

**PUBLIC INFORMATION ACT:  
E-MAIL AND ELECTRONIC MEDIA**

**By**

**C. ROBERT HEATH  
Bickerstaff Heath Delgado Acosta LLP**

When the Texas Open Records Act, the predecessor to the Public Information Act, was enacted in 1973, documents were prepared on typewriters. Personal computers that a person might have in his or her home were a dream for the future. Phones were something that plugged into the wall and were used for talking with other persons. The drafters of the Act surely did not contemplate that records would be developed and retained largely in electronic form and that the capability to create and store such records would be commonplace in person's homes and even on wireless cell phones, laptop computers, tablet computers, and other portable devices. In fact, in the original version of the Act, "public records" were defined as "documents, writings, letters, memoranda, or other written, printed, typed, copied, or developed materials which [contain] public information." Texas Open Records Act; Act of May 17, 1973, 63<sup>rd</sup> Leg., R.S., ch. 424, sec. 2, 1973 Tex. Gen. Laws 1112, 1113. In the 38 years since the Act's initial passage it has been amended to recognize new technology and now specifically recognizes that information may be recorded on "a magnetic, optical, or solid state device that can store an electronic signal" and can be "held in computer memory." Texas Public Information Act, TEX. GOV'T CODE §§ 552.002(b)(3), (c). While the statute has been amended as new technology became commonplace, compliance and interpretation of how the statute interacts with new technology is still developing.

The emergence of electronic records has produced at least three impacts on the operation of the Act and on open government law generally. First, it has greatly increased the volume and

accessibility of records. Second, it raises questions of whether the records created and stored on personal devices rather than on workplace computers are covered by the Act. Third, the ability of public officials easily to communicate on personal electronic devices has increased the opportunity to unknowingly violate the Open Meetings Act and other laws and, at the same time, to leave a record of the violation.

### **THE IMPACT OF THE EMERGENCE OF ELECTRONIC RECORDS ON THE VOLUME AND ACCESSIBILITY OF RECORDS**

In the early days of the Act, requests were primarily for paper documents. The ability to find a document was limited by the filing system. If the requestor asked for a document in a way that was consistent with the filing system, it is likely that the document could be located. Thus, for example, if a request was for all the documents referencing XYZ project, the governmental body would likely produce everything filed under the subject heading of the XYZ project. If, however, some documents related peripherally to XYZ project but were located in file folders that did not reference the project, it is unlikely they would be located and produced. The ability to respond fully to a request was dependent on filing decisions made long before any request was received.

With electronic records, the volume of records is likely to be larger. Many versions of a document may be stored electronically while in the past, only the final version might be kept in the paper filing system. Further, a search for records is not so dependent on the filing decisions. Often it will be possible to locate any documents containing specific words or that were addressed to or created by a specific individual. Thus, for example, in the past, if a requestor wanted all the documents sent or received by a member of the city council, the records custodian would need to guess where the correspondence might be filed and look through the individual records. Since the person responsible for filing is unlikely to have anticipated all the different

sort of requests that might be made in the future, it is probable that the response might not be complete.

When the request is for electronic records, such as e-mails, the custodian is able to do an electronic search for any e-mail containing certain words or with the name of a particular person in the address or sender line. There is little need to guess where the subject under which the correspondence might be filed. While this permits more complete responses, it also has potential problems.

One problem is that a simple request can result in a massive amount of information. Requests for all e-mails to or from a public official over a specified time period can result in thousands of individual messages, many of which contain elaborate chains of earlier messages. In addition to the huge amount of time required to process such requests, the city may find that the volume of information precludes careful review of the documents prior to the time the city must specify the exceptions that may apply or to the time it must elaborate on its rationale for withholding specific documents. At times a news story or controversial action may produce a flurry of requests from multiple individuals or media outlets that overwhelm the city's ability to gather and review the information. Even in a city with a large legal staff, the volume may be so great that much of the staff will be devoting virtually all of its time to ensuring that Public Information Act deadlines are being met to the exclusion of being able to attend to other business. Additionally, a controversy that produces open records requests at one level of government may produce copy-cat requests at other governmental bodies. While voluminous requests can be an issue with paper records, the additional volume and greater accessibility associated with electronic records magnifies the issue.

The search capabilities that exist for electronic records produce the possibility of inconsistent results. When an e-mail is deleted from a computer it still may be recoverable. After deletion from the computer's in-box, it will remain in a recoverable file. At some point that file will likely be erased, but, for some time at least, it will likely be available on a back-up disk or tape. A councilmember, for example, may search his or her computer inbox or perhaps even the recoverable trash, and find nothing there. An information technology specialist, though, would likely make a more thorough and sophisticated search and recover documents the less technical person would have missed. When subsequent searches produce documents the city previously represented no longer existed, it can be very embarrassing. Similarly, the search terms used will govern what is produced. When cities receive multiple similar requests, the very real danger exists that it will produce inconsistent responses to substantively identical requests. It is good practice to have a procedure by which searches will be performed by the IT staff or similar person who will be expected to perform a more thorough search than someone with less technical expertise. Similarly, great care should be taken in drafting search terms so that the search is comprehensive. Even though a city may make a truly extraordinary effort to comply with a public information request, it may appear that it is hiding information or being lackadaisical in complying with the Act if a document is produced in response to one request when that same document was missed when responding to another request a week or so before.

### **RECORDS ON PERSONAL ELECTRONIC DEVICES**

A council member receives an e-mail on his home computer from a neighbor complaining of a pothole in a city street. Two council members communicate using their personal e-mail addresses regarding an issue that will come before the council. The city manager sends an e-mail from her home e-mail account to a city employee. Because it is a Sunday, the

manager sends the message to the employee's personal account. Are some or all of these messages covered by the Public Information Act? The answer may depend both on the facts and on whom you ask.

Under the Act

“public information” means information that is collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business:

- (1) by a governmental body; or
- (2) for a governmental body and the governmental body owns the information or has a right of access to it.

TEX. GOV'T CODE § 552.002(a).

The Attorney General has taken an expansive view of this definition. In Open Records Letter Rulings, the Attorney General has relied on a test that finds e-mails sent or received through a city official's personal account to be covered by the Public Information merely if they satisfy the test of being related to official business. Thus, in OR2005-06753 e-mails on the mayor's “private business or personal e-mail accounts” were public information under the Act because they “discuss official city business” and because “the mayor signs the documents and e-mails in his official capacity.” OR 2005-06753. In another letter ruling the Attorney General stated the test as being “to the extent that the personal cellular, personal office, and home telephone records, as well as the e-mail correspondence from personal e-mail accounts, of the mayor and the commissioners relate to the transaction of official city business,” it was subject to disclosure under the Act. OR 2003-1890. *See also* OR2003-0951. In other words, the test used by the Attorney General seems to focus exclusively on whether the contents of the message relate to official business. While this test guards against creating a loophole by which one might take information out from under the purview of the Act by maintaining it on personal electronic

devices rather than on workplace smartphones or computers, it fails to consider the part of the statutory definition that requires the governmental body to create the information or to have access to it.

This relaxed test now used by the Attorney General was not always employed, at least in cases involving more traditional records. At least two of the three rulings discussed above regarding e-mails on personal devices purport to be based, in part, on Open Records Decision No. 635 (1995) where the Attorney General was faced with the question of whether the hard-copy appointment calendars of public officials and employees were public information. There the Attorney General employed not a one-part, but rather a three-part test looking to whether (1) public resources were used to maintain the calendars, (2) whether the calendars were accessible to other employees, and (3) whether a significant part of the entries related to public business. Open Record Decision No. 635 (1995) at 6. Applying the three-part test, the Attorney General in that decision found that the commissioner's calendar, which met all three parts of the test, was public information under the Act, while the employee's calendar was not. In the more recent letter rulings relating to electronic documents, the first two elements of the test seem to have disappeared, and the only question appears to be whether the record relates to public business. Further, this single-element test does not address the elements of the statutory definition.

By contrast, in what appears to be the only reported case on the subject, the court hews to a test based on the language of the statutory definition. *City of Dallas v. Dallas Morning News*, 281 S.W.3d 708 (Tex. App.—Dallas 2009, no pet.) involved a request for e-mails sent to or from the personal Blackberry of the mayor of Dallas. While the district court granted summary judgment for the newspaper and determined that the mayor's e-mails were public information,

the court of appeals found that neither the *Morning News* nor the city had met their summary judgment burden and reversed and remanded. The court of appeals characterized the heart of the dispute as being “whether Mayor Laura Miller’s Blackberry e-mails that never go through the City server are public information under the Act. *City of Dallas* at 713. While the court, like the Attorney General, looked to whether the e-mails were collected, assembled, or maintained in connection with the transaction of official business, apparently unlike the Attorney General, it also included other elements in its test. Relying on the statutory definition, it required that the e-mails had to be collected, assembled, or maintained (1) by a governmental body; or (2) for a governmental body and that the governmental body owns the information or has a right of access to it. *Id.* at 714. In applying those elements of the statutory test, the court ruled that the mayor was not a governmental body. *Id.* The city itself was the governmental body. Its officers and employees were not. Thus, the information did not meet the first alternative under the statutory definition of being created or maintained by the governmental body. Because the mayor was not herself a governmental body, the inquiry moved to the question of whether the city either owned the information or had a right of access to it. The court concluded that the evidence was inconclusive on that point. The summary judgment affidavits suggested that the city did not have access to the mayor’s e-mails, but some of the affidavits were inconsistent and certainly were not definitive on the point. In addition, the court noted that the city had produced some of the mayor’s e-mails for the Attorney General’s review, which suggested that the city might, in fact, have access, yet the record was silent on how the city had obtained the e-mails. *Id.*, at 715. As the appellate court reversed the summary judgment and remanded the case for trial, we currently have no final resolution of the issue. It appears clear, though, that at least the Dallas Court of Appeals has a different, and more onerous, test than the Attorney General does for

determining if e-mails sent on a personal account are public information. Under the court of appeals test, if the city does not have access to the e-mails on its officials' and employees' personal accounts, then they are unlikely to be covered by the Act.

### **WHAT'S A CITY TO DO?**

If a city receives a public information request for e-mails or similar communications on its mayor's or council members' personal computers or smart phones, and it asks the Attorney General for a decision, it is likely the Attorney General will rule that the e-mails are public information covered by the Act. Alternatively, if it contends it has no right of access to the information on the officials' personal computers then it has authority from at least one court of appeals suggesting that the information may not be covered by the Act. The definition of public information in the statute seems more consistent with the court's interpretation rather than the Attorney General's.

If a city wants to argue that e-mails on personal devices are not covered by a public information request there is good authority to support such a position, although the city should plan to seek confirmation of its position from the courts rather than the Attorney General. While the greater weight of legal authority would suggest that the better option is to take the position that the e-mails are not public information, such a course is not without risk. The risk factors include:

- To maximize the chance of prevailing on the argument that the city has no right of access to the e-mails on a personal computer, the better course is probably to decline to submit the issue to the Attorney General---or at least to decline to produce copies of the e-mails. If the e-mails are produced, the Attorney General or a court may conclude that the city, in fact, has access to them. Thus, if it is to pursue a course that is designed to increase the



odds that the e-mails will be found to be outside the scope of the Act, the city may have to waive the opportunity to assert the argument that the e-mails are protected from disclosure by one of the exceptions in the Act. TEX. GOV'T CODE § 552.302 (information is presumed to be subject to disclosure if not submitted to the Attorney General in a timely manner).

- Other courts of appeal may not follow the Dallas court's lead.
- The city and its officials will subject themselves to accusations that they are withholding information that the Attorney General has fairly consistently said is covered by the Act. Explanations based on the contention that the Attorney General may be wrong or that a court has come to a different conclusion may bear little weight with a public that is not likely to follow a nuanced legal argument.
- The city and its officials may be subjecting themselves to sustained criticism by the local media and to accusations that they are both hiding something and violating the Public Information Act. This can be a particular factor when a member of the media is the one requesting the information. Or to put it another way, it is seldom a good idea to get in a fight with someone who buys ink by the barrel. When the client consists of elected officials or others who depend on the good will of the public, that can be a significant factor.

### **ONE CITY'S RESPONSE**

Perhaps the primary argument supporting the Attorney General's interpretation is that a reading of the Act that permitted officials to avoid public scrutiny of documents in which public business is transacted or discussed merely by using a personal, rather than a city-owned, computer would emasculate the Act. That is a compelling policy argument even if it does not

conform to the precise language of the statute, and cities generally would not want to be in the position of appearing to participate in a system to hide information.

When the City of Austin received multiple, sweeping requests for e-mails on personal computers and smart phones of the mayor, city council members, the manager, and city staff, it took the position, relying on the language of the statute and the *City of Dallas* case, that such documents were not public information under the Act. Nevertheless, the officials decided to submit them voluntarily to the city and, by doing so, to bring them within the scope of the Act.

Once the officials turned over the documents stored on their personal computers and smartphones to the city, the documents unquestionably fell within the definition of public information and were subject to being released unless they fell within one of the Act's exceptions. The city additionally adopted a policy to cover future situations. Under the policy, the council will use city, rather than personal, accounts for electronic communications. By using city accounts, the documents will be maintained by the city from their inception and clearly will be covered by the Act. In the event that a councilmember is unable to use a city account, the policy requires the councilmember to forward the communication to the city. This will cause them to be stored on the city's server. In this way all electronic communications relating to city business will be on the city server and in the possession of the city. In the event there is a request for a council member's e-mails, there will be no question that they are possessed by the city and are public information within the meaning of the Public Information Act. By ensuring all such communications end up on the city server, the individual council members avoid the problem of having to know what documents have to be retained and for how long. Instead, the city, and not the individual councilmember, will be responsible for ensuring that appropriate records retention protocol is followed. Because the charter placed responsibility for direction of

city employees under the manager, rather than the council, the council was not able to apply the policy to employees; however, it directed the manager to develop a policy for employees, and he implemented one that is essentially the same for city employees.

**THE POTENTIAL THAT COMMUNICATIONS ON  
ELECTRONIC DEVICES MAY VIOLATE THE OPEN MEETINGS ACT**

While the Open Meetings Act, TEX. GOV'T CODE § 551.001, *et seq.*, generally contemplates formal meetings at which all members of the governmental body have the opportunity to be present and participate, it also extends to less formal gatherings and to situation that one typically would not think of as a meeting of a governmental body. For example, fairly early in the Act's history, a series of telephone calls by which members of a school board were individually polled about a decision to send a letter to parents in the district was found to constitute a meeting covered by the Act. *Hitt v. Mabry*, 687 S.W.2d 791 (Tex. App.—San Antonio 1985, no writ). Thus, it has long been settled that members of a governmental body need not be physically present in the same place or to participate at the same time in order to participate in a meeting within the meaning of the Act. Additionally, the Attorney General has rejected any interpretation of the Act as not extending to “forms of nonspoken exchange, such as written materials or electronic mail.” OP. TEX. ATT'Y GEN. No. JC-0307 (2000). Since one can meet through non-spoken means such as electronic communication, e-mails among members of the city council can lead to a violation of the Act.

There are two criminal provisions of the Act that are potentially at issue. Under section 551.144, it is a criminal offense to participate in an unauthorized closed meeting. Conceivably a council could be found to meet by means of an e-mail chain or similar electronic communication. More troubling is section 551.143, which forbids conspiring to circumvent the provisions of the Act by meeting in numbers of less than a quorum for the purpose of secret deliberations. TEX.

GOV'T CODE § 551.143. Under this section governmental officials have found themselves charged with a crime for conduct they never realized might constitute a meeting within the meaning of the Act. Of course, the governmental official need not realize that the action constitutes a violation to be charged. *Tovar v. State*, 978 S.W.2d 584, 587 (Tex. Crim. 1998) (en banc).

One example of how section 551.143 may be violated comes from a San Antonio case. In *Esperanza Peace and Justice Center v. City of San Antonio*, 316 F. Supp.2d 433 (W.D. Tex. 2001), members of the San Antonio city council met with the mayor and the city manager in small groups taking care always to avoid the physical presence of a quorum. In addition, some members spoke with the mayor by telephone. The purpose of the discussion was to reach a consensus on the city budget, which was to be voted on by the council the next day. After the discussions, the members signed a memorandum setting forth the council's consensus on the budget and outlining amendments that would be presented to implement the consensus. While the council members realized that the memorandum was not binding, no one departed from it in the meeting. *Esperanza*, 316 F. Supp.2d at 471-72. Although the issue was presented in the civil rather than the criminal context, the court had no problem finding that the council had violated the Act. *Id.* at 477. The court's decision was based in large part on its finding that the purpose of the small meetings and circulation of the memorandum was to avoid the requirements of the Act—*i.e.*, to arrive at a majority decision in private while avoiding the technical requirements of the Act. *Id.* at 476-77.

Similarly, in 2005, an Upshur County grand jury, at the request of the Attorney General, returned an indictment charging that the president of a school board violated the provision of the Act that prohibits conspiring the circumvent the provisions of the Act by meeting in numbers of

less than a quorum by conferring individually with members of the school board on a matter he planned to bring before the board. In another case involving the City of Alpine, a city councilmember sent an e-mail to four other councilmembers asking if they believed an item should be placed on a future agenda so that it could be discussed by the council. One of the four councilmembers responded saying that she agreed that the item was relevant and should be discussed. There was no discussion of the merits of the proposal, only whether it should be placed on a future agenda. The Brewster County District Attorney believed the exchange violated the Act, and the two councilmembers were indicted by the grand jury for violating the Open Meetings Act.<sup>1</sup> Scott Houston, Texas Municipal League, *Texas Open Meetings Act: Constitutional?* (April 2011). In neither the Upshur County nor the Alpine cases were the governmental officials convicted, but the mere fact of being indicted can be devastating.

The use of e-mails and similar electronic communications poses a real risk for governmental officials. Because of the capability to use the “Reply All” function or to forward an e-mail chain to other persons, there is the possibility that a public official can discuss an issue with a quorum of the governmental body without realizing that he or she has done so. And it is not just conversations that attempt to address and resolve an issue before it comes before the city council or other governmental body prior to the time the council acts in a formal meeting that will pose problems. As the Alpine case demonstrated, at least one grand jury believed that an e-mail merely asking if an issue should be posted for an open meeting was a violation of the Act. Further, it is not simply conversations that relate to items that are scheduled for ultimate action

---

<sup>1</sup> This led to the well known Alpine case in which the constitutionality of the Open Meetings Act was challenged. The original case produced a Fifth Circuit opinion saying that strict scrutiny should be the standard to apply in deciding the constitutional question, *Rangra v. Brown*, 566 F.3d 515 (5<sup>th</sup> Cir. 2009); however, the full court agreed to hear the case en banc but ultimately dismissed it for mootness. *Rangra v. Brown*, 584 F.3d 206 (5<sup>th</sup> Cir. 2009). After *Rangra* was dismissed, another case was filed raising the same issue. It is now pending in the Fifth Circuit. *Asgeirsson v. Abbott*, No. 11-50441.

by the governmental body that can lead to a violation. The statutory definition of deliberations that are prohibited under the Act indicates that it is an exchange “concerning as issue *within the jurisdiction of the governmental body or any public business.*” TEX. GOV’T CODE § 551.001(2). It is certainly possible that a conversation could involve an issue within the city’s jurisdiction even though it is not something that has been or is likely to be on a specific agenda of the city council.

The danger of a councilmember’s communicating by e-mail with other members of the council regarding city is exacerbated by the fact that the communication produces a record of the violation. If members simply talk, it may be violation, but it may be difficult to establish exactly what was said and who were the parties to the conversation. With e-mail, though, there is a written record, not only of the specific communication, but also of other communications that can be pieced together to show a walking quorum or daisy chain. Councilmembers should take great care to avoid violating the Open Meetings Act, and certainly should take care to avoid doing so by creating a record for a potential prosecutor.

**THE POSSIBILITY THAT THE INCREASED USE OF ELECTRONIC COMMUNICATIONS WILL RESULT IN INADVERTENT VIOLATIONS OF RECORD RETENTION STATUTES**

Dozens and perhaps scores of times every day a governmental official or employee will read an e-mail and, after reading, routinely delete it. Similarly, that official or employee may create and send e-mails and make no effort to ensure that the record of the communication is not automatically erased after some period of time. When the electronic communication is on a home computer or personal cell phone, the user may give even less thought to retention issues than he or she might when using an office computer. These innocent, routine acts, however,

potentially can result in a violation of state record retention policies or statutory prohibitions against the destruction of government records.

The Texas Public Information Act prohibits anyone from destroying, removing or altering public information, and carries criminal penalties for violations. An offense under this section is a misdemeanor punishable by (a) a fine of not less than \$25 and not more than \$4,000, (b) confinement in county jail for not less than three days and not more than three months, and/or (c) both the fine and confinement. TEX. GOV'T CODE § 552.351. The Local Government Records Act ("LGRA") may also prevent the destruction of personal emails that pertain, in whole or in part, to public business. Under the LGRA cities are required to create records retention programs to maintain "all local government records." These records are broadly defined to include any materials "in electronic medium" ... "regardless of whether public access to [them] is open or restricted" ... "that are created or received by a local government or any of its officers or employees ... in the transaction of public business." TEX. LOC. GOV'T CODE § 201.003. Governing bodies must also (a) prepare a records control schedule to inventory documents and establish a period for their maintenance, and (b) designate a records management officer to administer the retention program. TEX. LOC. GOV'T CODE §§ 203.041, 203.025. The LGRA mandates that (a) no public record may be destroyed unless its retention period has expired, and (b) the destruction of public records prior to the end of the retention period is a Class A misdemeanor. TEX. LOC. GOV'T CODE §§ 202.001, 202.008.

In regard to e-mails, the retention period, assuming that a local records control schedule does not establish a longer period, will generally be controlled by the schedule for correspondence and internal memoranda found at section 1000-26 of Local Schedule GR (3<sup>rd</sup> Edition) promulgated by the Texas State Library and Archives Commission. 13 TAC § 7.125

(2011). For correspondence and memoranda relating to policy and program development the retention period is five years. 13 TAC § 7.125, Local Schedule GR (3<sup>rd</sup> Edition), § 1000-26(a). If the correspondence relates to an administrative matter—*i.e.*, “pertaining to or arising from the routine administration or operation of the policies, programs, services, and projects of a local government—the retention period is two years. 13 TAC § 7.125, Local Schedule GR (3<sup>rd</sup> Edition), § 1000-26(b). If, however, it is routine correspondence, such as “letters of transmittal, requests for publications, internal meeting notices, and similar routine matters” the documents need not be retained. 13 TAC § 7.125, Local Schedule GR (3<sup>rd</sup> Edition), § 1000-26(c). It is important for officials and employees to be familiar with these rules and to remember them in their day-to-day interaction with e-mail. Depending on the capability and design of a city’s computer system, it may be possible to simplify this task by providing for automatic retention or by forcing a choice of how to categorize an e-mail prior to sending a newly created e-mail or deleting a received one.

Exactly what happens to a deleted e-mail may vary from system to system. Generally, when a person deletes an e-mail it is simply moved to a “trash bin” or similar location on the computer so that it is simply retained at that different, less conspicuous location. The trash bin may be emptied automatically or manually after some period of time, in which case, it may no longer be accessible. Most offices, though, will periodically back-up information on a computer so that the information will be retained on back-up disks or tapes. These, however, may be written over periodically, which will eliminate the old data. The bottom line is that data that are deleted may be recoverable---at least for some period of time---and that systems can be designed and operated so that even deleted data can be retained and available through back-up and storage



media. This is important in being able to recover e-mails that might be thought to have been deleted and to be able fully to respond to public information requests.

### **STRATEGIES FOR SUCCESSFULLY DEALING WITH ELECTRONIC RECORDS**

Although electronic records are subject to the Public Information Act and similar statutes to much the same extent as more traditional records, they do pose special problems due to their volume, accessibility, and occasional propensity to be located on home computers or personal electronic devices. There are things a city can do to minimize or avoid problems that might otherwise occur in dealing with electronic records.

#### **Keep records on the city computer system rather than on personal devices**

Perhaps the most difficult issues arise in regard to electronic records, such as e-mails, kept on home computers or personal cell phones and similar devices. As discussed earlier in this paper, there is a very good argument that such records are outside the scope of the Public Information Act. To take that position, though—even if the city would ultimately be successful in court—almost certainly puts the city on the opposite side as the Attorney General and may well subject the city to media accusations that it is not complying with the law and to the perception that it is hiding damaging information. While such accusations and perceptions may be ill-founded, a city and its public officials may well find that it is in their interest to avoid that situation. The policy recently adopted by the City of Austin is a good way to avoid these problems and to assure the citizenry that the city is conducting business in the open. This policy includes:

- Requiring that e-mails and similar communications be made on city, rather than personal e-mail accounts, and.
- In the event it is not possible to use a city account, to forward the e-mail to a city account.

By following these steps, all e-mails involving city business should reside on city computers. This will centralize the search function so that it can be done with on the city computer system rather than needing to be done, at least in part, on councilmembers' home computers and other personal electronic devices. Also, it keeps council members and employees from having to make records retention decisions about the records on their personal devices as the records will be either originally created on or transferred to the city system.

As part of the effort to ensure that all records are kept on city, rather than personal, devices, council members should avoid putting their personal e-mail address, rather than a city e-mail address, on business cards, web-sites, and stationery. In those situations where a city chooses to continue to conduct correspondence that might relate to city business on home computers and personal smartphones, avoiding noting personal e-mail addresses on city business cards, stationery, and web-sites will strengthen the legal arguments that any messages to or from those address are not created by or for the city.

### **Have a Records Retention and Management Policy**

State law requires local government bodies to designate a records management officer and to adopt a records control schedule. TEX. LOC. GOV'T CODE §§ 203.025(a), 203.041(a). Cities should make sure that all officials and employees who create or handle records are familiar with their duties under the policy so that records are not inadvertently destroyed. Additionally, cities should work with their information technology specialists and their records manager to design the computer system whenever feasible to simplify records retention.

### **Take special care in responding to requests for electronic records**

It is often the case that cities will receive multiple requests for the same or similar information. These may involve overlapping date ranges or somewhat different definitions of

the information sought so that the city will be required to conduct unique searches for each request. This can result in producing some records for one request that should have been produced in response to other requests but that were not. This can be embarrassing to the city and its officials and can create the perception that the city is less than competent or is hiding something. A good way to avoid this possibility is to have a central search function. It is generally a good idea to have the information technology department involved in searches for electronic records. Those specialists will be able to conduct a more thorough search and perhaps locate documents that appeared to have been deleted. Having a person in charge of all searches can assist in seeing that consistent search terms are used. It is a good idea to brainstorm the various terms that might be included in the requested documents to ensure that the search is designed to produce the maximum opportunity to locate any relevant document.

The number and variety of electronic records can be massive and the technical issues daunting and failure to respond quickly or accurately can result in a media firestorm. These suggestions may reduce the opportunity for error and provide a greater opportunity for the city to comply with the statute and to preserve public confidence in its actions.