SanDiego LAFCO
Local Agency Formation Commission

OFFICE OF THE GENERAL COUNSEL

M E M O R A N D U M

TO: Michael D. Ott, Executive Officer

FROM: Michael G. Colantuono, General Counsel
Aleks R. Giragosian, Assistant General Counsel

CC: Holly O. Whatley, Assistant General Counsel

DATE: May 1, 2017

SUBJECT: New Supreme Court Ruling on Public Access to Electronic Records Generated on Personal Devices and in Personal Email Accounts

EXECUTIVE SUMMARY

As you know, on March 2, the California Supreme Court published its decision in *City of San Jose v. Superior Court*,[1] concluding the California Public Records Act ("CPRA") applies to electronic communications that local government officials and employees send on private devices from private accounts. The case will require LAFCO to consider its policy regarding access to such communications and, as promised, we write to advise you of your policy options.

These include: (1) prohibiting the use of personal accounts for the conduct of LAFCO business (as the federal government does); (2) allowing the use of personal accounts, but requiring all electronic communications to be copied to LAFCO's server (so records requests can be honored without resort to private devices and accounts); or (3) allowing the use of personal accounts only if the electronic communications are stored for a minimum of two years and are searchable. In the alternative, LAFCO may adopt a policy designating some or all emails, text messages, and social media posts on personal accounts as non-records because they are not retained in the usual course of LAFCO business.

[1] *City of San Jose v. Superior Court* (March 2, 2017, S218066) ___Cal.5th___ <http://www.courts.ca.gov/opinions/documents/S218066.PDF>, [p. 3].

ANALYSIS

1. FACTS

In *City of San Jose v. Superior Court*, a resident of that city requested all the voicemails, emails or text messages sent or received on private electronic devices used by the mayor, city council members, and city staff regarding any matter concerning the city. San Jose provided all the requested records stored in city accounts, but refused to provide records stored in personal accounts, asserting these items were not public records under the CPRA. The trial court ordered production of the records, the Court of Appeal reversed, and the Supreme Court granted review, agreeing on March 2d with the trial court.

2. EARLIER LAW

As you know, the CPRA requires disclosure of public records upon request.[2] A public record "includes [1] any writing [2] containing information relating to the conduct of the public's business [3] prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[3] The CPRA is interpreted broadly to promote public access to government information.

3. SUPREME COURT'S RULING

The Court analyzed the statute's definition of "public record" and held, "a city employee's writings about public business are not excluded from CPRA simply because they have been sent, received, or stored in a personal account."[4] "If public officials could evade the law simply by clicking into a different email account, or communicating through a personal device, sensitive information could routinely evade public scrutiny."[5]

---

[2] Gov. Code § 6253.
[3] Gov. Code § 6252, subd. (e).
[4] *City of San Jose v. Superior Court* (March 2, 2017, S218066) ___ Cal.5th ___ [p. 21].
[5] *Id*. at p. 16.

i. ANY WRITINGS

It was undisputed that voicemails, emails, or text messages are "writings" subject the CPRA. All three fall within the CPRA's broad definition of that term.[6] The Court added that "[e]mail, text messaging, and other electronic platforms" can all be used to prepare, exchange, and store writings. The phrase "other electronic platforms" likely encompasses Twitter, Facebook, blog posts, and other social media.

ii. CONTAINING INFORMATION RELATING TO THE CONDUCT OF THE PUBLIC'S BUSINESS

The Court acknowledged electronic communications on private devices and servers blur the line between personal and public business. The Court clarified that an electronic communication does not become a public record just because the public finds it interesting. At a minimum, the communication must relate in some substantive way to the conduct of the public's business. "Communications that are primarily personal, containing no more than incidental mentions of agency business, generally will not constitute public records."[7]

Whether a communication is subject to the CPRA turns on factors "including (1) the content itself, (2) the context in, or purpose for which, it was written, (3) the audience to whom it was directed, and (4) whether the writing was prepared by an employee acting or purporting to act within the scope of his or her employment."[8] For example, an email to a spouse complaining about a coworker would likely not be a public record, whereas an email to a superior reporting a coworker's mismanagement would be.[9] Comparably, a constituent's email to a Commissioner concerning a LAFCO-related matter, regardless of the constituent's expectation of privacy, is likely a public record.

---

[6] *Id*. at p. 6.
[7] *Id*. at p. 7.
[8] *Ibid*.
[9] *Id*. at pp. 6–7.

iii. PREPARED, OWNED, USED, OR RETAINED BY A STATE OR LOCAL AGENCY

The Court held a writing prepared by a public employee conducting agency business is "prepared" by the agency within the meaning of the CPRA, even if it is prepared using a personal account.[10] The Court did not distinguish between the personal writings of an individual and the official writings of an agency.

Similarly, a writing retained by a public employee conducting agency business is "retained" by the agency for purposes of the CPRA, even if it is retained in an employee's personal account.[11] The content and context of the writing are what matter, not the means of communication or its location.

RECOMMENDATIONS

The Court did not specify how agencies may comply with its decision and provide public access to records stored on private devices and in private accounts. "Agencies may develop their own internal policies for conducting searches."[12] In light of the Court's decision, the LAFCO should adopt a policy addressing public records on personal accounts while protecting the privacy of public officials and employees and giving the public fair warning their electronic interactions with public officials will be treated as public records.

Three potential options include: (1) prohibiting the use of personal accounts for conducting LAFCO-related business; (2) allowing the use of personal accounts, but requiring all electronic communications to be copied to the LAFCO's server; or (3) allowing the use of personal accounts only if the electronic communications are stored for a minimum of two years and employees and officials agree to search those accounts (or allow the LAFCO to do so) when necessary to respond to records requests.

Prohibiting the use of personal accounts for conducting LAFCO-related business is the most straightforward approach and is the federal policy. But enforcing the policy will be challenging as administrators cannot easily track which electronic

[10] *Id*. at p. 10.
[11] *Id*. at p. 13.
[12] *Id*. at p. 19.

communications are taking place via personal or LAFCO account. This method also imposes significant burdens on officers and employees who may find it difficult to communicate LAFCO-related business remotely, in the absence of LAFCO-issued devices. It may also be difficult for agencies which cannot fund devices or accounts for their elected officials

Another option is to allow the use of personal accounts, but require all electronic communications to be copied to an address on the LAFCO's server. For example, all LAFCO-related emails sent from a personal email account could carbon copy the individual's LAFCO account (if LAFCO establishes such accounts), a designated LAFCO staffer, or an email address established for this purposes. LAFCO-related posts from a personal Facebook account might tag a LAFCO Facebook page. However, some forms of communication, like text messages and voicemails, cannot easily be copied to a LAFCO server. They bear separate treatment under the policy and may be best defined as records not ordinarily retained in the course of LAFCO business unless consciously archived.

A third option is to allow the use of personal accounts for electronic communications only if the electronic communications are stored for a minimum of two years and the account holder agrees to search the account (or allow LAFCO to do so) when necessary to comply with records requests. Searches of personal accounts may be conducted by the owner if he or she has undergone CPRA training to identify public records. In addition, LAFCO should create a form to be signed by the official or employee stating that he or she: (1) was trained, (2) completed the search, and (3) did or did not find relevant public records.

Short of a complete prohibition on the use of personal accounts to conduct agency business, nothing will shield from the CPRA private electronic communications concerning LAFCO business. LAFCO may withhold confidential and purely personal records and may redact private or privileged information (at some cost), but cannot withhold a public record entirely. LAFCO officials and employees engaging in personal or political communication regarding LAFCO business should note somewhere in the communication that they are expressing their personal views and not conducting LAFCO business. Furthermore, sensitive topics should be discussed in person and not in electronic format.

We recommend LAFCO consider these options and prepare a policy in consultation with technology and records-management staff. We will be happy to assist and can provide model policies if you wish.

If you would like more information regarding the issues discussed in this memo, please do not hesitate to contact Michael at 432-7357 or MColantuono@chwlaw.us or Aleks at (213) 542-5734 or AGiragosian@chwlaw.us.

SAN DIEGO LOCAL AGENCY FORMATION COMMISSION
ELECTRONIC DOCUMENT RETENTION POLICY
(Approved by the Commission on May 1, 2017)

The Electronic Document Retention Policy of the San Diego Local Agency Formation Commission ("LAFCO") governs the retention of text messages, voicemail messages, social media posts, and email messages sent or received in the conduct of LAFCO business.

Definitions

1. Email Message: An electronic communication sent and received via web mail or email client.

2. Social Media: Information posted to websites and applications that enable users to create and share content or to participate in social networking, including Facebook, Twitter, Instagram, Snapchat, and LinkedIn.

3. Text Message: An electronic, written communication sent and received via telephone or Internet connection.

4. Voicemail Message: An electronic, oral communication sent or received via telephone or Internet connection.

Text Messages, Voicemail Messages, and Social Media

Text messages, voicemail messages, and social media posts not saved to an archive or a more permanent medium are intended to be ephemeral documents, not preserved in the ordinary course of business. Accordingly, they do not constitute disclosable public records, as that term is defined by Government Code section 6252, subdivision (e). LAFCO officials and employees are not required to retain these electronic documents. Business done on behalf of LAFCO that requires the creation and preservation of records should be conducted in other media.

Email Messages

1. The San Diego LAFCO has an email server account with the County of San Diego for purposes of sending and receiving email messages. LAFCO email messages are accordingly subject to LAFCO's and the County of San Diego's email retention policies and procedures. The County of San Diego currently retains emails that are sent and received by LAFCO for a period of 60-days and then they are automatically deleted from the server. Therefore, email messages sent or received by the San Diego LAFCO from and after May 1, 2017 will be preserved for a period of 60-days and will be made available for public inspection on the same terms as other LAFCO records. Exceptions to this 60-day retention provision will be emails that are preserved on paper or electronic archives. Emails that are preserved electronically or on paper will be retained and made available for a period of two years.

2. Except as provided in point 3 below, LAFCO officials and employees are required to use (or copy to an address on) the LAFCO email account with the County of San Diego for all

email messages regarding matters of LAFCO business. Such email messages that fall within point 1 above will be preserved pursuant to point 1 and will be made available for public inspection on the same terms as other LAFCO records.

3. Commissioners (but not LAFCO staff) need not use the LAFCO's server account with the County of Diego for email messages to and from residents, business owners and property owners within the LAFCO's jurisdiction that are not addressed or copied to any other LAFCO officials and employees, and these Email Messages fall outside points 1 and 2 above. Nor need these officials use the LAFCO server account for email traffic in their personal, political and professional lives unrelated to LAFCO business. These Email Messages, too, fall outside points 1 and 2 above.

4. LAFCO will continue to comply with Government Code § 54957.5 which deems to be a public record any document communicated to a majority of officials, whether at the same time or seriatim, with respect to an item of LAFCO business regardless of the means of that communication, including via non-LAFCO email accounts. Commissioners are encouraged to forward such email messages not received via the LAFCO server account nor copied to LAFCO staff or to an email address designated for that purpose so they can be preserved in the LAFCO's email retention system, relieving individual Commissioners of any duty to preserve such email messages or make them available for public inspection.

This policy applies only to the conduct of LAFCO business. It has no application to communications to or from Commissioners in their other public and private capacities nor to communications to or from LAFCO staff that are personal, private or otherwise not LAFCO business.