Fagen Friedman & Fulfrost LLP

Fourth Amendment Rights in the Internet Age

California County Superintendents Educational Services Association

PASSCo General Session Meeting

May 13, 2016

Presented by
Kerrie McNally, Partner
Justin Simpson, Senior Associate
Fagen Friedman & Fulfrost, LLP
www.f3law.com

TABLE OF CONTENTS

Page

Senate Bill 178, Electronic Communications Privacy Act
Frequently Asked Questions

Q: What is Senate Bill ("SB") 178?

A: SB 178 is the Electronic Communications Privacy Act. Under SB 178, with limited exception, unless a ***government entity*** possesses a warrant, wiretap order, subpoena, or specific consent, it shall do none of the following:

1. Compel the production of or access to electronic communication information from a service provider;
2. Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device; or
3. Access electronic device information by means of physical interaction or electronic communication with the electronic device.

Q: Does SB 178 apply to school districts?

A: The legislative history shows that the intent of the law was to prevent law enforcement from conducting unlawful searches and seizures. However, the law defines "government agency" as "a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof." School districts are a political subdivision of the state. Therefore, based on the definition of "government agency", SB 178 appears applicable to school districts.

Q: Can a school district demand that an employee or student return a district-owned electronic device?

A: Yes. SB 178 relates only to the search/review of "electronic device information." SB 178 defines "electronic device information" as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." Therefore, a school district can demand that an employee, student, or parent return a district-owned electronic device. However, if the district desires to review the information stored on the device, it must consider the implications of SB 178.

Q: Can a school district search/review electronic device information stored on district-owned devices?

A: Yes. A school district may obtain "specific consent" from the "authorized possessor" of the device to review the electronic information on a device. Alternatively, the school district may revoke the authorization to possess a district-owned device and then obtain the electronic information from the district-owned electronic device.

SB 178 defines "authorized possessor" as "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device." If the school district designates an employee, student, or parent the "authorized

possessor" of a district-owned device, the school district may require the individual to return the devise and then search the electronic device information stored on the device. However, a district may compel no one other than the "authorized possessor" (e.g., the employee's spouse, family member, co-worker, etc.) to grant access to the electronic information on the device. Therefore, when providing district-owned devices to employees, school districts should carefully identify the "authorized possessor." Regarding devices issued to students, school districts should carefully identify the "authorized possessor" to include both the student and the student's parents.

SB 178 defines "specific consent" as "consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient or member of the specific audience is a government entity."

If an authorized possessor grants traditional consent, sends electronic information through the district's server/network, or sends electronic communication to any district employee, we believe it may be argued that the individual granted "specific consent" to the district to search the electronic information on a device. Text messages and photographs are the two sets of information that may escape the reach of the district under the definition of "specific consent." We recommend school district revise their Acceptable Use of Technology Policies to grant the district specific consent to the district to search electronic device information contained on district-owned devices.

Q: Can a school district search/review electronic device information stored on its server/network?

A: Yes. Under SB 178, a governmental agency may access "electronic device information" if it receives "specific consent" from the "authorized possessor" of the device to do so . Under the definitions of "specific consent" and "authorized possessor", we believe that when an employee or student (1) sends electronic device information through the district's network/server, or (2) stores electronic device information on the district's network, the employee or student is arguably sending the material to the government entity and thereby granting the government entity specific consent to access the information. We recommend that districts review/revise their Acceptable Use of Technology Policies to reflect that consent is granted to the district to search/review electronic device information sent through and stored on the district's network/server.

Q: Can a school district seize and search a student's personal electronic device?

A: Maybe. Under SB 178, a student is likely the "authorized possessor" of a personal electronic device in his/her possession and the electronic device information contained therein, even if his/her parent is the owner. Therefore, if a student or parent grants consent to the school district to search the device, the school district may do so. If the student or parent does not grant consent, the question remains regarding whether the school district may compel the production of the electronic device information under the longstanding rules and regulations regarding

student searches and seizures. (See, *New Jersey v. T.L.O.* (1985) 496 U.S. 325.) However, SB 178 does not impact confiscation or seizure of the electronic device.

Q: What can school districts do to limit the impact of SB 178?

A: We recommend that school districts review/revise their Acceptable Use of Technology Policies to include provisions that:

- Define the term "authorized possessor" for the purposes of district-owned devices;
- Identify that consent is given to the district to access all information sent or stored on the district's server/network;
- Grant consent to the school district to access all district-owned electronic devices and the information created by those devices; and,
- Identify that consent is given to the district to access all information sent by or to district employees.

Q: What are the consequences of violating SB 178?

A: Under SB 178, the process for excluding evidence obtained in violation of SB 178 is through a Penal Code suppression hearing. There is no mechanism for suppressing evidence in an administrative hearing. It may be very difficult, if not impossible for a student or employee to suppress evidence in an administrative proceeding, even if the evidence is obtained in violation of SB 178. SB 178 also provides that the Attorney General may bring a civil action against the school district to compel compliance with the law. Additionally, an individual may have a legal claim for violation of his/her civil rights, if a search or seizure violates constitutional standards.

Potential Acceptable Use of Technology Policy Language
To Be Integrated Into Current Policy

Computing devices (including computers and mobile devices) and the district's network communication systems (including but not limited to the email system and district on-line collaboration and file storage services) are owned and/or managed by the District and are maintained for the express purpose of staff carrying out the district's educational mission which includes teaching, information processing for school business, and enhancing communication between district staff, parents, students, and community members.

1. Authorized Possessor

District-owned computing devices may be given to staff members to carry out the District's educational mission. Upon receipt of a District-owned device, the staff member is the authorized possessor as defined by the California Electronic Communications Privacy Act (also known as CalECPA or SB 178). Staff members understand and acknowledge that the District may, at any time, without cause, confiscate any District-owned device and search the electronic communication information stored therein. Upon such confiscation, the staff member is no longer the authorized possessor of the District-owned device. While serving as the authorized possessor of a District-owned device, the staff member is personally responsible for keeping the device free from illegal content or material inappropriate for the school setting. District-owned devices issued to staff are not to be used by staff members' family or friends for personal uses.

2. Specific Consent

Users of the District's computer systems should be aware that the data they create, store, or transmit on the District's systems including email, voice mail, and any computer files are not private and remain the property of the District. The District reserves the right to monitor all files, programs, apps, internet traffic, and communications that reside on District computers (including iPads) and servers or travel over its network at any time without additional notice or consent. Staff using personal accounts to load apps and resources onto a District-owned device must exercise prudent judgment to ensure that only appropriate apps and resources for the school setting are loaded onto the District-owned devices. Staff should not expect personal apps, files, or email accounts residing on a District-owned device or District managed service to remain private. The District retains the right to inspect, delete, and report any apps, information, and files that find their way onto district owned computing devices (including iPads) or remote storage systems (including district maintained internet/cloud storage accounts). By the use of the District's computing and communications systems and devices, staff members grant specific consent, as defined by CalECPA, to the District to review and monitor electronic communication information and electronic device information created, stored, or transmitted on the District's systems and devices.

Potential Employee Acceptable Use Policy Consent Form
To Be Integrated Into Current Consent Form

[Insert Name of District]
STAFF TECHNOLOGY ACCEPTABLE USE POLICY
Acknowledgement and Annual Signature Page

[INSERT NAME OF DISTRICT] employees are expected to review, understand, and abide by the policies described in the Staff Technology Acceptable Use Policy and the accompanying procedures provided by the District Technology Department. This document is legally binding on employees, whether or not they have signed the Acceptable Use Policy. [INSERT NAME OF DISTRICT] supervisors are required to enforce these policies consistently and uniformly. No supervisor has the authority to override the policies unless he or she obtains the written permission of the Superintendent. Signed Acceptable Use Policies are kept on file at [INSERT NAME OF DISTRICT]. Any employee who violates any provision of this Acceptable Use Policy shall be considered as having acted in an individual capacity and outside the scope of employment and, as such, may be subject to disciplinary action, up to and including termination or criminal prosecution by government authorities. The following statements are provided in accordance with Board Policy 4040.

No Possessory Interest: I have read and understand the Staff Technology Acceptable Use Policy, the latest version of which is posted on the district website at www.[Insert Name of District]. I understand that I have no specific ownership or possessory right in the District device I use or in the information stored or created therein. The Device is the property of the District. This Device and the information contained therein may be assigned or used by other employees, on as-needed basis, in furtherance of the District's operational and administrative objectives. I further understand that the District has the right and does periodically upload information from my device to District maintained servers and databases and that my internet use may be monitored and restricted by District filtering devices.

District Access to Device: I recognize that the District will periodically access my cellular telephone, computer (laptop and/or desktop), and/or other personal computing and communicating devices to perform the following functions:

a) Repairs or maintenance of the device.

b) Upgrading of device.

c) Retrieval of information in response to Public Records Act.

d) Retrieval of records in compliance with the Pupil Record Act, Education Code section 49062, et seq., FERPA and AB 1584.

e) Fulfill the District's statutory duties and Board policies to maintain public records.

f) Conduct administrative searches of the device.

g) Monitor employee compliance with state and federal law and District policy.

I understand that I shall have no expectation of privacy when using District computing equipment or technological resources, including but not limited to District provided email, file storage systems, and other communication and collaboration services.

I also understand that any District or school records maintained on any of my personal devices or messages sent or received on a personal device that is being used to conduct District business may be subject to disclosure, pursuant to a subpoena or other lawful request.

I also understand that in order to comply with state and federal student privacy laws, I will not allow people who are not District employees (such as parents, volunteers, or students) to use or access my District issued computing device since confidential or protected student information or sensitive District email communications may be stored or accessed from there.

Employee Name: _____
(Printed)

Employee Signature: _____

Date: _____

Effective School Year: _____

School Site Administrator and Staff Guidelines for Search and Confiscation/Seizure of Student Electronic Devices, Senate Bill 178

Overview

On January 1, 2016, the California Electronic Communications Privacy Act (also known as CalECPA or SB 178) took effect placing new restrictions on "government entity" searches of electronic devices. The definition of "government entity" under the CalECPA is broad and appears to include school districts.

The CalECPA prohibits government entities from searching the electronic device of any person or compelling the person to provide access to the electronic information on the device, except in very limited circumstances including:

- The person affirmatively consents to the search of his/her personal electronic device.
- If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device.
- If the government entity, in good faith, believes the device to be lost, stolen, or abandoned. However, the search must be limited only as necessary to identify, verify, or contact the owner or authorized possessor of the device.

In sum, CalECPA is broad and appears to eliminate the "reasonable suspicion" standard for search of student personal electronic devices thus prohibiting school administrator and staff member searches of student personal electronic devices except in these limited circumstances.

We are assessing our current District Policies and Regulations for necessary revisions to ensure compliance with CalECPA, as applicable. On an interim basis, we are providing these *working guidelines* to assist our site administrators and staff members to conduct lawful and effective searches and/or confiscations of student electronic devices consistent with CalECPA. These guidelines may not address all potential situations where searching/confiscating a student's electronic device may be considered. If you have any questions about a particular situation, please contact [INSERT DISTRICT CONTACT].

How is electronic device defined?

For the purposes of these guidelines, an electronic device means a student's personal device that stores, generates, or transmits information in electronic form. This includes but is not limited to computers, disks, drives, tapes, mobile phones, smart phones, and other communication devices, cameras, music and other media players, and any other electronic or digital devices.

Can I confiscate a student's electronic device?

A student's device may be confiscated when an administrator or staff member has reasonable suspicion that the device contains evidence of misconduct, or if there is reasonable suspicion that the student is using the device to engage in misconduct (for example, the student is using the

device during instructional time or otherwise using the device against school rules of conduct or the technology use policy). Once the student's device is in the possession of the administrator or staff member, the administrator or staff member should store the device in a safe and secure location (for example a locked or secure drawer or office). The device may be retained for a reasonable time to ensure the misconduct does not persist or to determine whether the device may be searched, if necessary.

Administrators/staff members should NOT access or search student electronic devices except in compliance with the guidelines contained herein.

What do I do if a student is disrupting school activities with an electronic device?

If a disruption occurs or a student uses any electronic device in violation of District or school policy, an administrator or staff member should direct the student to turn off the device and/or confiscate it. If confiscated, the device should be returned at the end of the class period or school day. The administrator or staff member should NOT access or search the device in this circumstance.

Can I search an electronic device if there is an imminent danger of death/serious physical injury?

In an emergency, if the administrator or staff member reasonably believes that a student's electronic device contains information necessary to prevent death or serious physical injury, the administrator should confiscate the device, seek the consent of the student to search the device, and notify law enforcement immediately. If law enforcement assistance is not immediately available, and the student does not consent, the administrator or staff member, as necessary, may immediately search the contents of the electronic device. The administrator must promptly file an incident report with [INSERT DISTRICT CONTACT] detailing the circumstances necessitating the search, the scope of the search, and the information discovered during the search.

Can I search an electronic device if the student is suspected to have engaged in criminal conduct with **no imminent danger** of death/serious physical injury?

If the administrator has reasonable suspicion to believe that a student's electronic device contains evidence of criminal misconduct, and there is **no imminent danger of death or serious physical injury**, the administrator should confiscate the device, contact law enforcement to assess and conduct the search, and then contact the student's parent/guardian to notify them of the circumstances and the confiscation of the device. The administrator or staff member should **NOT** access or search the device in this circumstance.

Can I search an electronic device if the student is suspected to have engaged in misconduct (non-criminal) with no imminent danger of death/serious physical injury?

If the administrator has reasonable suspicion to believe that a student's electronic device contains evidence that a student is violating Board policy, administrative regulation, or other rules of the District or the school, but, the administrator does not suspect that the student is engaged in criminal conduct or there is no imminent danger of death or serious physical injury, the

administrator may confiscate the device, and should seek consent from the student or parent/guardian to search the device. If the student or parent/guardian does not consent to the search, or if the administrator has any questions or concerns regarding the search, the administrator should confiscate the device, and contact [INSERT DISTRICT CONTACT] for further guidance ***prior to*** searching the device.

Should teachers or staff members search student's electronic devices?

Absence of imminent danger of death or serious physical injury, it is recommended that teachers and staff members contact their site administrators for guidance before searching any student's electronic device.

What happens if an unlawful search of a student's electronic device is conducted?

The student may have a legal claim for violation of his/her civil rights and/or the Attorney General could bring a civil action against the District to compel compliance with the law. Additionally, evidence obtained from an unlawful search may be excluded from use or consideration in a disciplinary proceeding.

Paid Administrative Leave Checklist

When placing an employee on paid, administrative leave, school districts frequently restrict the employee's access to school/district grounds and students. School districts should also consider restricting the employee's access to electronic systems and devices.

Upon placement on paid, administrative leave, school district administrators should consider the following:

1. Confiscating employee keys.
2. Confiscating and securing district-owned and issued portable electronic devices (e.g., cell phone, iPad, tablet, etc.).
3. Confiscating and securing district-owned desktop computers.
4. Restricting employee access to district network, including email.

Human resource administrators should consult with IT administrators when making decisions regarding items 2 through 4 above. A school district should have articulable reasons for taking, or not taking, the above-identified actions when placing the employee on paid, administrative leave. If a school district takes action to confiscate or restrict employee access as identified above, district administrators should document the date and time that access is restricted and/or device is confiscated.

Caution: If a device is confiscated and the school district believes that it contains information that is the basis for misconduct and a forensic investigation is required, the school district should not reboot the device or use the device before the forensic investigator images the device.

Legally Defensible Investigations

1. **Think and Act Like an Expert.**

    a. There are three types of witnesses: lay witnesses, character witnesses, and expert witnesses. When testifying about an IT investigation, the investigator will likely be called as an expert witness.

    b. When examining an expert witness, an attorney will always review the following topics with the witness.

        i. IT Investigator/Witness Qualifications
        ii. IT Investigator/Witness Training in the Field
        iii. IT Investigator/Witness Experience in the Field
        iv. Industry Standards
        v. IT Investigator/Witness Investigation Protocol
        vi. Results of Investigation at Issue
        vii. IT Investigator/Witness's Expert Opinion
        viii. Review of IT Investigator/Witness Report

    c. School district IT administrators who act as investigators in human resources investigations should maintain a current resume, receive continuing education in their field, and remain current in educational technologies.

    d. Additionally, IT administrators who act as investigators in human resources investigations should receive training regarding general investigation protocols and the preservation of electronic evidence, and develop strong report writing skills. Human resources administrators should invite IT administrators to investigation trainings provided to school site administrators.

2. **Chain of Custody.**

    a. The term "chain of custody" refers to the documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence. Evidence must be accounted for – from the moment it is seized, to the day of trial.

    b. **Identify and Label**. When initially seized, everything should be identified and labeled. The investigator should identify everything, including computer, monitor, cables, and periphery devices. It is best practice to give all equipment a label with a barcode number to track the item through the chain of custody until trial. When identifying and labeling seized equipment, the investigator should note the condition of the equipment and describe the equipment in a case log. The investigator should note any dents, scratches, or otherwise unremovable marks on the equipment.

c. **Date and Time**. At the time of the initial seizure, the actual date and time should be recorded. Every time the evidence changes hands, the date and time should be recorded.

d. **Witness**. It is best practice to have two investigators assigned to a case. A lead investigator and a "witness" investigator. The witness lends credibility to the investigation, can testify about the truth of any anomalies that occur in the investigation, and can testify in the lead investigator's absence.

e. **Avoid Contamination**. Along the chain of evidence, the evidence must not be contaminated by a third party. Refrain from rebooting (if the computer is off) or using the computer until the computer can be imaged.

f. **Best Evidence**. In a perfect world, the school district will maintain the electronic device through trial. This allows the school district to produce the "best evidence" at trial.

3. Lawful Search and Seizure.

a. The Fourth Amendment to the United States Constitution protects individual privacy rights. Specifically, it protects individuals against unreasonable searches and seizures.

b. When a school district seeks to confiscate an employee's electronic device, the school district must consider the employee's privacy rights, if any, in the device.

c. Employees have very little, if any, privacy rights in the district-owned devices issued to them and the information created on those devices. However, SB 178 complicates a school district's ability to search a district-owned device.

4. Documenting the Investigation Process.

a. All investigators are encouraged to document their investigation process. A "case log" identifies all activity in the investigation. The case log is an overview of the investigation process. All activities should be recorded in the case log, even if the activity is not helpful to the overall investigation. For each step of the investigation, the case log should identify: who, what, when, where, why, and how. The case log lends credibility to the overall investigation and is a tool that the investigator may use to refresh his/her memory regarding the investigation if the case proceeds to trial.

Date	**Time**	**Activity**
February 29, 2016	8:00 – 11:00 a.m.	J. Simpson and P. Fagen conduct interview with K. McNally regarding interaction with suspect employee on 2/28 which led to investigation. Will be a great witness. Credible. See interview notes.
March 1, 2016	10:02 a.m.	Seize employee laptop computer, battery cable, and wireless mouse. Present: J. Simpson and P. Fagen. <u>Laptop Computer</u> Computer Serial No. 12345678. Computer was found in "off" mode. No dents, scratches or other unremovable marks. Appears to be in good condition. Barcode number assigned and label affixed. Barcode number 987654. (Repeat for battery cable and other auxiliary components.)
March 1, 2016	11:15 a.m.	Remotely review employee internet use. Present: J. Simpson and P. Fagen. No improper websites discovered. Apparent excessive use of internet. See report generated by "X" Program.

Tips from a Forensic Computer Investigator

1. **Provide the forensic investigator with the computer.**

    a. School districts may be inclined to extract the hard drive and provide it, alone, to the forensic investigator. This is not sufficient.

    b. The BIOS (basic input/output system) is also required as part of the forensic investigation. The BIOS contains the date and time stamp of the computer. The BIOS is located in the laptop computer or the tower of the desktop computer.

    c. In many, if not all, investigations, the time and date of the alleged event(s) is critical. Without the BIOS, the forensic investigation is incomplete. The investigator cannot rely on the date and time provided by an external device because the BIOS may not account for daylight savings time or may otherwise differ from the actual date and time.

2. **Create an image of the device first.**

    a. Districts often seize employee devices before contacting a forensic investigator. At times, the district IT department will attempt to uncover the employee's wrongdoing without the assistance of a forensic investigator. This can create a challenge because now the district has altered the information on the device. If no image has been created, the district may unwittingly create a defense for the employee.

    b. For instance, the district investigator will load the employee's web browser and visit potentially illicit websites on the employee's computer. As a result, the employee's web activity history will include searches and other web activity after the date and time that the employee's access was restricted. The employee may argue that he did not visit the improper websites, rather the district visited the sites. It is a best practice to not start the device and/or using the device until an image is made of the device.

3. **Remember the Best Evidence Rule.**

    a. Under the California Evidence Code, if a writing is offered as evidence, a copy of the evidence is not generally accepted unless there is an adequate explanation for the absence of the original. The original document (electronic device) is the best evidence.

    b. Districts are best served to refrain from "re-deploying" an electronic device that is the subject of a forensic investigation until after all legal proceedings are complete. This will allow the district to use the original computer in trial.

Fagen Friedman & Fulfrost LLP

Kerrie E. McNally
Partner

Governance & Leadership
Labor & Employment
Litigation
Student Services & Special Education

Inland Empire
Phone: 951.215.4900
Fax: 951.215.4911

Los Angeles office
Phone: 323.330.6300
Fax: 323.330.6311
kmcnally@f3law.com

Kerrie E. McNally is a partner at Fagen Friedman & Fulfrost, working from both the Inland Empire and Los Angeles offices. Ms. McNally is co-chair of the firm's Labor & Employment Practice Group. She represents and advises school districts in the areas of labor and employment, litigation, special education, and student discipline and property issues. A member of the firm's eMatters Practice Group, Ms. McNally has experience working with school districts on employee discipline matters arising from improper use of technology. Ms. McNally has successfully represented school districts in federal and state court, teacher dismissal hearings, certificated layoff hearings, classified termination hearings, grievance arbitrations and special education due process hearings. She has also defended school districts before the California Department of Education, the Office for Civil Rights, the Department of Fair Employment and Housing and the Equal Employment Opportunity Commission. Ms. McNally has lectured on the role of general education teachers within the special education matrix at the University of La Verne's College of Education and Organizational Leadership.

Prior to practicing law, Ms. McNally taught middle school science, math, Spanish and physical education. She received her Juris Doctor from the University of San Diego School of Law, cum laude, and is a member of the Order of the Coif. Ms. McNally was a law clerk for the University of San Diego's Children's Advocacy Institute. She was also a member of the University of San Diego Appellate Moot Court Board. While she was in school, she worked as a law clerk for the San Diego District Attorney's Office in the Family Protection Division.

Ms. McNally received her bachelor's degree from the University of California, Los Angeles and her California Clear Multiple Subject Teaching Credential from Chapman University.

Fagen Friedman & Fulfrost LLP

Justin J. Simpson
Senior Associate
eMatters
Governance & Leadership
Higher Education
Labor & Employment
Student Services & Special Education

Sacramento office
Phone: 916.443.0000
Fax: 916.443.0030
jsimpson@f3law.com

Justin J. Simpson is a senior associate in Fagen Friedman & Fulfrost's Sacramento office and co-chair of the firm's Labor & Employment Practice Group. He is also an active member of the Governance & Leadership and eMatters Groups. Mr. Simpson regularly advises K-12 and community college governance teams across a broad spectrum of issues including labor negotiations, contract interpretation and administration, grievance handling, classified and certificated employment matters, Board governances, conflicts of interest, ethics, Brown Act requirements, the California Public Records Act compliance, uniform complaint investigation and resolution, and student matters.

Mr. Simpson's practice focuses on working with clients to meet their individual labor and employment goals while maintaining compliance with Education Code and other relevant state and federal laws. In that capacity, Mr. Simpson regularly drafts and interprets collective bargaining language, implements classified and certificated employee discipline and layoffs, and counsels on the enforcement and adequacy of local agency policies, rules and regulations. Mr. Simpson also provides preventative training on topics including sexual harassment, discrimination, mandated reporting, and others. He is certified as a school management negotiator through the School Employers Association of California (SEAC), having completed the School Management Negotiators Certification Program.

Mr. Simpson has exclusively practiced education law throughout his career. He currently serves as outside counsel to numerous school districts and county offices of education throughout California. Prior to moving to private practice in 2008, Mr. Simpson served as Assistant General Counsel for the former Grant Joint Union High School District, now the Twin Rivers Unified School District. In this capacity, he reported directly to the District General Counsel and assisted with myriad issues ranging from student rights, school district reorganization and employee investigation/discipline to statutory and regulatory compliance.

Mr. Simpson received his Juris Doctor, with distinction, from the University of the Pacific, McGeorge School of Law in 2007. In addition to writing regularly for the McGeorge Law Review, Mr. Simpson served as a primary legislative editor. He holds a bachelor's degree in Business Administration from San Diego State University.