



By Gena M. Stinnett, Associate, Richards, Watson and Gershon

During the last ten years, the use of email and other electronic communications has grown exponentially.

Cities and other public agencies now rely on email, instant messaging, and other forms of text messaging to conduct business. These electronic communications are frequently written as casually as people speak, and without thought that they might one day be released to the public. Yet open government laws or litigation rules could compel a city's employees to locate and disclose email or text messages that were never intended to be a public record.

Under California's Public Records Act (Gov't Code § 6250 et seq.), cities are required to disclose "public records" upon request, unless the record is exempt from disclosure pursuant to a statutory exemption. A public record is "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." (Gov't Code § 6252(e).) Emails and other electronic communications may fall within this broad definition.

To diminish the risk of disclosing sensitive emails and text messages, you and your city might consider the following suggested practices:

**Avoid using city-owned devices for personal matters.** You may have a reduced privacy interest in electronic communications sent or received using a city-issued electronic device, depending in part upon the policies adopted by your city. There is a significant probability that electronic information stored on a city's computer system or on other city-issued electronic devices will be discoverable

in litigation or disclosable pursuant to a Public Records Act request.

For example, Detroit Mayor Kwame Kilpatrick used a city-issued text pager while conducting an extramarital affair. He engaged in frequent "text sex" messages with his chief of staff, Christine Beatty. Later, each denied the affair under oath. When the text messages surfaced, both were charged with obstructing justice and are now serving jail time.

**Remember the headline test.** Emails you send discussing city business might be obtained by the press, and the contents appear in the headline or text of a newspaper article. You can lessen the risk of embarrassment if you avoid sending an email that you would not be comfortable reading about in your local newspaper. At times it may be wiser to discuss city business by phone or in person.

**Avoid commingling work and personal electronic communications on your home computer or personal electronic devices.** For example, if you take electronic files home with you, or if you download city email onto your home computer or a BlackBerry you own, think about ways to keep your private computer files and email separate from your city files and email.

If you use your home computer or personal electronic devices to work on city business, and your city receives a Public Records Act request or litigation discovery demand, you may have to produce records from your personal devices. If you have not effectively segregated your private electronic files and email from your city-related files and email, an attorney might need to review both your personal and work-related information to determine what is city business and what is not city business.

**Clean files of metadata before using email to forward documents.** You may be accustomed to attaching documents or spreadsheets to emails sent to colleagues, consultants or even members of the public. Those

attachments contain metadata. Metadata is defined as "information describing the history, tracking, or management of an electronic document." (Williams v. Sprint, 230 FRD 640, 646 (D. Kan. 2005).) In MS-Word, you may view some of the metadata by clicking on "File" then "Properties." Someone sophisticated with electronic documents can mine metadata to reveal edits to the document. Also, if you make edits using Track Changes, merely "turning off" the display of tracked changes does not eliminate the trail of edits. The receiving party can simply turn the display of Track Changes back on, and view the edits.

Metadata can range from misleading (the author is not the person listed) to harmful. An example of harmful metadata is metadata that allows someone outside the scope of the attorney-client privilege to see attorney-client communications, such as comments or edits made by your city attorney. Metadata mining may also reveal changes to a document that you or your colleagues made, revealing your thought process. Software programs are available to scrub metadata and clean the document so that prior edits, author information and document sharing information is not revealed. Your city may want to consider implementing software that removes metadata, if it has not done so already.

In conclusion, these are just a few "best practices" you and your city may want to consider. It is also important for cities to adopt email policies that give clear guidance to staff in the proper use and retention of email or other electronic communications. Preventive action may be a lower priority in these constrained budgetary time, but the harm caused by the release of embarrassing or confidential information could be devastating. 📌

*Gena M. Stinnett is an associate with Richards, Watson and Gershon in their downtown Los Angeles office. She is chair of the firm's E-Documents and Public Records Practice Group. She is also Assistant City Attorney for the cities of Rancho Palos Verdes, Monrovia and Beverly Hills. She can be contacted at [gstinnett@rwglaw.com](mailto:gstinnett@rwglaw.com).*