TIPJar

TRENDING LEGAL DEVELOPMENTS IN THE WORLD OF TECHNOLOGY

SUMMER 2017

Public Records.

In this Issue:

The Aftermath of *City of San Jose*
Private Emails and Public Records
Metadata: Insight from an Industry Expert
Litigation Holds
Paper Laws, Electronic Records
Curbing Troublesome Texts

LS Lozano Smith
ATTORNEYS AT LAW

Published by Lozano Smith's Technology and Innovation Practice Group

Editor's Note:

The Aftermath of *City of San Jose*

BY PENELOPE R. GLOVER

When WikiLeaks published more than 20,000 leaked Democratic National Committee emails in the heat of the 2016 presidential election, political journalist Olivia Nuzzi famously tweeted that one should "Dance like no one is watching; email like it may one day be read aloud in a deposition."

Nuzzi's adage has long been true for public agency officials and employees, whose work communications are generally a matter of public record. But the California Supreme Court's recent decision in *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608 confirmed the application of the California Public Records Act to communications made from or stored on personal devices and in personal accounts, foisting an untested set of responsibilities onto public agencies and the people who serve them.

Now, there is no doubt that individual public agency employees are responsible for retaining agency-related emails and texts sent to or from their personal devices and accounts. They are also responsible for searching or consenting to a search of their devices and accounts for responsive records requested under the Public Records Act. With the law's affirmation of these responsibilities, it is now more important than ever that public agencies recognize the obligations they have to educate their officials and employees on their policies and procedures in order to better meet their evolving legal obligations.

In this issue of the TIP Jar, we explain *City of San Jose*'s big takeaways, guide public agencies through California's aging records retention laws, and talk tech tools for retaining communications between folks like teachers and students. We also provide real-world, expert guidance on spotting metadata—data about your data—and discuss a related records retention topic, litigation holds.

If you'd like more information on the *City of San Jose* decision or any other technology-related legal issue you're facing, feel free to get in touch with an attorney in our Technology & Innovation Practice Group at one of our eight offices located statewide. And if you've got questions or suggestions for the TIP Jar, feel free to get in touch. ■

Penelope R. Glover is Senior Counsel in Lozano Smith's Walnut Creek office and chair of the firm's Technology & Innovation Practice Group.

Now What?

PRIVATE EMAILS DISCUSSING PUBLIC BUSINESS ARE PUBLIC RECORDS.

BY
HAROLD M.
FREIMAN

As public agency officials and employees have increasingly turned to text messages and email to facilitate communication anytime and anywhere, they lost touch with a basic truth: Electronic communications are writings. As such, they may fall within the reach of the California Public Records Act (CPRA). Now that the California Supreme Court has opened the door to disclosure of public agency-related communications made or stored on private devices and in private accounts, California's local agencies will need to develop policies and procedures to address these practices.

In *City of San Jose v. Superior Court*, the California Supreme Court held that the CPRA grants the public a right to access texts, emails and other records relating to the business of public agencies even if they were created, received by or stored in a private device or account. "If public officials could evade the law simply by clicking into a different email account, or communicating through a personal device," the Court wrote, "sensitive information could routinely evade public scrutiny."

This case had its origins in a 2009 lawsuit against the City of San Jose, its redevelopment agency and several city officials. The plaintiff claimed that the city's failure to provide voicemails, emails and text messages that were sent and received by city officials on personal devices using personal accounts violated the CPRA. The Supreme Court's March 2, 2017 ruling finally (and for the first time in California) put the issue of whether such communications can constitute a public record to rest: An email or text sent to or from a private device or account can indeed be a public record.

While providing certainty on this issue, however, the case also raises many new questions. Public officials will need to tighten their seat belts: The road ahead is likely to be bumpy.

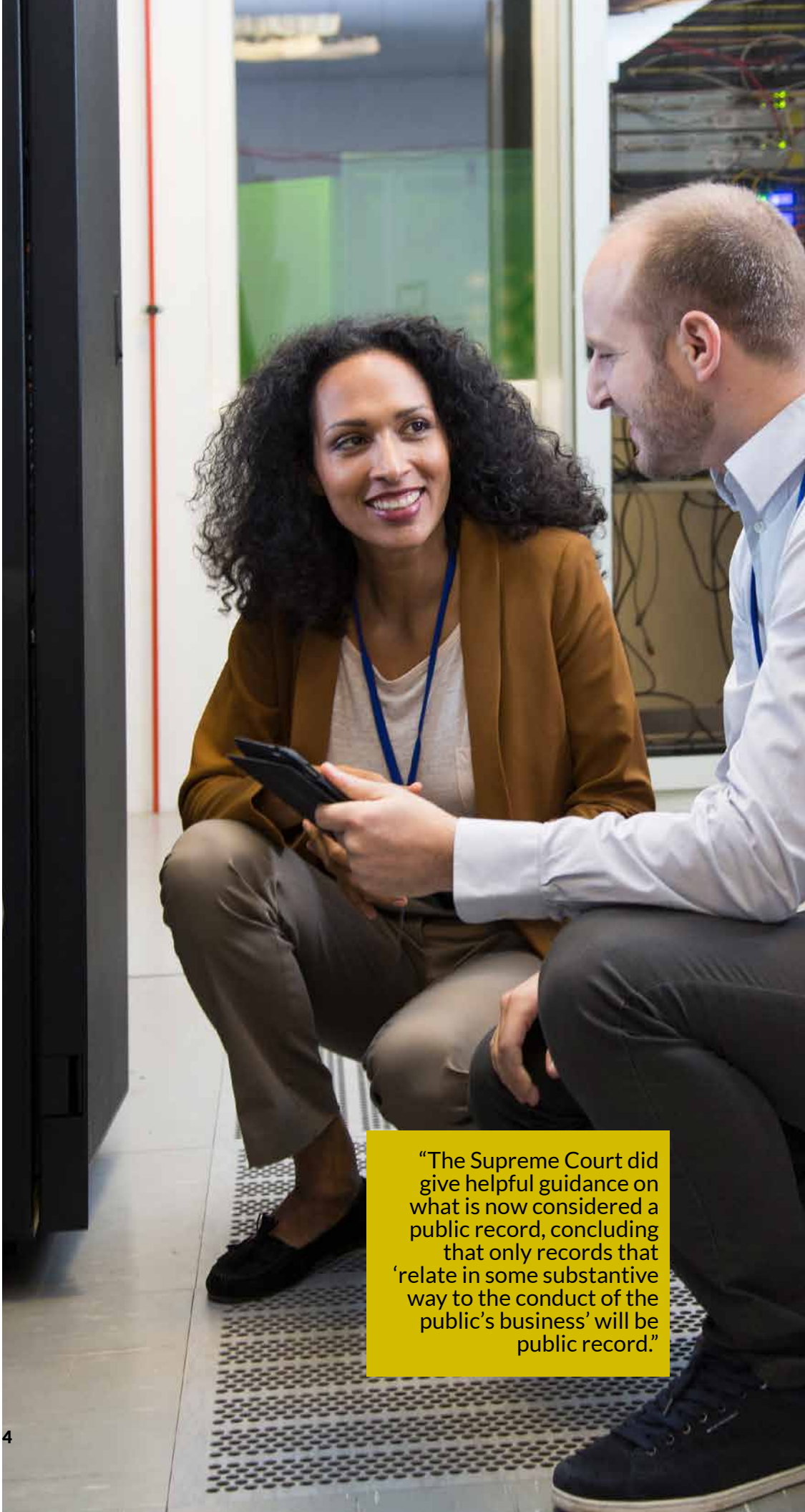
The Supreme Court did give helpful guidance on what is now considered a public record, concluding that only records that "relate in some *substantive* way to the conduct of the public's business" will be public record. The Court narrowed the scope of records subject to disclosure, specifying that communications that are primarily personal, containing only incidental mentions of agency business, generally will not be considered public records. The Court thus pulled back from prior cases holding that the mere mention of public business in a communication could make that communication subject to the CPRA.

The Court also recognized the practical challenges of retrieving records from personal accounts while respecting the privacy of account holders and their correspondents. Although the Court did not establish a specific process, it did point to procedures adopted by federal courts applying the Freedom of Information Act and by the Washington Supreme Court that applied that state's public records law. The Court favorably noted that individuals can be allowed to search their own devices and accounts for responsive records when a request is received, and to submit an affidavit regarding potentially

responsive documents that the individual withheld. To have such a practice, the Court noted that training the individuals who are undertaking such searches is appropriate. The Court also discussed the adoption of policies that would prohibit the use of personal accounts for public business, unless messages are copied and forwarded to an official government account. While these methods were offered as examples, the Court did not endorse any specific approach, leaving it to each public agency to develop its own practices.

While the Court gave some clues as to how public agencies can attempt to comply with its ruling, it left open a host of other issues. Public agencies will have to determine how to address evolving technologies, including apps that do not preserve messages; how to deal with public officials and employees who refuse to produce records from their personal accounts; and how to distinguish gossip from the substantive conduct of public business.

The ruling may also create collective bargaining issues. For instance, if an agency wishes to compel its employees to make their personal accounts



"The Supreme Court did give helpful guidance on what is now considered a public record, concluding that only records that 'relate in some substantive way to the conduct of the public's business' will be public record."

available or prohibit employees from using personal devices or accounts to conduct agency business, negotiation with bargaining units could be required.

In addition to queries for advice on implementing new procedures in light of *City of San Jose*, we have received three repeated questions:

1. *Does the ruling apply retroactively?* Yes. Nothing in the case limits its holding to how documents are created and retained after the ruling, meaning that a CPRA request for electronic records can reach back to an indefinite time period.

2. *What types of communications are governed by the ruling?* Again, there is no limit to the breadth of the holding. It applies to all forms of electronic communication relating to public business. In fact, there is nothing that limits the decision to electronic communications: It would appear that personal correspondence in letters, longhand written notes, and other forms of writing may now be subject to the CPRA if they discuss agency business, even if they are possessed and maintained only by individual officials outside of the agency's offices.

3. The third question has been the most frequent one, reflecting a state of disbelief: *Does this decision really mean that an individual's private email accounts could be opened to disclosure under the CPRA?* The answer is yes.

Moving forward, *City of San Jose* supports the notion that local agencies should be developing and adopting policies and practices to address the disclosability of electronic communications and the use of personal accounts for public business. Records retention policies will also be relevant, as agencies will need to consider how email records, now including those on personal accounts, will be retained by the agency or its public officials.

Developing such policies is not a job for lawyers alone. Various stakeholders should be involved in determining what process the agency will use to address communications on personal accounts, potentially including IT staff, elected officials, legal counsel, student service staff in school districts, city managers and superintendents, business officials, and possibly employee union representatives. Once policies are developed, training will be critical for bringing local agency officials and employees up to speed on the policies that were adopted and the procedures that will be followed when CPRA requests are received.

Lozano Smith was the first law firm in California to develop and broadly distribute email retention policies for use in school districts. We have now developed model school district policy language to address the *City of San Jose* decision. The most recent version of this model policy language is available by contacting the author of this article or **clientservices@lozanosmith.com**. We are available to assist all types of local agencies with developing their own policies and best practices, including development of agency-specific affidavits for public officials and employees who may possess agency-related business communications in their personal accounts.

It is a brave new world for public officials. Until policies can be developed and put in place to address how a public agency will implement *City of San Jose*, public officials may wish to limit the use of their personal devices and accounts for substantive communications regarding their agency. In the meantime, remember the old adage: Don't put it in writing unless you want it on the front page of the newspaper! ■

Harold M. Freiman is a Partner in Lozano Smith's Walnut Creek office.

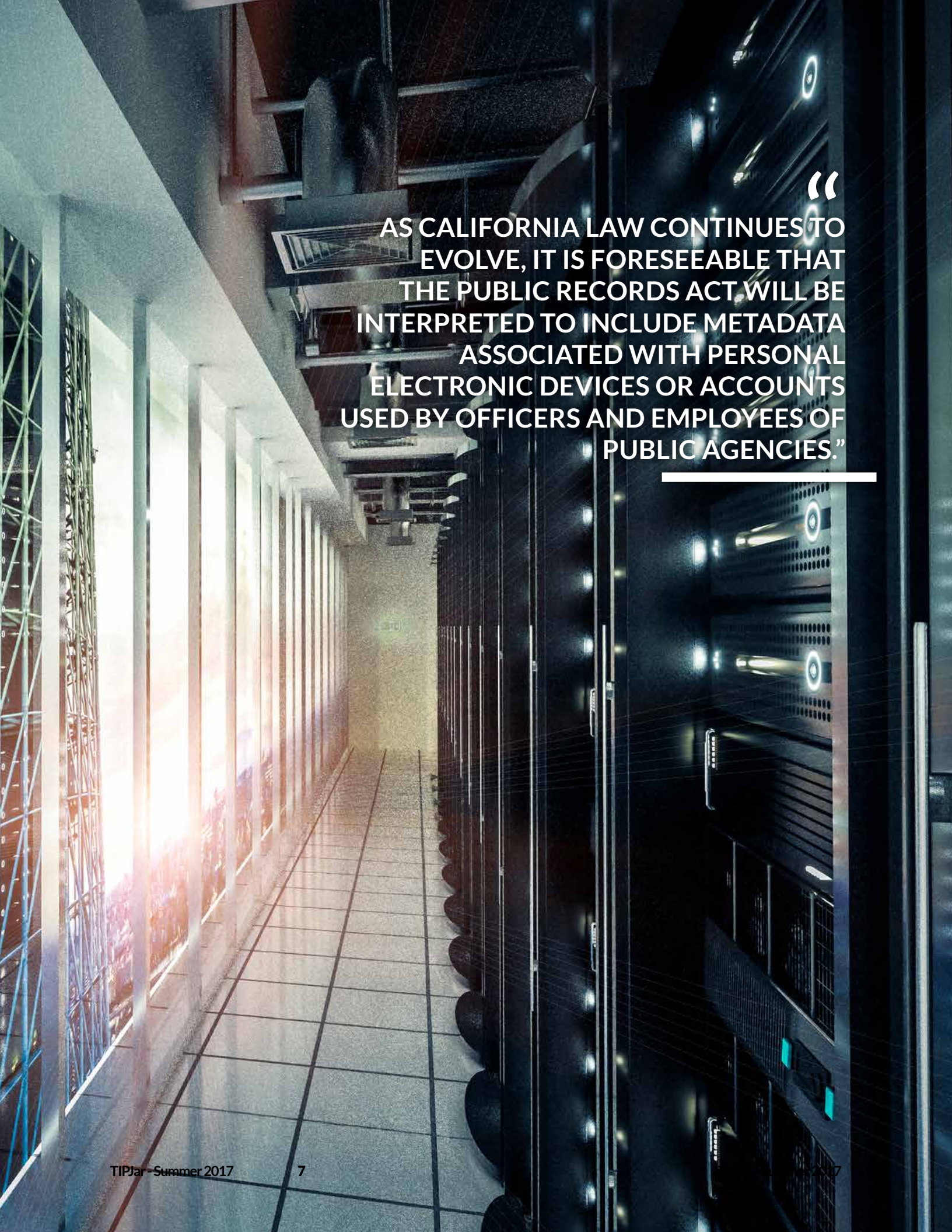
Metadata

Insight from an Industry Expert

BY
DARREN C. KAMEYA,
PENELOPE R. GLOVER
AND
JULIE LEWIS

In our technology-driven world, a California Public Records Act request typically seeks some form of electronic communication or record created using a computer and software program. Frequently, an agency's response is to send an email attaching the requested record if it is not otherwise exempt from disclosure. Public agencies must be careful when responding to these requests. Without taking adequate precautions, this common response may actually reveal hidden electronic data, called "metadata." In some instances, a requester of records may specifically ask for metadata. If a request for metadata involves an employee's personal account or device, this could implicate an employee's privacy rights. Best practices may warrant that the public agency take an active role in searching for the information or guiding the employee to search his or her personal electronic device or account.

In *City of San Jose v. Superior Court*, the California Supreme Court looked in part to the Washington Supreme Court for guidance on how a public agency could establish the adequacy of a search for public records on an employee's personal device or account. The Court offered as an example the Washington Supreme Court's approach, which relies on employee affidavits to verify that the employee searched his or her personal devices and accounts and to explain why any records were not produced. The California Supreme Court held that this struck an appropriate balance between a public agency's "responsibility to search for and disclose public records without unnecessarily treading on the constitutional rights of its employees."



> “AS CALIFORNIA LAW CONTINUES TO EVOLVE, IT IS FORESEEABLE THAT THE PUBLIC RECORDS ACT WILL BE INTERPRETED TO INCLUDE METADATA ASSOCIATED WITH PERSONAL ELECTRONIC DEVICES OR ACCOUNTS USED BY OFFICERS AND EMPLOYEES OF PUBLIC AGENCIES.”

While not yet addressed by California law or mentioned in *City of San Jose*, Washington is also one of the few states in the nation with case law establishing that metadata is a disclosable public record. In *O'Neill v. City of Shoreline* (2010) 240 P.3d 1149, the Washington Supreme Court found that metadata associated with an email was subject to disclosure after a public records act request was made in order to determine its original sender. In that case, the city's failure to respond to the court's satisfaction proved costly. After deciding against the city, the Court ordered the city to pay over $500,000 in fees to the plaintiff.

As California law continues to evolve, it is foreseeable that the Public Records Act may be interpreted to include metadata associated with personal electronic devices or accounts used by officers and employees of public agencies. Consequently, it is in the best interest of public agencies to better understand what metadata is, how to control the creation and maintenance of metadata and how to respond to requests for it.

To explain metadata within the context of an employee or employer search of personal electronic devices or accounts, we consulted Digital Mountain, a leading global provider of electronic discovery, computer forensics, cyber security and next-generation Web-based solutions. In response to our questions, Digital Mountain's founder and CEO, Julie Lewis, provided the following information.

Q: What is metadata and what types of information does it provide?

A: Metadata is simply data about data. For email, metadata may be information such as sender, mail size, subject, sent date, sent time, received date, received time, to, cc, bcc, message ID, mail internet headers, sensitivity and importance. For files at a file system level, metadata may be such information as original file name, modified date, accessed date, created date, file size, file extension and original file path. Additional metadata may exist based on the specific application and version of the software used. For example, for Microsoft Word, there may be metadata for comments, date created, primary author, last saved by, revision number, source, last saved date, last print date, pages, words, characters (without spaces), characters (with spaces), lines, paragraphs, total editing minutes and company. If you are dealing with picture files, there is something called exchangeable image file format (EXIF) metadata which has the source camera make and model, date, time, geolocation if recorded and a lot of metadata that may be noise (irrelevant data). As you can see, with any request for metadata it's important that metadata being sought is properly defined or there can be a lot of extraneous information.

Q: Where is metadata found?

A: This is a bit of a loaded question. If metadata is embedded within a file, it can be extracted with processing. However, if you are seeking metadata at a file system level, metadata is extracted differently based on the operating system. For example, if you are seeking a creation date within a file, that would tell you when a document was created versus if you obtain the creation date at a file system level, the creation date is typically when the file was first placed on a hard drive.

For email, metadata is embedded within the email message. For security logs in the cyber security realm, the data is typically in a database. For a wearable device (like a Fitbit or smart watch), it could be on the device or stored centrally in a database in the cloud.

If you compare metadata to a human being, there may be data stored about you externally (e.g., Social Security

number, birth date, home address). There may also be metadata that is part of your system that consists of blood type, DNA, blood pressure or cholesterol level. Documents follow a very similar pattern, where there may be metadata stored externally and embedded. Rather than getting caught up with the word "metadata," it's important to preserve what you can and ensure that the requesting party defines what they are seeking when metadata is requested, as each system can vary in what metadata is maintained.

Q: Does an employer or employee need to take any steps to preserve metadata?

A: For discovery purposes in litigation, it's critical that metadata is preserved based on how documents are held in the ordinary course of business. This involves forensic preservation that ensures no data is altered along with proper chain of custody procedures and processing documentation. Many employers and employees are tempted to cut corners and do such things as forward relevant emails to their attorneys. However, this does not properly preserve the email for evidentiary purposes.

Q: If a public agency is legally obligated to produce metadata that is located in an employee's personal electronic device or account, how would it go about doing so?

A: It depends. At Digital Mountain, we have a separate form that custodians sign providing authorization to collect their digital evidence. For metadata extraction, what information is processed depends on the type of device that is subject to discovery. For desktops or laptops, a forensic preservation would need to take place, so metadata is not altered. In the processing phase, relevant metadata is extracted so it can be displayed alongside the actual document view. For devices such as smartphones, the device is forensically preserved, reports are typically parsed out from SQLite databases and then filtering is performed for relevant information. For cloud-based accounts, we obtain the user's authorization to access personal accounts prior to preserving. Metadata varies across different cloud-based applications. It's important to know what metadata is relevant and what's considered noise. Bring your own device policies have created a lot of complexity in our industry. It's always best to have written policies upfront that address how business documents or communication on personal devices or cloud accounts may be treated for investigations, Public Record Act requests, litigation or other purposes. ■

Darren C. Kameya is a Partner in Lozano Smith's Los Angeles office.

Penelope R. Glover is Senior Counsel in Lozano Smith's Walnut Creek office, and chair of the firm's Technology & Innovation Practice Group.

Julie Lewis is Founder and CEO of Digital Mountain, a leading global provider of electronic discovery, computer forensics, cyber security and next-generation Web-based solutions.

Hold On:

LITIGATION HOLDS AND ELECTRONIC RECORDS

BY MARK K. KITABAYASHI AND MICHAEL R. LINDEN

You may have experienced the following situation working for a local public agency. You open your mail and you see a document entitled "Litigation Hold." An attorney wants your employer to preserve records for discovery in a legal dispute, including emails and other electronic data. Initially, you have no idea where relevant emails and data might be kept, whether they are even being saved or what policies are in place regarding the retention of emails and other electronically stored information. How can such a situation be avoided?

A request for a litigation hold often arises before the filing of a lawsuit in order to ensure that information relevant to the case is preserved. Such requests are normally made by an attorney representing an individual who intends to sue the public agency. In other instances, public agencies receive litigation hold letters from their own legal counsel, based upon either existing or anticipated litigation.

In general, a party receiving a litigation hold has a duty to preserve evidence that it reasonably should know is relevant to litigation. The clock may start from the moment a public agency reasonably anticipates litigation, before a plaintiff ever files a lawsuit. This is especially true for public agencies, as a would-be litigant cannot file a lawsuit until after they have already presented a claim for damages administratively, and that claim has been acted upon.

While the cost of locating and storing electronic data for lawsuit discovery purposes can be high, failure to do so may be higher: Sanctions for destroying evidence can include monetary penalties, adverse jury instructions or a default judgment against your agency. Unfortunately, while courts have found certain broad requests by litigants for electronically stored information overly burdensome, public agencies generally cannot use budget issues as a defense against costly "e-discovery" requests.

The California Supreme Court's opinion in *City of San Jose v. Superior Court* added a new layer of complexity and cost for public agencies facing records requests under the California Public Records Act (CPRA): Electronic communications sent by or stored in an employee or official's personal device or account may now be subject to disclosure under the CPRA. The court's decision was not expressly prospective, so if a search was pending at the time the decision was issued, a public agency may be obligated to expand it. The decision will likely also have implications for public agencies involved in lawsuits and related litigation holds. With our ever-changing technologies, it is best that public agencies are knowledgeable about what electronic data they possess, in what form, and where and how long it is stored, so they are poised to properly respond to such requests when received.

How can public agencies adequately prepare for litigation holds? The key is proactive readiness, as opposed to a reactive response. An updated records retention policy that covers email and other electronic data is essential. Such a policy would relate to records in all management systems. For municipal agencies, certain records are subject to special retention requirements; otherwise, the general rule is that such agencies retain records for two years. School districts are subject to a different set of rules and record retention timelines, which are discussed in detail in a separate article in this issue of the TIP Jar. Therefore, it is important for a public agency to have the ability to archive and retrieve electronic communications that they are required to maintain under applicable laws, as well as delineated processes and schedules for the maintenance and destruction of records. Such a policy may also address the timeline or cycle on which emails are regularly purged, subject to any litigation hold that requires their retention. It may also address how the maintenance and destruction of such emails interact with any backup system the public agency has in place for such electronically stored information.

Public agencies should also work with their IT department staff or consultant before a lawsuit or CPRA request comes to pass to find out who has electronic data and where it is stored—especially if data is stored in private devices or accounts. If a plaintiff files a lawsuit, a public agency's IT experts can guide other public agency employees regarding the methods and costs of storage and retrieval of electronically stored information, documents, and data where preservation requirements apply.

Another proactive step is to preserve potential evidence for incidents that have generated an administrative claim. Once a claim has been presented, a public agency is on notice it may face a lawsuit so a litigation hold has already, in essence, been submitted. This is a great opportunity for the agency's risk managers to work in conjunction with counsel to gather records relevant to the claim. The claimant is required to set forth all of the facts and circumstances related to the claim, so the public agency is justified in using the claim as a guide for records retention. Under these circumstances, a public agency should identify all possible custodians of relevant records. If a public agency is not diligent about having its employees preserve agency communications made through personal accounts and devices, then the job of the custodians may prove more difficult and time consuming.

Certain types of events generate litigation so often that it may be in a public agency's best interest to preserve records before a claim is even made. For example, employee disciplinary matters are often highly contested, and may generate a large amount of email traffic that is subject to preservation if the case ultimately makes its way to court. Law enforcement actions, especially those involving the alleged use of force, often generate lawsuits. In such cases, the policies, practices, and customs of the agency are a likely issue in the case, and a litigant is apt to ask for information about the agency's involvement in similar incidents. A litigant may also request items like videos from body cameras worn by law enforcement officers. If a plaintiff claims civil rights violations under federal law, he or she is not required to present an administrative claim to the public agency before filing a lawsuit. In fact, such a plaintiff may not file suit until up to two years after the event. Therefore, public agency evidence preservation is ideally taking place much sooner.

In any situation involving potential litigation, it is important for a public agency to confer with counsel to identify the best steps to take with respect to evidence preservation, and then take those steps. If the public agency is able to produce favorable evidence prior to the initiation of formal litigation, it is quite possible that potential litigants will be convinced not to pursue litigation at all. Even if litigation is unavoidable, work on the front end will help the public agency achieve a better result. ■

Mark K. Kitabayashi is a Partner in Lozano Smith's Los Angeles office and co-chair of the firm's Litigation Practice Group.

Michael R. Linden is Senior Counsel in Lozano Smith's Fresno office.

Paper Laws, Electronic Records:

AN OVERVIEW OF RECORD RETENTION LAWS FOR CALIFORNIA SCHOOL EMPLOYEES

BY DEVON B. LINCOLN AND RYAN P. TUNG

Now that the California Supreme Court has directly addressed the universe of records accessible under the Public Records Act, it is more important than ever that school district employees and elected officials familiarize themselves with their obligations in retaining school district records to ensure that emails, texts and other electronic communications made or stored in private devices and accounts are maintained in accordance with these obligations. This article outlines California regulations governing record retention for school districts, and provides practical tips and resources for school employees when retaining and destroying records.

What is a "record"?

Regulations promulgated by the Superintendent of Public Instruction in the 1970s govern the retention and destruction of school district records in California. The regulations define a "record" for K-12 school districts as all records, maps, books, papers and documents of a school district required by law to be prepared or retained, or which are prepared or retained as necessary or convenient to the discharge of official duty. It is important to remember that these regulations have not been updated in more than 40 years, and are a poor fit for many 21st century document retention questions.

How long does a school district need to retain each record?

The contents of a particular record will determine how long a school district must maintain that record. Records must be retained or may be destroyed based on the following classifications:

• ***Class 1 – Permanent Records***: Permanent records are records deemed important enough to require permanent retention. Examples include personnel records, payroll documents and school board minutes.

• ***Class 2 – Optional Records:*** Optional records are records that the superintendent or designee determines are worthy of temporary preservation but do not require permanent retention. Optional

“THE CONTENTS OF A PARTICULAR RECORD WILL DETERMINE HOW LONG A SCHOOL DISTRICT MUST MAINTAIN THAT RECORD.”

records must be retained until they are reclassified as disposable records. Once this reclassification occurs, the school district must follow the timeline for destruction of disposable records discussed below.

• ***Class 3 – Disposable Records:*** Disposable records are those records that are not classified as permanent or optional. Disposable records cannot be destroyed until either: (1) after the third July 1 succeeding the completion of all legally required audits, or (2) after the ending date of any retention period required by any agency other than the state, whichever date is later.

• ***Continuing Records:*** All records must be classified prior to destruction. But the regulations provide restrictions on *when* a record may be classified as Class 1, Class 2 or Class 3. For example, certain records, known as "continuing records," may not be classified as permanent, optional or disposable until their "usefulness ceases." Continuing records are those records that remain active and useful for administrative, legal, fiscal or other purpose.

If records may be destroyed, what is the proper manner of destruction?

Neither the Education Code nor regulations address the procedures for the actual destruction of records belonging to a school district. However, regulations do prescribe steps for community colleges to follow, detailed below:

1. The superintendent (or designee) submits a list of documents that may be destroyed to the board, certifying that none of the documents included in the list are included in conflict with the Education Code or the regulations.

2. The superintendent (or designee) recommends that the documents in the list be destroyed.

3. The board may either approve or deny the proposal. Alternatively, the board may approve the proposal in part, ordering certain documents in the list reclassified. This will be an action on the agenda that must be recorded in the board minutes. The list of documents that are approved for destruction must be attached to the board minutes.

4. The records that the board has ordered destroyed may be destroyed by shredding, burning or pulping. The superintendent (or designee) must supervise this process.

Retaining emails as records

Because they have not been updated since their adoption, the regulations applicable to school and community college districts do not specifically address the retention of emails, and thus do not account for the intricacies and unique issues that email retention raises. A school district's staff may exchange thousands, tens of thousands or even hundreds of thousands of emails per day, and the notion of a single person reviewing each one of those emails on a yearly basis is unrealistic. Therefore, school districts may wish to consider establishing or updating their own policies to provide clear guidelines for school district employees on how to handle the retention of school district emails, and to reflect *City of San Jose*'s expansion of what must be disclosed under the Public Records Act.

These policies are generally adopted to supplement existing record retention regulations. To help school districts in preparing such policies, Lozano Smith has created guidance which provides optional policy language for school districts addressing email retention. A copy of this guidance is available at no cost to school districts by emailing Lozano Smith's Client Services department at **clientservices@lozanosmith.com**. Additionally, districts may wish to train employees on implementation of these new policies.

These regulations raise many questions. For instance, can a school district retain electronic copies of old records and destroy the physical originals? How does a district comply with these rules while also complying with the Family Educational Rights and Privacy Act and other state and federal laws? The answers to these questions are surprisingly complicated and frequently require consultation with legal counsel, so proceed with caution before you hit "delete." ■

Devon B. Lincoln is a Partner in Lozano Smith's Monterey office, and co-chair of the firm's Facilities & Business Practice Group.

Ryan P. Tung is an Associate in Lozano Smith's Walnut Creek office, and co-chair of the firm's Charter Schools Practice Group.

Curbing Troublesome Texts

It's often a headache for school administrators: A teacher opts to forego the district's email system and instead gives out his or her personal cell phone number, reasoning that the most effective way to communicate with his or her smartphone-obsessed students is by text. What's a district to do?

Fortunately, there are apps on the market that convert emails to text messages, allowing educators to communicate effectively with students without being forced to give out their personal phone numbers. For example, Remind allows educators to message one or multiple devices about everything from assignments to field trips and office hours without giving out personal phone numbers—while preserving a record of every message sent. Class Dojo is another app teachers can use to communicate with families, either through one-on-one messages or group messages that share photos and fun moments with families.

While such tools may provide a safer and more effective way for educators and families to communicate, it's still important for districts to do their due diligence to ensure the tools align with their district's needs, rules and values. It's also important for districts to oversee the process for selecting which apps teachers use to communicate with families, have strong acceptable use policies governing the use of district technology, establish procedures for vetting contracts and new technologies and maintain any records in accordance with the district's retention policies. ■

About The Authors

Penelope (Penny) R. Glover is Senior Counsel in Lozano Smith's Walnut Creek Office and chair of the firm's Technology & Innovation Practice Group. Her practice is also focused on the Labor & Employment and Student aspects of public agency law.

Harold M. Freiman is a Partner in Lozano Smith's Walnut Creek office. He represents school districts, county offices of education, and community college districts in such areas as school facilities, property, general education law, governing boards, student issues, business, and general litigation.

Mark K. Kitabayashi is a Partner in Lozano Smith's Los Angeles office and co-chair of the firm's Litigation Practice Group. Mr. Kitabayashi has more than 28 years of litigation experience, predominantly in the areas of employment law, local government issues, labor and employment, environmental, business, construction issues, and personal injury defense.

Devon B. Lincoln is a Partner in Lozano Smith's Monterey office and co-chair of the firm's Facilities & Business Practice Group. She is also involved in the firm's Charter Schools Practice Group.

Darren C. Kameya is a Partner in Lozano Smith's Los Angeles office and is the co-chair of the firm's Investigations practice area. For many years, Mr. Kameya has advised school district clients in both the Northern and Southern California regions.

Michael R. Linden is Senior Counsel in Lozano Smith's Fresno office. His practice is focused on assisting local government and school district clients in a wide variety of legal issues. Mr. Linden has represented numerous local public entities, both as a Deputy County Counsel in Fresno and Merced counties, and as an attorney in private practice.

Ryan P. Tung is an Associate in Lozano Smith's Walnut Creek office, and co-chair of the firm's Charter Schools Practice Group. Mr. Tung's practice focuses on charter schools, special education/student issues, school district reorganization, and work place investigations.

ADDRESSING THE COMPLEXITIES OF ELECTRONIC COMMUNICATION.

Lozano Smith has created an in-depth resource to help districts deal with issues raised by the retention of emails and the creation, sending and receipt of electronic communications related to school district business by employees and officials.

Request a free copy today.
LozanoSmith.com/electroniccommunication.php

LS Lozano Smith
ATTORNEYS AT LAW

Leading with purpose.

Disclaimer:
As the information contained herein is necessarily general, its application to a particular set of facts and circumstances may vary. For this reason, this document does not constitute legal advice. We recommend that you consult with your counsel prior to acting on the information contained herein.