California Supreme Court Ruling on Public Agency Disclosure of Private Communications

What Cities Need to Know

Background

In a survey by The Associated Press, multiple top elected officials in California acknowledged using personal email accounts to conduct government business. Usage of private email accounts by public officials has faced scrutiny in recent years, with accusations that some have used them as a way to avoid public disclosure. At the federal level, an appellate court ruled last year that work-related emails from a private account used by the White House's top science adviser were subject to disclosure under federal open records laws. This issue was highlighted for California on March 2nd, when the California Supreme Court issued its ruling in the case of *City of San Jose et al. v. The Superior Court of Santa Clara County*.

In 2009 a man named Ted Smith requested voicemails, emails, and texts that were sent or received on private devices used by San Jose's mayor and City Council, in relation to a land development agreement in downtown San Jose. The City of San Jose did not disclose the documents Smith requested, claiming that the City only had access to documents kept on public servers. Smith took the City to court, claiming that it was irrelevant that the documents weren't originally on the public server—because public officials do the work of the public agency, Smith claimed, it is their responsibility to turn documents over to the public agency. A Superior Court judge ruled in Smith's favor, a decision the City appealed and which was successfully overturned by the appellate court. The case then made its way to the California Supreme Court, which on March 2nd came back with a unanimous decision in favor of Smith. In their ruling the court wrote,

> "Here, we 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 (CPRA or Act). We overturn the contrary judgment of the Court of Appeal."

Court's Reasoning

When determining which communications on private devices are subject to disclosure under the California Public Records Act (CPRA), a 4-part test is used: "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". The court addressed each of the four parts as they related to communication about public business on private devices. Writing (1) refers to any kind of communication on electronic devices. The court acknowledged that content (2) will exist on a continuum from purely personal to purely business, but provided the guideline that the writing must relate "in some substantive way to the conduct of the public's business". When it came to the idea of preparation (3), the court invoked the notion of agency—that officials and employees act for and on behalf (as agents) of the public entity. Therefore, electronic communications prepared by public agency officials and employees are "prepared" by the agency as that term is used in the Act. And finally, the court held that a public record does not lose its status as such because it is located in an employee's personal account. A writing has been retained (4) by the agency even if the writing is located in the employee's personal account.

The final component of the court's reasoning is significant, because it establishes that the location of a document ***has no significance in determining if it is public record***. The court essentially fashioned a 'moment of creation' test: once something is written, it is either public record or it is not. Under this ruling, where the document resides after being created has no relevance, nor does the specific program or device it is created on. As a result, communications on social media and messaging applications are subject to the same disclosure guidelines as communications on more conventional mediums such as email or text.

Only communications that are primarily personal with ***no more than incidental mention*** of public business can be considered exempt from the definition of "public record" put forth by the court. When private communications contain a mix of both public business and personal information, the personal information is redacted in the disclosed version to protect employee privacy. Additionally, this new ruling could be seen as applying retroactively to CPRA requests; therefore, relevant records that still exist on public employee's private accounts may be considered accessible under the new CPRA guidelines. Public agencies would be wise to immediately round up any such communications and place them on a public server, and to remind employees that by Government Code §6200 it is a felony offense to intentionally destroy a known public record.

Implications

The court stated that public agencies have an obligation to make "***reasonable efforts***" to search for and obtain all records which are relevant to the subject of the request. The court made it clear that public agencies should not attempt to carry out intrusive searches of employee's private accounts in their efforts to obtain records. Such efforts must only be "reasonably calculated to locate responsive documents". Upon receiving a request, a public agency's first step should always be to communicate that request to the employees in question. The agency may then reasonably rely on these employees to search their own accounts/devices for relevant material. The success of this hinges upon employees having been properly trained to identify such material.

Citing a practice under the Freedom of Information Act (FOIA) and Washington State law, the court proposed that affidavits could be provided to employees if, after searching their private accounts, no relevant documents were found. A similar affidavit could also be used to disclose if an employee located contested documents and chose to withhold them. Such affidavits could be given directly to the records requestor or be used in future court proceedings.

Challenges

There remain multiple challenges and unanswered questions facing local cities and counties with respect to electronic communications. The court did not clarify whether a request for public records held in employees' private accounts must specify the specific source or name of the employee from whom the records are sought in order to trigger the agency's obligation to communicate the request to its employees. While an argument can be made that yes, the source must be specified, agencies may choose to err on the side of caution.

Large agencies may be faced with challenges maintaining timely compliance with a records request. Requiring an agency with hundreds of employees to obtain full compliance within ten days would place far too large a burden on the agency. There is language in the court's decision that allows an agency to go back to a requestor and obtain further specificity/clarification, which could help to narrow search parameters. Nonetheless, large public agencies may find themselves confronted with this challenge in the future, and the court's ruling does not fully address it.

If an employee or official refuses to comply with a request, they may be judicially compelled to do so. The *Tracy Press* decision held that a requestor who seeks judicial compulsion for disclosure must name the individuals, as Smith did in the *City of San Jose* case. The CPRA is enforceable against individuals[1], so an argument that 'the agency doesn't have it' cannot be used as a defense in the case of employee refusal to comply. This is further complicated by the fact that if the plaintiff prevails in such a case, the agency is responsible for the attorney fees, not the specific public official.

Policy

In order to avoid and mitigate potential challenges, public agencies should not wait to implement certain policies. Examples of possible internal policy changes include:

- Setting standards for communications on private devices that reduce the likelihood of records being held on private devices, and explicitly prohibiting employees from using private accounts for public business.
- Training employees to what is and is not considered a "public record"[2]

[1] §6258 [judicial enforcement of rights]; §6259 [OSC; in camera inspection (see, County of Los Angeles v. Superior Court (Axelrad) (2000) 82 Cal. App. 4th .819)

[2] Such training reduces the likelihood of public business occurring on private devices and educates employees in case they are ever called upon to make the determination.

- Require all agency related communications on private devices be CC'ed to the agency server.
- Have officials and employee sign an agreement that their devices are subject to agency review and disclosure, and/or advise them that refusal to disclose relevant documents and communications will result in advice to the requestor to seek judicial enforcement.

Conclusion

The court provided only general guidance in its decision, which poses a challenge for cities and counties forced to balance employees' privacy against the public's right to agency information. The court opinion states that a "reasonable effort" to search records must be made, but allows agencies to decide exactly how such an effort is undertaken. Going forward, public agencies will need to craft their own policies to determine how public records are collected from private accounts.

In terms of policy formation, a public agency must be able to defend its process in making inquiries and obtaining records from employees. The goal ultimately must be to design policy that will ensure compliance with CPRA while also protecting the privacy interests of public employees and officials.