# PUBLIC RECORDS PRACTICES AFTER THE *SAN JOSÉ* DECISION

**Thursday, July 20, 2017 – 10:00a.m. - 11:30a.m.**

**Jolie Houston,** Interim City Attorney, City of Merced
Assistant City Attorney, City of Gilroy
Partner, Berliner Cohen

**HongDao Nguyen,** Assistant City Attorney, City of Stanton
Assistant City Attorney, City of Lake Forest
Deputy City Attorney, City of San Juan Capistrano
Associate, Best Best & Krieger

## PUBLIC RECORDS PRACTICES AFTER THE *SAN JOSÉ* DECISION

Local agencies throughout the state have wrestled with the decision in *City of San José v. Superior Court* since the California Supreme Court issued its opinion earlier this year.[i] The court found that records in local agency employees' personal accounts or devices may be subject to the California Public Records Act (CPRA) if the records pertain to public business. In the opinion's aftermath, many local agencies have received requests for records in public employees' and officials' personal email, text messaging, and social media accounts.

### Background of the *San José* Case

The *San José* case was borne out of a PRA request by Ted Smith, described by media accounts as a former attorney with a background in nonprofit work. Smith's request to the City of San José asked for, among other things, "all electronic information relating to public business, sent or received by [San José's-then mayor and then-council members] using his or her private electronic devices" related to a real estate deal involving the City. When the City did not provide documents from Council members' personal accounts or devices, Smith sued and won in the trial court. The appellate court reversed the trial court decision, and on petition, the California Supreme Court reversed the appellate decision. The State's highest court ruled: "[W]e hold that when a city employee uses a personal account to communicate about the conduct of public business, the writings may be subject to disclosure under the California Public Records Act…."

### What This Resource Paper Will and Will Not Do

This resource paper will explore the issues surrounding the *San José* case with an important caveat: the law continues to evolve on the topic of public records in personal accounts and devices. The *San José* decision was filed in March 2017, and no subsequent case law has addressed this issue. Moreover, no legislation has been passed on this topic. Therefore, local agencies only have the *San José* case to dissect and interpret.

While the *San José* court provided "Guidance for Conducting Searches" of personal accounts or devices, even the *San José* court qualified that guidance by noting, "we do not hold any particular search method is required or necessarily adequate." As such, this resource paper will explore the many issues left unresolved by the decision with the understanding that those issues may later be resolved through subsequent case law or legislative action.

### Scope and Application of the Case to Local Agencies

#### Does *San José* apply to public officials or just public employees?

Most likely, *San José* applies to public officials in addition to public employees. The court held that "when a city employee uses a personal account to communicate about the conduct of public business, the writings may be subject to disclosure under the California Public Records Act."[ii] Some have questioned whether the ruling applies to public officials because the ruling only calls out city *employees.* However, there's a good reason why *San José* likely applies to public

officials, too: The CPRA request at issue targeted, among other things, text messages on council members' personal phones. Certainly the court was aware of the underlying facts of the case.

Moreover, the opinion is peppered with references to public officials. For example, in supporting its ruling, the court opined, "there is no indication the Legislature meant to allow *public officials* to shield communications about official business simply by directing them through personal accounts." The justices also opined, "We are aware of no California law requiring that *public officials* or employees use only government accounts to conduct public business. If communications sent through personal accounts were categorically excluded from the CPRA, *government officials* could hide their most sensitive, and potentially damning, discussions in such accounts." [Emphasis added.] As such, it would be risky for a local agency to assume that public officials are not subject to the *San José* ruling.

**Does *San José* really apply the CPRA to text messages?**

In the wake of *San José*, some have expressed dismay that text messages in public employees' and officials' personal phones could be public records under the CPRA. This is understandable, as text messaging is a newer form of electronic communication. However, the CPRA request at issue in *San José* targeted "emails and text messages 'sent or received on private electronic devices used by' the mayor, two city council members and their staffs." Thus, text messages in a public employee's or official's personal account or device may be subject to the CPRA if those text messages pertain to public business.

**Does *San José* apply to social media accounts?**

*San José* does not explicitly mention social media accounts like Facebook or Twitter. However, the court acknowledged that records in "other electronic platforms" could also be subject to the CPRA. For example, if a public employee or official emails a constituent from his or her personal account about a civic center groundbreaking, for practical purposes, that same correspondence should also be a public record even if the discussion occurred in a private Facebook message.

In *San José*, the court looked past where the message resided and which electronic medium was used. Rather, if a record meets the "factors" mentioned in this paper, it is probably a public record subject to the CPRA, regardless of the record's location or electronic medium.

## Public Record Requests and Responses under *San José*

**When a local agency receives a CPRA request for local agency correspondence, including emails, is the local agency required to automatically request that public employees and officials search their personal accounts or devices?**

*San José* did not change the way that local agencies typically respond to CPRA requests that ask for correspondence and emails. Rather, *San José* expanded the local agency's search obligation to include public employees' and officials' personal accounts or devices.

The *San José* court opined that the scope of a local agency's search for public records "need only be reasonably calculated to locate responsive documents." One way local agencies may fulfill that search obligation is to initially perform a search of the local agency server for responsive emails when the CPRA request is submitted. If there are responsive emails, then the custodian of records[iii] should ask the public employee or official whose name appears on the responsive emails if he or she has any "public records" in his or her personal accounts or devices. If there are responsive public records, they should be forwarded to the custodian of records for review and disclosure.[iv]

This search obligation should be governed by a rule of reasonableness. Not every CPRA request necessarily implicates public employees or officials. Routine CPRA requests may be fulfilled as they have been in the past. For example, a CPRA request for a routine local agency contract would not require that the local agency request that public employees or officials search their personal accounts or devices for that contract. Occasionally, especially on controversial topics, the requestor may revise or broaden his or her request, which may mean that public employees or officials will be required to search their personal accounts or devices for responsive records. As such, decisions regarding whether personal accounts or devices must be searched should be made on a case-by-case basis.

**Should a local agency assume that a CPRA request for public records from personal accounts or devices must be forwarded to *former* public employees or officials?**

Yes, if the former public employee or official was employed or in office, respectively, during the time period for which the records are requested. In *San José*, the court noted that "an agency's public records 'do not lose their agency character just because the official who possesses them takes them out the door.'" This appears to be true of former public employees and officials as well. In other words, just because a former public employee or public official may have left with public files or may have them filed in his or her personal email inbox does not mean that the records lose their public character. Of course, any record that the former public employee or official generated after he or she left the local agency would not be subject to the CPRA.

In some instances, when the local agency's custodian of records receives a CPRA request, he or she may have an idea of whether a former public employee or official may have responsive records in his or her personal accounts or devices and can reach out, directly, to those individuals. In other instances, the local agency's custodian of records may not have an indication of whether a former public employee or official has public records in his or her personal accounts or devices.

As discussed above, local agencies should conduct searches that are "reasonably calculated" to locate responsive records and must disclose records that the agencies can find with "reasonable effort." One way to fulfill the search obligation might be for the custodian of records to initially perform a search of the local agency server for responsive emails when the request is submitted. If there are responsive emails pertaining to the former public employees or officials, then the custodian of records should ask each former public employee or official whose name appears on the responsive emails if he or she has any "public records" in his or her personal accounts or

devices. If there are responsive public records, then they should be forwarded to the custodian of records for review and disclosure.

Regardless of how the local agency decides to deal with the issue, the agency should be prepared to demonstrate in writing (either to the requestor or a court or both) that it complied with *San José* and reasonably conducted its search by communicating the CPRA request to former public employees and officials, as necessary.

**In response to a CPRA request for "correspondence" related to a particular topic, should the local agency clarify whether the requester is seeking public records from a personal account or device?**

Under the *San José* case, a request for "public records" now includes public records wherever they are stored. That means that, in addition to searching local agency servers, the custodian of records should ask applicable public employees or officials whether they have public records in their personal accounts or devices each time a request comes in for "correspondence." Moreover, if a local agency *did* clarify whether the request was meant to include personal records in personal accounts or devices under Government Code section 6253.1, the answer would probably be "yes."

**What is the process of obtaining potential public records from public employees' and officials' personal accounts or devices?**

*San José* includes a section titled, "Guidance for Conducting Searches." In this portion of the opinion, the court emphasized that public employees and officials do not lose all of their privacy rights simply because they work for a local agency. The court explained that in responding to a CPRA request for public records in personal accounts or devices, a local agency does not need to seize computers or obtain individuals' user names and passwords to search for the records. Rather, local agencies are obligated to conduct searches that are "reasonably calculated" to locate responsive records and disclose records that the local agencies can find with "reasonable effort."

Like any other CPRA request, upon receiving a request for public records in individuals' personal accounts or devices, the local agency's custodian of records should reach out to the employees and officials who are the subject of the request. *San José* suggests that public employees and officials may then search *their own* personal files, accounts, and devices for responsive material.

**What "factors" should a local agency consider when deciding whether a record is public or personal?**

The court provided local agencies with the following "factors" to consider when determining whether a document is a public document or a private one.

**Content.** Does the content of the email relate in a substantive way to the conduct of the local agency's business? In *San José*, the court stated, "Whether a writing is sufficiently related to the public business will not always be clear. For example, depending on the context, an email to a

spouse complaining 'my coworker is an idiot' would likely not be a public record. Conversely, an email to a superior reporting the coworker's mismanagement of an agency project might well be."

**Context/Purpose.** Why was the email written? Was it written to conduct the local agency's business or further the local agency's interest?

**Audience.** To whom was the email sent? Was it sent to an agency employee, official, resident, consultant, agency stakeholder, etc.? Or was the email sent to a friend or family member?

**Scope.** Was the email written in the individual's capacity as an agency official or employee representing the agency? Or was the email written as a private individual?

Each record must be reviewed on a case-by-case basis to determine whether it is a public or personal record.

**If a local agency chooses to use an affidavit like the one the court referenced in *San José,* what should the affidavit contain?**

In *San José*, the court suggested that if a public employee or official withholds documents from his or her personal accounts or devices, then the individual may "submit an affidavit with facts sufficient to show the information is not a 'public record' under the CPRA." This practice is modeled after the federal Freedom of Information Act and a practice used in the State of Washington.[v]

There is no consensus, however, on whether local agencies should follow this practice or how to implement it. The CPRA and *San José* do not *require* this practice. However, if a local agency decides to use an affidavit to demonstrate that it has asked public employees and officials to search their personal accounts or devices, the affidavit could include the following: a description of the CPRA request, language stating that the employee or official searched his or her personal accounts and devices, and what action he or she is taking (for example, disclosing records, not disclosing records — including a description of why — or disclosing some and withholding some). The affidavit could then be filed away and produced if needed to defend the local agency in litigation or it could be provided to the requestor.

**How have other states, such as Washington, dealt with similar laws and case law providing that records in a public official's or employee's private devices or accounts may be subject to public disclosure?**

Other states, like Washington, have had more time to digest the idea of public records residing in personal accounts and devices. In *San José,* the court relied on a case decided by the Washington Supreme Court: *Nissen v. Pierce County.*[vi] In *Nissen*, the court held that an elected county prosecutor's text messages regarding work-related matters sent and received from his private cell phone could be public records. Following *Nissen,* additional case law is beginning to emerge, giving us a glimpse of what may eventually transpire in California.

For example, in 2016, a Washington appeals court found that under *Nissen*, a trial court could require an elected city council member to produce emails stored in his personal email account that were deemed city records. The trial court was also allowed to require the council member to submit an affidavit attesting to the adequacy of his search of his personal account.[vii] The council member had refused to provide records in his personal accounts, arguing (among other things) that he had a constitutional privacy right to personal records. Moreover, the city and council member argued that *Nissen* applied only to elected executive officers, not elected legislative officials. The Washington appellate court rejected those arguments.

**How long should public employees and officials retain public records in their personal accounts and devices?**

Although the CPRA is not a record retention statute, local agency public records on the agency's server generally must be retained in accordance with Government Code section 34090, which requires certain public records[viii] to be kept for at least two years.[ix] The retention statutes do not address records stored on personal accounts or devices, nor do they provide a specific retention period for emails, texts, or other forms of social media.

Now that we know public records may be stored in personal accounts or devices, public employees and officials should be made aware of their respective agencies' retention policies.

If a public employee or official is concerned about following retention schedules for messages on personal accounts or devices, the easiest solution is for him or her not to use personal accounts or devices for public business. If that's not possible, then a public employee or official could routinely forward public records from his or her personal accounts or devices to the local agency's server. Another solution could be to courtesy copy (cc) a local agency account on the message so that the message reaches the local agency's server. After taking one or both of those actions (forwarding or cc-ing the messages) the messages in the personal account or devices may be deleted. The CPRA does not require an agency to keep duplicate copies of a record.

Another way a local agency may ensure the retention of public records stored in personal accounts or devices is to ask all public employees and officials to conduct searches of their personal accounts or devices that are "reasonably calculated" to locate public records and forward those records to the custodian of records before a certain date. After the public employees or officials have forwarded all public records from his or her personal device or account to the custodian of records, the public employees or officials should delete those public records in their personal accounts or devices. Going forward from the established "cut-off" date, public employees and officials should <u>stop</u> using their personal accounts or devices for local agency business.[x] If this "cut-off" process is followed, then the local agency should have the public employees or officials confirm **<u>in writing</u>** that that they have complied with this request. Thereafter, the local agency should be able to rely on the public employee's or official's confirmation that after the "cut-off" date, there have been no public records generated from or stored in his or her personal accounts or devices.

**Are public officials' campaign-related records in their personal accounts or devices subject to disclosure under the CPRA?**

No. Campaign-related records in personal accounts or devices are not subject to the CPRA. State law prohibits individuals from using public resources for political purposes. Public officials may lawfully use only their personal or campaign accounts and devices for campaign purposes; such proper use of personal accounts or devices would not expose those political messages to public scrutiny under the CPRA.

## Policies, Best Practices, and Training to Comply with *San José*

### Make the public employees and officials aware.

If your local agency's employees or officials are not yet aware of the *San José* decision, then they should be made aware of it. This is as simple as the local agency's attorney or custodian of records sending an email to all public employees and officials apprising them of the court's decision and letting them know that records pertaining to local agency business in their personal accounts or devices may be subject to the CPRA.

### Update the local agency's CPRA policy

Similarly, the local agency should update its CPRA policy to implement the *San José* case. The policy update should acknowledge that public records may be found in personal devices or accounts, and that public employees and officials may be asked to search for and disclose such records to the local agency. Those records may then be turned over to a CPRA requestor, subject to applicable exemptions and privileges. Local agencies should also consider including a protocol that addresses public employees and officials who leave public employment or office to ensure that all public records stored in personal devices or accounts have been transferred to the local agency.

### Training local agency employees and officials

Once a policy is in place, local agency employees and officials should be trained to understand that records in their personal devices or accounts relating to agency business may be subject to the CPRA. Local agency employees and officials should be trained in how to distinguish between a personal record and a public record. Specifically, local agency employees and officials should be trained in the "factors," mentioned in this paper, that may make a record public or not.

Local agency employees and officials should also be trained in the agency's records retention schedule. If employees and officials keep records in their personal devices and accounts longer than the time period the agency keeps such documents, responsive documents kept in those devices or accounts may need to be produced to a requestor.

### Documentation

Local agencies should take care to document that they have asked their public employees and officials whether they have public records in their personal devices or accounts, when applicable.

In CPRA litigation, this information will be used as part of the local agency's defense as to whether it performed a reasonable search as required by the *San José* case, or not. Moreover, whether or not a local agency uses affidavits or not, the local agency should document whether public employees or officials have conducted a search for public records in their personal accounts or devices and whether those public employees or officials have provided any responsive documents as a result of that search. If a public employee or official has not responded to the local agency's request, the custodian of records (or city attorney) should follow-up in writing with that public employee or official. Again, a court will review a local agency's action to determine whether the local agency conducted a "reasonable" search.

---

[i] *City of San José v. Superior Court* (2017) 2 Cal.5th 608.

[ii] *Id*. at p. 614.

[iii] For purposes of this paper, we used the more general reference to the custodian of records, but it will most likely be the local agency/city clerk.

[iv] Once a record is forwarded to the custodian of records or local agency attorney, the record should be reviewed to determine whether applicable CPRA exemptions or privileges apply.

[v] *City of San Jose*, *supra*, 2 Cal.5th at p. 628, *citing Grand Central Partnership, Inc. v. Cuomo* (2d Cir. 1999) 166 F.3d 473, 481 and *Nissen v. Pierce County* (2015) 183 Wn2d 863.

[vi] *Nissen*, *supra*, 183 Wn2d 863.

[vii] *West v. Vermillion* (2016) 196 Wn.App. 627.

[viii] Though there is no definition of "records" for purposes of the retention requirements applicable to local agencies, the retention requirements and the disclosure requirements of the PRA should complement each other. Local agencies should exercise caution in deviating too far from the definition of "public records" in the PRA in interpreting what records should be retained under the records retention statutes. *See* League of California Cities: "The People's Business: A Guide to the California Public Records Act" revised April 2017, p. 67.

[ix] Retention of special district records are governed by Government Code sections 60200 through 60203, which do not include the same two-year minimum retention as Section 34090. However, many special districts follow the general two-year retention in Section 34090 for emails.

[x] For some local agencies, it may be difficult for all public employees and officials to cease using their personal accounts and devices for public business. In those instances, a best practice is to encourage public employees and officials to use their personal accounts and devices as little as possible for public business. If the personal accounts and devices are used for public business, the public records should be forwarded or copied to a local agency account.