Technology & Innovation Practice—Jurisprudence and Resources

TIPJar

TRENDING LEGAL DEVELOPMENTS IN THE WORLD OF TECHNOLOGY

WINTER 2018

Privacy Matters.

In this Issue:

Lozano Smith
ATTORNEYS AT LAW

Published by Lozano Smith's Technology & Innovation Practice Group

Editor's Note

BY PENELOPE R. GLOVER

Do citizens care about privacy anymore? If they don't, must our public agencies nonetheless protect it? These are questions with answers complicated by the accepted expansion of technology into our personal lives and institutions. Even so, most of us maintain some privacy boundaries. We don't want our data hacked or our identity stolen, and some of us don't want to be tracked, monitored, or subjected to targeted marketing. Yet, when we download apps, post to social media, and use our Internet of Things (IoT) devices, we effectively loosen our privacy boundaries in the interest of efficiency, convenience and connectedness. When we operate drones and enable our surveillance systems, we effectively loosen the privacy boundaries of others too.

When it comes to the government's use of technology and data, the boundaries are tighter and the expectations are higher. The government is both a technology user and a guardian of the public and its data. Public agencies like fire departments, cities and schools must balance the expectation that they invest in technology that saves lives, decreases crime, and enhances learning with their various legal obligations. In using technology to identify threats to public safety, for instance, public agencies must respect our constitutional "right to privacy" which protects citizens from governmental intrusion. But the government's obligations extend beyond this right to privacy. Public agencies must often collect, but not compromise, data about the public. They also must protect the public from those whose zeal for technology may endanger or violate the privacy rights of others.

In this issue of the TIP Jar, we discuss how public agencies must not only respect privacy, but protect it, as they consider technologies like drones, surveillance cameras, and education technology. Lozano Smith is compiling resources and best practices on information privacy and security to help public agencies navigate these emerging opportunities and challenges. As always, if you have questions or need assistance with a legal issue involving technology, 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.
pglover@lozanosmith.com

Does Anyone Really Expect Privacy?

BY
ROBERTA L. ROWE
AND
LEE BURDICK

A small drone flies 350 feet above the ground through the beautiful rust-colored mountains. A dusty road flows around the mountainside and opens up to a plateau of rock and sand. There sits a cluster of large industrial buildings, caked with red mountain dust. The buildings cover approximately a million square feet, the size of three football fields in each direction. The facility is shielded from the road by 10-foot concrete walls and a checkpoint with guards, dogs and guns.

Inside, the buildings hum with the whir of supercomputers that store gargantuan amounts of data, including emails, phone calls, Google searches and electronic communications from around the world. The machines download data at the rate of 20 terabytes—the equivalent of the entire Library of Congress—every minute. Is this a delusional conspiracy theory? A dark fantasy? An imagined dystopian future? This is the National Security Agency's $1.5 billion Utah Data Center, located in Bluffdale, Utah, the first place the government goes to search for terrorists, foreign and domestic.

While our government hunts terrorists around the world, another battle rages within U.S. borders: The conflict between our government's obligation to protect America's homeland and each citizen's right to be free from government intrusion. That conflict is magnified when new surveillance technologies disturb the balance between privacy and safety. More importantly, that war is being fought locally, in our cities, counties and school districts.

Since 1998, Americans have increased their Internet use by over 42 percent, and 75 percent of citizens now access it regularly, for everything from telephone service and email to online shopping and schooling. What most Internet users often don't consider is that almost any electronic communication can be monitored, scanned and stored indefinitely without their knowledge. Their public activities can be watched and recorded in the finest resolution. Facial recognition software can identify people in public spaces almost instantaneously. Yet most of us move through the world with little concern for these technological intrusions.

But what happens when the line blurs between our personal freedom from government intrusion and our social contract to forgo personal interests, when necessary, for greater public security? As government use of technology advances exponentially faster, that line may disappear entirely, which begs the question: Do we have a reasonable expectation of privacy anymore?

A Brief History of Privacy

Though the right to privacy is revered as fundamental, the phrase never appears in the U.S. Constitution, nor in the Bill of Rights. The closest our founders came to a "right to privacy" is inferred from various constitutional amendments. In 1965, Justice William O. Douglas explained in *Griswold v. Connecticut*:

> "Various [constitutional] guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. … The Third Amendment, in its prohibition against the quartering of soldiers 'in any

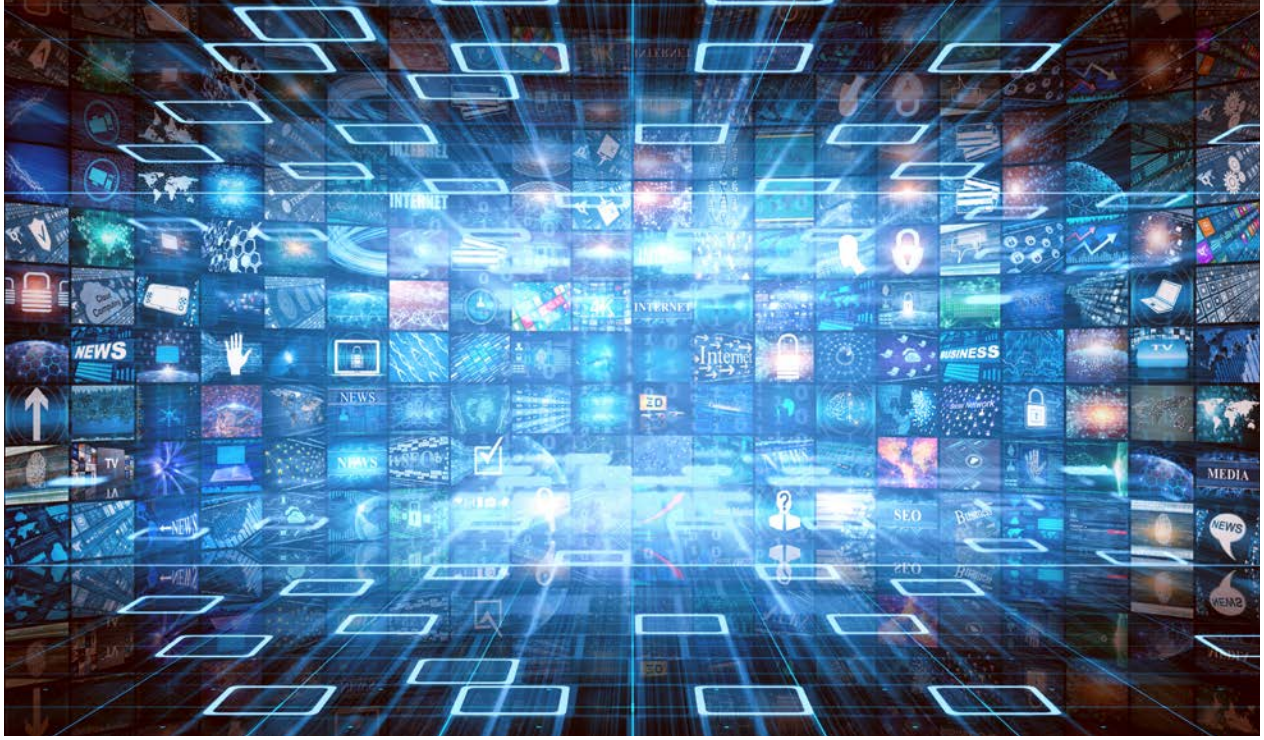
> house' in time of peace without the consent of the owner, is another. … The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."

Many court cases today address the privacy interests between private parties, involving issues like hacking personal data, identity theft and use of personal information for targeted marketing. In contrast, the U.S. and California constitutions were drafted to protect citizens from all levels of *government* intrusions into their daily lives. Whether it's federal, state or local agencies, or even school districts, government usurpation of individual freedoms has always been perceived as a threat. With the innovation of new technologies, that perception has only grown.

On the heels of the terrorist attacks on 9/11, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" or the "Patriot Act." It was unprecedented in its overhaul of the nation's surveillance laws and vastly expanded the government's authority to spy on American citizens, while simultaneously reducing the checks and balances on those powers. Following passage of the Patriot Act, U.S. intelligence agencies were allowed to collect the phone records and other electronic communications of millions of Americans and to store them at the NSA's Utah Data Center. In light of 9/11, most Americans were willing to concede some privacy interests to foster greater national security.

Several key provisions in the Patriot Act that allowed expansive surveillance expired on May 31, 2015, only to be revived and circumscribed two days later as part of the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act" or the "Freedom Act." That law now requires federal agencies to purge data regarding Americans' telephone calls after 90 days, but allows them to retain other electronic data—like emails and social media postings—indefinitely.

The Patriot Act and the Freedom Act triggered new debate over balancing privacy and national security. This is not just a federal issue. Local agencies are



dealing with video surveillance, monitoring of employees' computers, and drone issues, among others. Often, the battle lines are drawn no farther away than city hall or the school district office.

What Are "Reasonable Expectations of Privacy" Today?

As the framers debated the Fourth Amendment following the 1787 Constitutional Convention, the word "search" typically meant physically breaking into someone's house and searching it. It took the Supreme Court almost 200 years to articulate that an unreasonable "search" could be something more than just a physical intrusion. In 1967, the Court held in *Katz v. United States* that taping a microphone to the top of a phone booth and listening in on a call "searched" the phone booth, though there was no physical intrusion. In *Katz*, Justice John Harlan introduced the concept of a "reasonable expectation of privacy." He defined it this way: Is society prepared to recognize an expectation of privacy as reasonable? If so, a government intrusion into it would be patently "unreasonable" and (presumably) unconstitutional.

Since then, new technologies have presented new challenges related to privacy expectations. In 2012, Justice Samuel Alito opined for the Court in *U.S. v. Jones*:

> "[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. ... New technology may provide increased convenience or security at the expense of privacy, and many people may find the trade-off worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."

In contrast, U.S. District Court Judge Jeremy Fogel of the Northern District of California reminded us in a 2014 article for the American Bar Association's litigation journal that for "every inveterate user of social media who tweets random comments while standing in line at the grocery store, there is someone ... who is indignant when she learns that the cookies in her web browser permit all manner of advertisers to include her in their target audience." When individual norms vary so broadly on the terrain of constant technological change, what constitutes a "reasonable person's" expectation of privacy? Perhaps continued dialogue will create a standard adaptable enough to survive the challenges of new technologies. In the meantime, local agencies will have to walk this thin line carefully, and are well advised to work closely with legal counsel on how best to do it, protecting their constituents' safety while respecting their privacy. ■

Roberta L. Rowe is a Partner in Lozano Smith's Fresno office.
rrowe@lozanosmith.com

Lee Burdick is Senior Counsel in Lozano Smith's Fresno office.
lburdick@lozanosmith.com

Cameras, Questions and Collaboration

BY
HAROLD M. FREIMAN

When Greg Blount embarked on a project to install cameras in the Merced City School District's schools in an effort to quell a tide of vandalism and break-ins, a host of legal questions greeted him.

Could cameras be used to record threats of violence made in a school office, or would a right to privacy shield the person who made them? Could audio recordings be made on campus at all? How long should the cameras' recorded footage be kept, and who would have the right to view it? Would the district be required to bargain with its employees before cameras could even be installed? Similar questions would be raised by most public agencies considering the acquisition of cameras or other surveillance devices.

"It's not just (about) getting a camera in place," said Blount, the Merced district's director of IT and support services.

While the goals of installing cameras on campus—curbing theft and vandalism, safeguarding students and staff—may be noble, efforts to deploy the technology have raised legal issues with respect to student and employee privacy, public access to records and the right to be free from unreasonable government searches.

Whether a camera runs afoul of a student or teacher's privacy rights, for example, can depend on where the camera is placed and whether it records audio. While Blount recommended installing actual cameras that record video (instead of "dummy" cameras intended to deter unwanted activity), public access to video can depend on how long a district ordinarily retains it and whether students are depicted in it.

Allowing police to control, view and record data under the auspices of a grant raises another set of policy questions about how they will use video the cameras produce, Blount said, so it's important that before such a program gets underway, clear expectations are set.

Blount said it's important for IT departments considering cameras to be aware that they pose many legal questions and that there must be solid policies in place before they are in use. He said that the district's process relied on "a lot of collaboration" between its IT, facilities and

“A WISE IT DIRECTOR WILL ASK A LOT OF QUESTIONS ABOUT THE PROCESS BEFORE PUTTING CAMERAS IN OR THEY WILL BE CAUGHT IN THE MIDDLE OF WARFARE BETWEEN DIFFERENT GROUPS.”

personnel departments and the district's administration. They worked together to determine which policies would govern various uses such as proactive monitoring during the school day and the review of video depicting vandalism and break-ins.

"Each group helped bring their 'lens' to the problem so that the solution was more comprehensive than would have occurred if one department had embarked on its own version of solving the security problem," Blount said. "The team approach is the healthiest approach when building something this complex."

Ultimately, Blount opted to place cameras outside only and to avoid recording audio, though he said the district might consider expanding its use of cameras in the future. So far, he said, the cameras have been effective.

When students see that they are being monitored, he said, "That is a surprisingly good deterrent."

Blount recommended that school districts that choose to employ video cameras on campus ensure that everyone who comes on campus knows they are being recorded.

"You have to be ready to have those conversations," he said.

Blount indicated that a school district's IT department should be able to focus on technical questions like how long the cameras should record and at what resolution, and how much server space should be set aside to store the footage they produce. Ideally, the answers to those questions would be guided by district policy.

An IT department can facilitate this policy discussion, Blount said—avoiding arguments and allowing the department to maintain its proper niche as caregivers of the equipment and the data it produces. He said that getting people together to talk about the issues that on-campus cameras may raise could save IT departments a lot of work.

"A wise IT director will ask a lot of questions about the process before putting cameras in or they will be caught in the middle of warfare between different groups," he said.

Lozano Smith's Technology & Innovation Practice Group can answer your school district's questions about the potential legal issues cameras pose and can also help your policy makers craft clear policies for their use. ■

Harold M. Freiman is a Partner in Lozano Smith's Walnut Creek office.
hfreiman@lozanosmith.com

Drones

Serving and Disturbing the Public

BY
DAVID J. WOLFE
AND
IAIN J. MACMILLAN

The Federal Aviation Administration (FAA) estimates that nationwide, ownership of small unmanned aerial systems, better known as drones, will increase from 2.5 million in 2016 to 7 million in 2020. The technology's benefit to public agencies is enormous: Local public agencies can and do use drones for search and rescue activities, emergency medical response, survey and mapping purposes, student learning and more. But the rising number of drone-related incidents in California and elsewhere illustrates the need for local rules that protect public safety and privacy.

For example, the City of Seattle held a four-day trial in 2017 to prosecute a drone operator for reckless endangerment after a drone flying over a parade fell from the sky and struck and injured two people. A local prohibition on flights over crowds or in certain downtown areas would have eliminated the need for a long, fact-intensive trial and would have allowed the city to make it clear to operators that such conduct was prohibited.

The FAA takes the position that navigable airspace free from inconsistent state and local restrictions is essential to the maintenance of a safe and sound air transportation system, and has warned state and local lawmakers against enacting regulations that may be preempted by federal law. The FAA has traditionally held that its jurisdiction begins about 500 feet above ground, but the rise of drones has led the FAA to assert a more dominant role in the "gray zone" below 500 feet.

In 2016, the FAA released new rules for operators of small, commercial drones that included a rule prohibiting them from flying more than 400 feet above the ground. (Small commercial drones are those weighing 55 pounds or less; the FAA also regulates larger commercial drones, subjecting them to the same regulatory processes as civil aircraft.) Current FAA rules for small commercial drones regulate permissible hours of flight, line-of-sight observation, altitude, operator certification, aircraft registration, and marking and operational limits. But the rules are notably silent about privacy.

Owners of recreational drones were required to register with the FAA until 2017, when a federal circuit court ruled that the FAA Modernization and Reform Act expressly forbade the FAA from regulating recreational drones. The court did not rule on whether state and local agencies could fill this regulatory gap.

Despite the uncertainty, state and local governments are stepping forward to fill what they see as holes in the regulatory framework. To address privacy concerns, California lawmakers added Civil Code section 1708.8, subdivision (b), which makes an individual liable for invasion of privacy when they use a device to attempt to capture any type of visual image, sound recording or other physical impression of someone engaging in a personal or familial activity under circumstances in which they had a reasonable expectation of privacy, even if no images were captured or sold. State lawmakers also approved a law prohibiting drone operators from interfering with emergency responders in performance of their duties.

Governor Jerry Brown vetoed other bills that would have made drone operators who fly into the airspace over someone else's property less than 350 feet off the ground without permission civilly liable for trespass and would have prohibited drones from flying over state parks, schools, and prisons and jails. In his veto messages, Brown expressed concern about the creation of new crimes, the potential for a piecemeal approach to drone regulation, and federal preemption.

Cities are also stepping into the regulatory breach. In 2016, the City of West Hollywood enacted restrictions on drone use that include prohibitions on flying drones within 25 feet of any person other than an operator or their helper, over city parks during city sponsored events without a permit, or within 350 feet of airspace over a school without an administrator's permission. The city's rules, which were enacted after a drone crashed into power lines and knocked out power to hundreds of residents, extend to both commercial and recreational drones. Violators could be charged with a misdemeanor.

Local lawmakers may wish to avoid drafting drone-specific rules or restrictions that clearly infringe on the FAA's regulatory space. The City of Los Angeles withdrew charges against a filmmaker accused of violating its drone restrictions when a drone he was piloting allegedly interfered with efforts to land a police helicopter after his attorney claimed federal law preempted the city's rules. The filmmaker was subsequently acquitted of charges he operated the drone in a "careless and reckless" manner.

Local public agencies can bridge the regulatory gap by adopting laws traditionally related to local police power, including land use, zoning, trespass and nuisance and applying them to drone use. Cities

and counties should consult their legal counsel when considering laws regulating drones, including:

- Regulating where and when drones can take off and land.
- Prohibiting careless and reckless operations that endanger life or property.
- Creating rules for drone operations during parades, celebrations, and other jurisdiction-wide events.
- Creating rules for drone operations in parks and other recreational areas.

Effective management of drone use will also require monitoring of federal and state law regulating drones to avoid preemption of the local regulatory scheme. Lozano Smith is closely watching the evolution of drone rules and stands ready to help local agencies craft policies that protect public safety and privacy without intruding on federal law. ■

David J. Wolfe is a Partner in Lozano Smith's Fresno office.
dwolfe@lozanosmith.com

Iain J. MacMillan is an Associate in Lozano Smith's Los Angeles office.
imacmillan@lozanosmith.com

Tech TIP: Defining Privacy and Security

According to the International Association of Privacy Professionals (IAPP), "Information privacy" is the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." "Information security" is "the protection of information for the purposes of preventing loss, unauthorized access and/or misuse" and "the process of assessing threats and risks to information and the procedures and controls to preserve confidentiality, integrity and availability of information." ■

Shielding Student Data

BY
MEGAN MACY
AND
PENELOPE R. GLOVER

Today's parents face tough questions when it comes to their children's use of technology: Is my child being tracked by malicious or harmful cookies? Could my child's personal information become public? Could this technology expose my child to pornography or other harm? Parents are understandably cautious about their children using technology: Student privacy matters.

Parents entrust schools with monitoring and controlling their children's use of education technology products or services (EdTech) in the classroom. As schools increasingly use EdTech to enhance student learning and improve classroom management, they authorize third parties to store, access, and manage students' personally identifiable information. Under state and federal law, school districts must take steps to ensure that student data is protected. That is one reason why student privacy matters to school districts, too.

Know the Laws

School districts and providers of EdTech are subject to various state and federal laws designed to protect information privacy and ensure information security. Laws governing information privacy are designed to ensure that users are fully aware of how their personal information will be collected, used, retained, and disclosed. For example, the federal Protection of Pupil Rights Amendment (PPRA) regulates student surveys related to protected categories of information, including income, political and religious beliefs, and sexual behavior. School districts must provide notice to parents before administering such a survey and either obtain parent consent or allow parents to opt out for their children. Other laws governing information security are designed to prevent third parties from accessing and using personal information in unauthorized ways.

The laws governing information privacy and security of student records are extensive. While many EdTech providers are aware of the requirements of well-established federal privacy laws such as the Children's Online Privacy Protection Rule (COPPA) and the Family Educational Rights and Privacy Act of 1974

(FERPA), many have been slow to incorporate state requirements into their privacy policies and user agreements. California's Assembly Bill 1584 (AB 1584), codified as Education Code section 49073.1, requires EdTech providers to incorporate specific security and confidentiality requirements into their contracts. When EdTech providers refuse to do so, school districts must weigh the potential benefits of an EdTech product against the potential risks of violating student privacy and incurring penalties as a result.

School districts can familiarize themselves with state and federal laws applicable to EdTech through a 2016 report issued by the California Attorney General entitled *Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data* (https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf). The California Department of Education's Data Privacy webpage (http://www.cde.ca.gov/ds/dp/) and the California Attorney General's Privacy Laws webpage (https://oag.ca.gov/privacy/privacy-laws) also provide a wealth of information.

Practice Due Diligence

Ensuring adequate protections are in place to use EdTech can be daunting. With limited financial and human resources available to address EdTech and information privacy issues, school districts are burdened with the overwhelming task of assessing and negotiating agreements with each EdTech provider.

Districts may wish to leverage some of their most critical resources—teachers and librarians—by engaging them in a dialogue about the EdTech they wish to use in the classroom. Districts should consider creating a process for EdTech adoption that allows EdTech users to explain the value of the EdTech tools they want and to conduct some of the due diligence necessary to ensure these tools meet families' privacy needs. Districts can use this process to ensure legal compliance and to engage in a dialogue that will allow administrators and district staff who engage directly with students to work together to address issues ranging from compliance quandaries to union buy-in.

School districts may be able to reduce their risks by taking measures that enable them to:

- Train employees about laws designed to protect information privacy and security, especially those who use EdTech on a daily basis.
- Regularly evaluate and update privacy and security policies and practices and incorporate them into a data governance plan.
- Develop and implement procedures for vetting and evaluating EdTech.
- Obtain consents from EdTech users and provide privacy notices as appropriate.
- Bolster the EdTech evaluation process by considering external reviews by organizations like iKeepSafe, which have been approved under the Federal Trade Commission's COPPA Safe Harbor Program (https://www.ftc.gov/safe-harbor-program).
- Consult legal counsel about risks and additional protective measures.
- Communicate with the school community about the use of EdTech and the associated benefits and risks.

While such measures do not eliminate all of the risks of using EdTech in the classroom, they may mitigate them. These are complex issues and Lozano Smith's Technology & Innovation Practice Group is committed to developing practical solutions. ■

Megan Macy is a Partner in Lozano Smith's Sacramento office and co-chair of the firm's Facilities & Business Practice Group.
mmacy@lozanosmith.com

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

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, governance, student issues, business, and general litigation.

Megan Macy is the Managing Partner of Lozano Smith's Sacramento office and provides general counsel to school districts and other public agencies. She is an active member of the Firm's Labor & Employment, Facilities & Business, and Charter Schools practice groups, and works closely with clients to develop the right solution for each legal issue.

David J. Wolfe is a Partner in Lozano Smith's Fresno office. Mr. Wolfe serves as the City Attorney for the City of Clovis and the City of Fowler. He regularly participates in activities with the League of California Cities. He has served as Judge Pro Tem for the Fresno County Superior Court.

Roberta L. Rowe is a Partner in Lozano Smith's Fresno office. She focuses on student and labor and employment matters for school and community college districts in her daily practice. Ms. Rowe has expertise in employee matters, termination and layoff hearings, collective bargaining, grievance arbitrations, and unfair labor practice charges.

Lee Burdick is Senior Counsel in Lozano Smith's Fresno office. Her practice is focused on the Local Government aspects of public agency law. She has more than 25 years of experience counseling clients regarding their relationships with federal, state, and local government agencies.

Iain J. MacMillan is an Associate in Lozano Smith's Los Angeles office. He assists public agency clients on a wide variety of local government issues. His practice is concentrated on code enforcement, Brown Act and Public Records Act compliance, conflicts of interest, risk management, procurement, transportation, and education.

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.