Private Emails Are Not So Private for Government Employees

Description

For the purpose of providing guidance to Law Enforcement our firm is dedicated to spotting emerging trends and staying abreast of developing law as advances in the technological world merge with law enforcement practices. Back in 2012, we first started discussing the effect and influence of emerging technology, and the difficulties surrounding the use, search, and seizure of cell phones in the law enforcement field, as well as the ramifications of employee use of personal cell phones while on duty.

During our continued review of this emerging area, we discovered that two recent cases have come out of California, which have addressed the issue of government employees using private Email accounts during the course of performing their official duties. One case has resulted in a ruling from the court. The other ended in settlement. Both provide guidance on the issue.

Smith v. City of San Jose

A superior court judge in California recently ruled that Californiaâ??s Public Records Act (the â??PRAâ?•) applies to government officialsâ?? e-mails and text messages about government business, even if those messages are sent or received using the officialsâ?? private Email or text accounts, rather than through accounts belonging to the government.

Ted Smith made a written request under the PRA for a list of communications, which had been created and/or received by the City of San Jose, the cityâ??s Redevelopment Agency, or any city officials, including the mayor and city council members concerning property issues relating to downtown development. Mr. Smith also sought â??all electronic information relating to public business,â?• which the mayor and 2 council members had sent or received using their personal electronic devices. In response, the cityâ??s attorney stated that he would not produce any communications created or kept by the mayor or the council members on any type of personal devices, as the city considered all e-mails and text messages stored outside of city computer servers not to qualify as â??public recordsâ?• under the PRA.

The court, however, did not accept this argument. It explained that it was unlikely that the California Legislature had intended to make documents confidential based on their location rather than their content. (That is, a document is entitled to protection as confidential if it is not stored on the cityâ??s server, but is subject to disclosure as a public record if it is.) Further, the court rejected the cityâ??s argument that it cannot be legally responsible for messages, which are stored in computer servers, the city does not own, lease, or control. The court reasoned that government officials, when they send e-mails or text messages about government business, are acting as agents of the city. Therefore, their ownership and control of the messages is imputed to the city.

This decision is consistent with the 2012 settlement reached in a lawsuit between the First Amendment Coalition and the City of Auburn (California). There, the defendant city agreed to adopt policies, which required city officials, when e-mailing about city business using their personal Email accounts, to â??cc:â?• the e-mails to a city Email server, where the e-mails would be stored to a searchable archive,

available to the public.

First Amendment Coalition v. City of Auburn

Last summer, a settlement was reached in a case involving public access to government Email messages. The agreement required the City of Auburn to save e-mails for at least 2 years, replacing the prior policy of deleting most e-mails after 30 days. The agreement also assured public access to e-mails concerning government business, even when government officials send or receive such e-mails using private Email accounts.

According to counsel for the plaintiffs, First Amendment Coalition (â??FACâ?•) and Victoria Connolly, â??This settlement sets a new benchmark for transparency in government communications. While not perfect, the procedures agreed to by Auburn will show cities, school boards and other agencies how they can increase citizensâ?? access to information without adding to operating costs.â?• Pursuant to the settlement agreement, the City of Auburn agreed to stop its practice of deleting most city e-mails. At the time of settlement, the city saved only a handful of e-mails selected by employees, while deleting all others after 30 days.

Other California agencies have used similar policies, though some wait longer â?? 60 or 90 days â?? before deleting e-mails. Pursuant to the agreement, Auburn agreed to adopt preservation policies, which provide â??that all Email sent or received by the cityâ??s Email server will be preserved for two years and made available for public inspection on the same terms as other city records.â?• â??As most government records became digital, public officials all over the state have fallen in love with their computerâ??s â??deleteâ?? key,â?• said Peter Scheer, executive director of FAC. â??This agreement establishes the principle that government e-mails about government business are public records and have to be treated as such â?? meaning they all have to be retained and made available for inspection and copying.â?• The city also agreed to change its practices regarding its officialsâ?? use of their own private Email accounts for communications concerning city business.

Under the terms of the settlement agreement, employees must forward or copy e-mails, which concern city business, from private Email accounts to an address on the cityâ??s Email server, from which copies can be made available to citizens in response to public record requests. This new policy for private accounts will have an exception for Email communications with constituents (defined as residents, business owners, and property owners) sent to or from City Council members, the city clerk, and city treasurer. For privacy reasons, these e-mails will not have to be saved or copied to the city server. For the first time, however, the public will have access to emails, which have been sent, using private Email accounts, between and among City Council members and between Council members and city staff. â??Government officials in recent years have come to view private email accounts as a way to completely bypass open records laws, not just in Auburn, but across the stateâ?• said co-plaintiff Connolly. â??Auburn, in this settlement, is agreeing to close substantially this huge loophole in the handling of public records.â?• The two Email issues, which the settlement agreement addresses â?? retention of e-mails and the use by government officials of private Email accounts â?? have been flash points for open-government advocates and government lawyers in cities and agencies across the state. No California appellate court, however, has addressed either issue on the merits.

While a settlement does not create a legally-binding precedent for other cities, FAC plans to use the agreement with Auburn as a model, which other governments and agencies could adopt. â??Other cities and counties, if they are serious about providing transparency in government, will follow

Auburnâ??s example,â?• said Scheer. â??It costs them nothing, while simplifying the management of emails and improving compliance with open-record laws.â?•

Conclusion

While the above cases pertain to Californiaâ??s â??Public Record Act,â?• its act is not unlike other Freedom of Information Acts adopted in states across the country. It is likely that, when faced with this issue, courts from other jurisdictions will follow suit and find that emails and text messages sent from personal devices are not shielded from disclosure. To avoid such conflicts in the future, Departments should institute policy which prohibits the use of personal devices, personal email accounts, or other social media to conduct Department-related business. If the department does not provide an email account the officers should open an account with the knowledge that the communication may be ordered to be disclosed. Command staff and officers should be aware that rulings such as the one above would likely extend to any type of communication that in any way is related to law enforcement activities, e.g., communications with dispatch during on-duty hours, or email or text communications between officers discussing arrests, suspects, or specific cases. The confusion on the issue actual leads us to consider a per se ban on all personal devices, social media, and accounts while officers are on duty to avoid any cross contamination between department and personal devices and media. Officers must understand that if they choose to utilize their personal devices or accounts during on-duty hours, a court may very well require them to hand over such devices for inspection.

Date Created
09/15/2013