Colorado Freedom of Information Coalition

July 2014
www.coloradofoic.org
@CoFOIC on Twitter

New Technologies Pose New Challenges: As the Volume of Public Records Increases, Access Diminishes

By Steven D. Zansberg

President, Colorado Freedom of Information Coalition

Increasingly, government agencies conduct the vast bulk of public business via digital and cloud-based platforms. Whether it is email, SMS messaging, Facebook or Snapchat, more and more public data and information is generated daily than at any previous period when pen, paper and typewriter were the primary means of written communications. With the rise and use of these technologies come new challenges to obtaining access to public records.

This CFOIC white paper examines three recurring questions: (1) Are emails and texts discussing public business, exchanged or housed on "private" email accounts or devices, subject to disclosure under the Colorado Open Records Act (CORA)? (2) If such messages are stored only on third-party servers, e.g., Gmail, are they "public records" *of* the government? (3) What obligations do government offices have to retain copies of emails and other electronically stored public information?

"Private" Emails/Text Messaging Accounts and Devices

More and more government entities across the state are allowing and even encouraging public employees, including high-ranking officials, to use handheld devices that are not paid for by the government and email and text-messaging accounts that are not maintained on government servers (*e.g.*, Gmail, Yahoo!). This raises the question of whether the use of such "private" communications devices and document repositories somehow removes such communications from being subject to the CORA, even when the content of the communications unquestionably addresses public business.

Existing Colorado Law

While this issue might strike some as novel or intriguing, in fact, under existing law, there is no ambiguity: Records made, maintained or kept by a government employee whose content bears a demonstrable connection to the conduct of public business are "public records" that are subject to the CORA. The law defines "public records" as any record "made, maintained, or kept" by any governmental employee or agency "for use in the exercise of functions required or authorized by law or administrative rule or involving the receipt or expenditure of public funds." The statute also defines "writings" that are subject to inspection under the CORA as any "documentary materials regardless of physical form of characteristics," and expressly includes "electronic mail." Thus, under the plain text of the statute, the actual physical location of a "writing" is immaterial to the question of whether a writing "made, maintained, or kept" by a governmental employee, whose content discusses public business, is a public record. The same definition would apply if a governor, mayor or police chief used personal stationery to communicate official directives to other government employees and stored them in a personal filing cabinet at home.

Colorado's appellate courts have decided two cases which demonstrate the converse of the above, by demarcating which records are *not* public records: Both cases turned entirely upon the *content* of the communication that was generated, sent or received by a governmental employee, not on the physical location where the record resided. In the first of these cases, *Wick Communications Company v. Montrose County Board of County Commissioners*, 81 P.3d 360 (Colo. 2003), the court determined that a county airport manager's personal diary, in which he made fleeting reference to his official duties, and which he maintained entirely for his own use and not for any other governmental employee, was not a public record under the CORA. In the second case, *Denver Publishing Company v. Board of County Commissioners of County of Arapahoe*, 121 P.3d 190 (Colo. 2005), the Colorado Supreme Court found that sexually explicit emails exchanged between the former clerk and recorder of Arapahoe County and his chief deputy were not public records even though they were sent using government-funded communications devices and housed on a government server. The court made clear that any portions of those text messages that discussed governmental business *were* public records and were required to be provided in response to a records request, with the sexually explicit, non-governmental portions redacted.

In this second case, the court interpreted and applied the provision added to the CORA in 1996 expressly to address emails and other electronic communications. In that set of amendments, the legislature made clear that "the acceptance by a public official or employee of compensation for services rendered or the use by such official or employee of publicly owned equipment or supplies shall not be construed to convert a writing that is not otherwise a 'public record' into a public record." In other words, merely because emails and text messages are transmitted or received over a government-funded communications system does not render the writing a public record; the determination is made based on the *content* of the communication – whether it bears a demonstrable connection to the conduct of public business. But just as the *presence* of public funding for the communications device does not determine the public-record status of the email or text message, neither does the *absence* of such public funding for the stationery, envelope, Gmail account or iPhone. After all, if lack of government funding and government agency access were itself sufficient to strip a record of its status as a "public record," the court in the *Wick Communications* case would not have needed to examine the *content* of the airport manager's diary; it was undisputed that no other government employee or agency had access to the airport manager's diary that he kept in his own private notebook.

Lastly, although it does not apply to any other state or local agencies, Colorado's General Assembly has adopted a policy which states that an email discussing public business is considered a public record, "regardless of whether the email was sent or received on a public or privately owned personal computer or whether a member or legislative staff utilized the state or a private service provider paid for at member or staff expense to send or receive the email."

Other Jurisdictions

Court decisions in eight other states (Alaska, Arizona, Arkansas, New York, Ohio, Pennsylvania, Virginia and Washington) have held that if the content of an email or text message sent or received by a government employee relates to the conduct of governmental business, it is subject to that state's open records act and the actual physical location of such a writing is immaterial. The California Supreme Court recently decided to hear a case in which it will resolve whether email messages maintained on a mayor's personal email account in which public business is discussed are subject to California's Public Records Act.

In addition to the above judicial opinions, attorneys general in 10 states (Alaska, Florida, Illinois, Maryland, New Mexico, North Dakota, Oklahoma, Oregon, Texas and Wisconsin) each have issued formal opinions stating that email messages created, sent or received by government officials discussing public business are public records, regardless of the physical location or records repository where such email messages reside. *See, e.g.*, 81 Md. Op. Att'y 140 (1996) ("Email messages among members of the Commission pertaining to Commission business would be public records, albeit housed only in the home computers of the members.")

Records in the Custody of Third-Party Vendors/Providers

But what happens if emails or other electronic/digital communications are *not* in the actual custody either of a government agency or the public employee who authored, sent or received such communications? After all, very few government officials maintain their own data servers on which they personally store emails or other digitized records. More and more government agencies (not merely individual employees) are contracting with third-party vendors, such as Google's Gmail, to host all official business communications. Are such writings, maintained "in the cloud" at the behest of a government agency, "public records" of that agency? Under existing law that predated the World Wide Web, they are.

In a Colorado Court of Appeals decision, the Denver Metropolitan Stadium District, the governmental entity established to oversee the funding and construction of Coors Field, was deemed to be the custodian of electrical subcontracting bids that were maintained outside of any stadium district office, in the exclusive custody of the private general contractor for Coors Field. The court ruled that, despite these facts, the bid proposals were the stadium district's public records because district employees had reviewed those records at some point previously, and the district had a legal right to obtain those records from the general contractor who maintained custody of them at the behest of the district. Under these facts, it is clear that when a government entity contracts with Google, Yahoo! or any third-party provider to maintain records (the same would be true for any third-party storage facility of paper files) from whom the government has a contractual right to retrieve those records, they constitute the "public records" of that agency. This would be true, as well, for old emails that are maintained in an archive or cache by a private vendor at the behest of a government agency. (*But see*

http://completecolorado.com/pagetwo/2014/06/18/state-agencies-stonewall-stall-on-deleted-emails-of-key-bureaucrat/.)

Duty to Retain E-Records: For How Long?

With respect to paper records, the CORA provides a right of access only to those records that exist at the time of the request; the government is not required to make a new record in response to a records request, nor to provide access to a record that it no longer has access to (because it no longer exists). Thus, the question becomes for how long must the government maintain copies of electronic records in which public business is discussed? The answer to that question turns on a separate set of laws and policies extraneous to the CORA. The CORA itself imposes no specified records retention schedule.

With respect to state agencies, Colorado law requires that each agency "establish and maintain a records management program … and document the policies and procedures of such programs." All such state agency programs must comply with the records maintenance manuals promulgated by the chief administrative officer over State Archives and Public Records. Municipalities and counties are not required to adopt or abide by the State Archives' records retention manuals. Nevertheless, many local governments either have adopted those schedules or their own records retention schedules. The overarching policy of all such schedules should be as articulated in the section of the State Archives' retention schedule for municipalities that addresses electronic records in general. It says that when such records (as opposed to copies) are retained for recordkeeping purposes, "electronic records have [the] same retention periods as paper or microfilm records with the same content." There remains some ambiguity in how these various records schedules are to apply to emails, in many instances vesting considerable discretion in the government employee who sends or receives them to determine how long they should be retained.

In short, the records retention schedule for electronic or digital records should turn on the *content* of the record, not its format or title.

Steven D. Zansberg, president of the Colorado Freedom of Information Coalition, is a First Amendment and media-law attorney with Levine Sullivan Koch & Schulz in Denver.