# California Supreme Court Rules that Public Business Conducted on Personal Devices Result in Public Records

**03.03.2017 | By Ashley K. Dunning, John T. Kennedy**

In a major development impacting all public entities subject to the California Public Records Act (Gov. Code § 6250 *et seq*., hereafter CPRA), on March 2, 2017, the California Supreme Court unanimously held that public officers' and employees' communications on personal devices and nongovernmental accounts concerning the conduct of public business, are public records. As such, they are subject to disclosure in response to a CPRA request, unless a specific statutory exemption applies. *City of San Jose et al. v. Superior Court of Santa Clara County* (Mar. 2, 2017, S218066). Such devices, include, but are not limited to, personal cell phones, personal computers, and personal email accounts.

In so concluding, the Court observed, in today's environment, not all employment-related activity occurs during a conventional workday, or in an employer-maintained workplace. The Court contrasted the context in which the Legislature first enacted the CPRA in which the distinction between writings subject to the disclosure were fairly formal and focused on the business at hand, and the present. Today, these tangible, if laborious writing methods have been enhanced by electronic communication. Email, text messaging and other electronic platforms, permit writings to be prepared, exchanged, and stored more quickly and easily. However, the Court commented, the ease and immediacy of electronic communication has encouraged a commonplace tendency to share fleeting thoughts and random bits of information, with varying degrees of import, often to broad audiences. As a result, the line between an official communication and an electronic aside is now sometimes blurred.

Nevertheless, the Court maintained that the relatively broad statutory definition of a public record under the CPRA did not support the lower court of appeals' conclusion that communications from private devices were exempt from CPRA disclosure. Instead it analyzed the following statutory predicates for CPRA coverage and

reached the opposite conclusion. The four aspects of a public include the following: It is (1) a writing, (2) with content relating to the conduct of the public's business, which is (3) prepared by, or (4) owned, used, or retained by any state or local agency.

As to the first element, the Court reached the already commonly understood conclusion that emails, text messages, and other electronic platforms are writings under the CPRA. The second element raised more difficult issues because, as the Court noted, The overall structure of the CPRA, with its many exemptions, makes clear that not everything written by a public employee is subject to review and disclosure. After reciting examples of writings that would likely not be a public record, such as an email to a spouse complaining 'my coworker is an idiot,' the Court clarified that to qualify as a public record under the CPRA a writing must relate in some substantive way to the conduct of the public's business. Though this standard is broad, it is not so elastic as to include every piece of information the public may find interesting. Communications that are primarily personal, containing no more than incidental mentions of agency business, generally will not constitute public records.

Defendant City of San Jose's primary statutorily-based challenge to the extension of the CPRA to communications on private devices, and thus another focus of the Court's opinion, were on third and fourth elements of CPRA coverage requiring that the writing be prepared, owned, used, or retained by any state or local agency. The Court focused on the disjunctive term or, and noted that In focusing its attention on the 'owned, used, or retained by,' aspect of the 'public records' definition, the analysis ignores the 'prepared by' aspect. Instead, the Court concluded that because agencies operate through their officers and employees who will have prepared the records that relate to the conduct of public business, they are subject to CPRA disclosure if they are in the agency's actual or *constructive* possession. Documents otherwise meeting CPRA's definition of 'public records' do not lose this status because they are located in an employee's personal account. The statute's clear purpose is to prevent an agency from evading its disclosure duty by transferring custody of a record to a private holder and then arguing the record falls outside CPRA because it is no longer in the agency's possession. A document's status as public or confidential does not turn on the arbitrary circumstance of where the document is located; specifically, the Court stated a city employee's communications related to the conduct of public business do not cease to be public records just because they were sent or received using a personal account.

Thus, the Court refused to adopt a categorical exclusion of documents from CPRA's definition of public records merely because they exist on personal accounts. 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. Acknowledging individual privacy concerns, the Court noted that they should be addressed on a case-by-case basis, and described certain existing statutory exemptions of certain types of preliminary drafts, notes and memoranda (§6254, subd. (a)), personal financial data (§6254, subd. (n), personnel and medical files (§6254, subd. (c)), and material protected by evidentiary privileges (§6254, subd. (k)). Finally, the Court commented that CPRA already includes a catchall exemption that allows withholding records if the public interest in withholding clearly outweighs the public interest in disclosure, permitting a balance between the public's interest in disclosure and the individual's privacy interest. [Citation omitted.]

Due to the potential complexity and time-sensitivity in responding to CPRA requests, public agencies should note the Court's practical guidance on how to conduct searches of writings on private devices while balancing individual privacy. When responding to a CPRA request, the agency's first step should be to

communicate the request to the employees in question. The agency may then reasonably rely on these employees to search *their own* personal files, accounts, and devices for responsive materials. The Court also provided that agencies may also adopt policies that will reduce the likelihood of public records being held in employees' private account, such as requiring all employees to use or copy their government accounts for all communications touching on public business. The Court further noted that federal courts applying the Freedom of Information Act (FOIA) have approved of individual employees conducting their own searches and segregating public records from personal records, so long as the employees have been properly trained in how to distinguish between the two. The Court endorsed the Washington Supreme Court's recent adoption of this procedure under its state public records law, holding that employees who withhold personal records from their employer 'must submit an affidavit with facts sufficient to show the information is not a 'public record' under the PRA. So long as the affidavits give the requester and the trial court a sufficient factual basis to determine that withheld material is indeed nonresponsive, the agency has performed an adequate search under the PRA.' [Citation omitted.]

Ultimately, the Court does not hold that any particular search method is required or necessarily adequate. We mention these alternatives to offer guidance on remand and to explain why privacy concerns do not require categorical exclusion of documents from personal account from CPRA's 'public records' definition. And, now, the matter returns to public agencies of California and their public officers and employees with the admonition that use of private devices for the conduct of public business now carries far more potential burdens than previously understood by many. Those seeking to avoid that burden may be well served to eliminate the use of private devices for communications pertaining to work in the future, except perhaps to the extent that such communications are to or from, or always copied to, accounts on their agency's server.