risk violating the open meeting law. In a recent case that came before the attorney general’s office, for example, a private individual emailed all three members of a board of selectmen requesting clarification of an item on the board’s meeting agenda. The board’s chair responded by hitting “reply to all.” In his response, the chair expressed, among other things, an opinion on public business. None of the other selectmen replied. The private individual to whom the chair responded subsequently filed a complaint with the attorney general’s office.

Although “by sending his email to the entire Board, the complainant invited [the chair] to respond to all recipients,” the chair was, nonetheless, found to have (individually) violated the open meeting law. [OML 2013-27] “Expression of an opinion on matters within the body’s jurisdiction to a quorum of a public body is a deliberation, even if no other public body member responds.” The board, however, was not found to have violated the open meeting law, because the other selectmen did not reply to the chair’s email. Had they done so, the board would have been in violation.

In another decision (OML 2012-93), a building committee co-chair sent emails to a quorum of the committee. In one email, the co-chair circulated a presentation intended for town meeting and requested comments. In a second email, the co-chair asked for comments on a public records request received by

the committee. Although some committee members responded to the co-chair’s emails, they did not send their emails to a quorum—they didn’t hit “reply to all.” The attorney general’s office held that the co-chair violated the open meeting law because the emails discussed public business within the committee’s jurisdiction. Since the other members who responded to the co-chair did not email their responses to a quorum of the committee, however, the attorney general’s office ruled that the committee did not violate the open meeting law.

Although a quorum of a public body may lawfully exchange emails on matters that do not constitute public business within the body’s jurisdiction, it is *never* prudent to do so. The problem, frankly, is that it is not always easy to know whether a subject is “public business within [a public body’s] jurisdiction,” and even if you (or your lawyer) think you know, the attorney general’s office may disagree with you. A 2012 decision (OML 2012-63) is a case in point: There, a quorum of a board exchanged emails on the work schedule of the board’s assistant, which the attorney general’s office ruled did not constitute public business. At some point, however, the emails discussed the decision-making authority of individual board members. This, according to the attorney general’s office, constituted “public business.” As a result, the board violated the open meeting law.

It’s a somewhat common misconception that a municipality may send serial emails without violating the open meeting law. For example, one member may send an email to a second member about public business, and that member may then forward that email to a third member, and so on; or a nonmember of the public body, like a town manager, may email each member separately to discuss public business. These emails would violate the open meeting law, because the existence of a deliberation (i.e., a “meeting”) turns *not* on the “simultaneity” of the communications among a quorum of a public body, but on the fact, and substance, of the communications.

According to the *Open Meeting Law Guide* published by the attorney general’s office, serial communications will constitute a deliberation if there are “multiple communications ... that together constitute communication among a quorum of members.” The result

would be the same if a nonmember, like a town manager, emails each member separately. “A public body may not use a nonmember, such as a staff member, to communicate on matters that the Board would otherwise save for discussion at an open meeting.”

Simply put, any conduct that skirts the spirit and purpose, if not the letter, of the open meeting law will likely be treated as a violation. “Governmental bodies may not circumvent the requirements of the open meeting law by conducting deliberations via private messages, whether electronically, in person, over the telephone, or in any other form.” [*District Attorney for the Northern District v. School Committee of Wayland*, 455 Mass. 561, 570-571 (2009); see also *McCrea v. Flaherty*, 71 Mass. App. Ct. 637 (2008)]

Rule of Thumb: Don’t use emails in your role as a member of a public body. If this is not practical, use email *only* to receive meeting materials from the person designated to distribute them. And if replying to an email sent to you and other members of your public body is an itch you must scratch, never—ever—hit “reply to all.”

Electronic Documents at a Meeting

Another trap for the unwary is the use of smartphones or computer tablets during a public meeting.

Under the open meeting law, with limited exceptions, “all documents and exhibits used at the [open] session shall be public records in their entirety and not exempt from disclosure pursuant to any of the exemptions under” the public records law. [M.G.L. Ch. 30A, Sec. 22(e)] (Documents used at an executive session may be withheld until the purpose of the session has expired, or even longer if they fall within one of the exemptions in the public records law or constitute attorney-client communications.) And they “shall, along with the minutes, be part of the official record of the session.” [M.G.L. Ch. 30A, Sec. 22(d)] The open meeting law does not explain what it means for a document to be “used at the session,” but the attorney general’s office has said that a document is so used, and thus a public record subject to disclosure, if it is “physically present” at the meeting (in paper or electronic form) and referred to

or discussed by members of the public body during the meeting. [OML 2011-17; OML 2012-42]

In a recent case (OML 2012-42), a town manager was observed reading from a document during a board of selectmen's meeting. Although he "never identified" the document, "[b]ecause it was physically present [at the meeting] and its contents were discussed by members of the Board," the document was "used at the meeting" according to the attorney general's office, and therefore was a public record required to be listed in the minutes of the meeting. Since the board failed to list the document in the minutes, the board violated the open meeting law. Although the document in this decision was in paper form, the same principle applies to electronic documents.

So if, for example, you (or a nonmember of your public body) pass a cellphone to one or more members during a meeting to show a photograph that becomes part of the deliberations, the photograph must be referenced in the meeting minutes and maintained, and be made available to the public, as a public record. In OML 2012-22, the attorney general's office writes: "We caution public bodies that distributing an image on a cellphone during a meeting may trigger requirements under the Open Meeting Law that the image be listed in the minutes as an exhibit used by the public body, and that the image be retained and made available as a public record." The result is the same if the cellphone is passed by a nonmember (e.g., a town manager).

Rule of Thumb: If you receive your meeting materials by email, print them out before the meeting and leave your smartphone, laptop and tablet at home, or tucked in your bag and turned off.

Texting is another hornets' nest. It is no different than email in its potential to result in an open meeting law violation. So if you find yourself punching the keys on your smartphone during an open meeting, don't be surprised if you receive a public records request. And if you happened to be texting another member of your public body during the meeting about public business within the body's jurisdiction, you must reference the text in the minutes of the meeting and maintain it as a public record.

Rule of Thumb: Don't text during a meeting.

Social Networking

Social networking websites pose another risk. In OML 2013-27, the attorney general's office warned that "social networking sites such as Facebook invite the temptation to deliberate outside of a properly posted meeting." If you use social networking websites, do not post messages on any public business—period. If you do so, and if the messages are viewed by other members of your public body (equaling a quorum), you will have violated the open meeting law, even if no one responds to your messages. [OML 2013-27; OML 2013-62] Posting such messages is no different than emailing or texting the members directly.

Improper electronic records management may also result in violations of a municipality's legal duty to preserve evidence in the event that the municipality becomes (or expects to become) involved in litigation.

In a recent case (OML 2013-62), the chair of an energy committee formed a private Facebook group to organize proponents for an energy project. The chair and three other members of the nine-member energy committee exchanged messages on Facebook about the project. The attorney general's office found "no evidence that a fifth member of the Committee was ever a member of the Facebook Group or communicated via the Facebook Group," and thus ruled that there was no "deliberation" among a quorum. If it had found such evidence, however, the committee would have been held to have violated the open meeting law.

Rule of Thumb: If you use social networking sites, don't use them in connection with your role as a member of a public body, and never use them to discuss municipal business.

Trap for the Unwary: Litigation

Improper electronic records management may also result in violations of a municipality's legal duty to preserve evidence in the

event that the municipality becomes (or expects to become) involved in litigation.

Consider this, from *Effectively Managing the Discovery of Electronic Records: Current Learning and Suggested Best Practices*, published by the National Electronic Commerce Coordinating Council: "The advent of electronic record keeping has increased the cost and annoyance associated with discovery. While easy and collaborative access, remote storage, inexpensive reproduction, quick distribution and near-indestructibility make the everyday use of electronic records infinitely preferable to old-fashioned paper records, these same features add exponentially to the cost, rigor and overall hassle of civil discovery."

Both the federal and Massachusetts rules of civil procedure allow litigants to request electronic data and information. [F.R.C.P. 26(a); Mass.R.Civ.P. 34] In fact, the federal rules require a litigant to disclose automatically, without request, "electronically stored information ... that the disclosing party ... may use to support its claims or defenses." [F.R.C.P. 26(a)]

In addition, under Massachusetts law, all litigants have a legal duty to preserve evidence as soon as litigation is commenced—and even earlier if a would-be litigant knew that litigation was likely. [*Fletcher v. Dorchester Mutual Insurance Company*, 437 Mass. 544, 549-550 (2002)] "Where evidence has been destroyed or altered by persons who are parties to the litigation ... and another party's ability to prosecute or defend the claim has been prejudiced as a result ... a judge may exclude evidence to remedy that unfairness," among other potential remedies available to the prejudiced party. Sanctions may be imposed even where the destruction of evidence was unintentional. A court will be unsympathetic to a municipal litigant who has destroyed, even unintentionally, paper or electronic records that it was required to preserve not only pursuant to this legal duty to preserve evidence, but also under the Massachusetts public records law.

Therefore, without an electronic records management plan, a municipality runs the risk of violating more than just the public records law. ❁

Municipalities may obtain assistance in the development of an electronic records management plan by contacting the Public Records Division in the secretary of state's office, or municipal counsel.