50 Years of School Technology: Lessons Learned from the Past and Legally Defensible Practices of the Future

Erin Gilsbach, King Spry Herman Freud & Faul, Bethlehem, PA

Presented at the 2017 School Law Seminar, March 23-25, Denver, Colorado

The NSBA Council of School Attorneys is grateful for the written contributions of its members. Because Seminar papers are published without substantive review, they are not official statements of NSBA/COSA, and NSBA/COSA is not responsible for their accuracy. Opinions or positions expressed in Seminar papers are those of the author and should not be considered legal advice.

© 2017 National School Boards Association. All rights reserved.
LESSONS LEARNED FROM THE PAST
and
LEGAL DEFENSIBILITY PRACTICES
OF THE FUTURE

Erin D. Gilsbach, Esq.

erin.gilsbach@gmail.com
# 50 YEARS OF SCHOOL TECHNOLOGY

## INTRODUCTION

- A Note to School Law Attorneys: ................................................................. 4
- A Note Regarding Formatting and References ............................................. 6
- Final Note ........................................................................................................ 6

## DATA PRIVACY

- Privacy and Employee Cell Phones ............................................................. 8
- Ransomware and Data Hacking Schemes ....................................................... 11
- 3rd-Party Providers and Data Privacy ............................................................ 15
  - Google Apps for Education / G-Suite ......................................................... 16
- School Visitors Information Collection and Data Breach Laws .................. 21
- 3rd-Party Apps, COPPA, and Parental Consent ............................................ 24

## BIOMETRICS

- ...................................................................................................................... 34

## DIGITAL RECORDING

- Student Recordings in School ................................................................. 41
- Policy Issues ............................................................................................... 45
- Wiretap Laws ............................................................................................ 47
- Prohibiting Recording at IEP Meetings ...................................................... 50

## PORNOGRAPHIC CONTENT IN SCHOOL ONLINE LIBRARIES

- CIPA Concerns ........................................................................................... 59

## DRONES

- ...................................................................................................................... 61

## 1:1 AND BYOD (BRING YOUR OWN DEVICE) INITIATIVES

- ...................................................................................................................... 64

## TECHNOLOGY AND SCHOOL HEALTH

- ...................................................................................................................... 72

## LIVESTREAMING

- Livestreaming in the Classroom ............................................................... 78
- Livestreaming of School Events ............................................................... 81

## SCHOOL DISTRICT CYBER OPTIONS

- Special Concerns Regarding Cyber-Options and Students with Special Needs ......................................................... 94

## REFERENCES

- ...................................................................................................................... 97

## APPENDIX A: STATE WIRETAP LAW CHART

- ...................................................................................................................... A-1
INTRODUCTION

The 50th anniversary of COSA is an ideal time to reflect upon the past 50 years and think about what’s ahead. Compare the pre-digital world of slide rules, handwritten book reports, and computers the size of small office buildings to today’s world, where students can enter a response to a teacher’s question on the phones from their pockets and wirelessly send the answer to the teacher’s computer instantaneously. It’s mind-boggling. Technology has changed at a dizzying pace over the last 50 years, and schools and educators have historically been eager to match its lengthy strides, attempting to use the latest technology in innovative ways that will improve students’ learning and academic performance.

The law, however, will, as a rule, always be behind advances in technology, and the faster a particular technology develops, the farther behind the law becomes. Technology is innovative by nature, yet our common law system is reactionary at its core, and statutes are promulgated as solutions to problems that already exist. Our law, whether statutory, regulatory, or caselaw, is created and honed through experiences, which result in a linear pattern of events. An act occurs; a consequence ensues; and legal action is commenced. Months or even years later, a decision is rendered that provides a glimpse of interpretative detail on a particular aspect of technology law. By the time cases involving the use of a fax machine are over, our fax machines have long-since been retired, and we are emailing information in PDF files or making educated guesses about how the legal theory behind that fax machine fact pattern would apply to an emailed PDF document. Sometimes the answers are clear and come easily; other times, they do not.

The juxtaposition of snail-paced legal development and ever-changing technology frequently leaves us with more questions than answers, and we are all-too-often required to apply technology law through analogy rather than direct comparison. We use legal premises established in 1st Amendment caselaw about a student’s use of MySpace to hypothesize about whether a similar premise would be
applicable to a Twitter feed. We analyze and analogize physical search and seizure cases to determine the legal boundaries of a search within the functions and features of a smartphone. And it is not only the practitioners that are faced with these sometimes difficult tasks. With each new technology, the courts, themselves, are required to first understand how it works and then draw legal conclusions and distinctions, through analogies and comparisons, to non-tech concepts or caselaw precedent involving outdated technology.

If these types of cases are presenting such significant challenges to the courts and seasoned practitioners of the law, think, then, how much more difficult it is for school administrators and personnel to keep up with the changes, legal obligations, and potential legal issues. In such a landscape, spotting potential liability, or even issues that should be brought to the attention of legal counsel, becomes difficult, if not impossible. Thus, it is incumbent upon the school attorney to spot such issues and potential liability with and for the client, wherever possible. This paper was created with that end in mind.

**A Note to School Law Attorneys:**

This paper was not intended to be an all-inclusive discussion of every technology law issue facing schools today. In fact, readers may be surprised to find that it is somewhat lacking in information on the more common technology issues with which school attorneys are familiar, such as sexting, 1st Amendment protections, cyber-bullying, student discipline for off-campus online speech and other issues. For those types of issues, there are many available resources from highly-respected experts. Indeed, COSA has a wealth of information on many of these issues (as well as hundreds of others). Instead, this guide was created and intended to assist practicing school law attorneys in identifying and understanding some of the education technology issues that are directly affecting public schools today but which may not be proactively brought to the attention of a school solicitor by the client.
districts. For further analysis of any of the issues discussed in this paper, I encourage readers to check COSA’s resources regarding the laws that are implicated. COSA has papers that provide in-depth analysis on most of the legal issues raised in this paper.

There are a number of reasons why schools may not bring an education technology issue to the attention of their solicitor or specialized legal counsel: perhaps the client district does not recognize the legal significance of an issue; perhaps the client feels that, if there are legal issues, they are inevitable due to the fact that an edtech contract has already been executed or a commitment has already been made to use a particular technology; or perhaps the district-level administrators, who would generally bring issues to the school solicitor, are not even aware of the practices of a particular employee, school administrator, or building level that may have given rise to one or more of the issues discussed herein. Regardless of the reason, it is simply a fact that education technology issues are often not brought to the attention of the school’s legal team until a lawsuit has been filed or liability is imminent. In other words, until it is too late. It is those issues that this paper seeks to illuminate in order to better enable school attorneys to know what questions to ask and to more proactively protect the legal interests of their clients.

With the assistance and support of such organizations as NSBA, COSA, and our state school boards associations, we have the ability to protect and assist our schools in both defensive and proactive ways. I have personally benefitted greatly by the assistance, support, and guidance of many of my colleagues through NSBA, COSA, and the PA School Boards Association’s Solicitor’s Association, and it is my intent and hope that these materials will be able to, in turn, provide at least a starting point for further research and discussion on the issues set forth herein.
A Note Regarding Formatting and References

These materials were designed with readability in mind and are not intended to strictly follow any specific scholarly formatting. In order to provide comprehensive resource information while emphasizing quick legal references for attorneys who really don’t have time to sift through comprehensive resource information (who does?), I decided on a unique hybrid format, which requires some explanation. All non-legal references, such as articles, websites, news sources, and other reference materials, are presented as endnotes, identified numerically in the text with numbers set in brackets. (In my opinion, APA format, with its embedded information and non-numerical references is too cumbersome and unwieldy.)

To enable better quick-reference for legal purposes, however, all legal citations, such as statutes, caselaw, and federal and state legal guidance documents (such as “Dear Colleague Letters,” etc.) are contained within footnotes on the page in which they are referenced, as are any side-bar discussions or peripherally-relevant information. I found this to be the best way to highlight the legal references without making the footnotes too burdensome or forcing attorneys to constantly flip back and forth to the endnotes for legal citations. I know that this method is entirely unorthodox, and, while I hope that it has the effect of being beneficial rather than burdensome, I apologize if the resulting organization is confusing. My intent was to lessen the burden, not increase it.

Final Note

Although I have worked diligently to try to catch errors and typos, I am certain that there will be some. Any errors or inconsistencies are solely my own error and do not reflect upon the wonderful team at COSA, who have been infinitely patient with me over the past few months as I kept finding “one more issue” to add. Likewise, all opinions, editorial comments, and legal conclusions are my own and do not necessarily reflect those of COSA.
In 2014, NSBA issued a publication called “DATA IN THE CLOUD: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era.” [1] That document, sparked, in part, by a New York Times article [2] that highlighted potential student data privacy issues in public schools related to cloud computing, highlighted the importance of keeping student data privacy at the forefront when making decisions regarding cloud computing contracts and partners. An excellent COSA resource on this topic is “Data Privacy Law Update: Ten Things to Advise Your School Board Clients – Before It’s Too Late.” [3] That paper, from COSA’s 2016 School Law Practices Seminar, outlines important issues related to data privacy and highlights the growing state trend to fill in federal gaps in student data privacy protection with state student data privacy legislation. Data privacy is the most common technology concern in schools today, and rightly so. A number of technology trends pose legal compliance challenges for schools. This section highlights a few of those and proposes solutions to some of those issues.
In 2017, most cloud computing options are now available not only on school-owned computer desktops and devices, but also on personal employee cell phones. In addition, increased device memory capacity allows users to carry huge amounts of information on their cell phones, including thousands of emails and electronic documents. Still, most districts do not have specific policies regarding employee access to student data on personal devices, let alone policies that would mandate basic security measures, such as requiring such devices to be password-protected and/or requiring employees to immediately report the loss or theft of a cell phone that does or may contain personally-identifiable student information. While these may seem like basic concepts to many professionals, a 2014 Consumer Reports study revealed that only 46% of cell phone users secured their cell phones with a 4-digit or stronger security password/pin or a fingerprint. [4]

Many school employees have cell phones that contain confidential student information in the form of emails, electronic documents, and sometimes even web access to school databases and programs that contain student information. A remote wipe feature is available for most smartphones. This feature allows owners to permanently erase all content from a smartphone remotely if the phone is ever lost or stolen. On most phones, however, this function must be activated in advance, sometimes by downloading a specific app like the “Find My Phone” app for iPhone. Schools should consider a policy that requires all phones that contain or may contain confidential student data to first demonstrate that their phone has a remote wipe option and require assurances that such feature will be used within a specified period of time after a phone has been lost or stolen.

And it is not just unsecured student data that should worry schools. In 2016, a teacher in Columbia, SC, was forced out of her job when she left her unsecured personal cell phone on her desk, unattended. [5] The event happened when she left
the classroom between class periods.\textsuperscript{1} A student picked up her phone, which was not password-protected, went through her photos, found a nude photo that the teacher later explained was taken as a Valentine’s gift for her husband, and forwarded the photo to an undetermined and undisclosed number of friends in the school. The teacher was given the choice to resign or have her employment terminated. The issue became national news almost instantly. Perhaps in response to the media attention, the superintendent issued a public statement (which did not deny that the teacher was forced out) that accused the teacher of making “false statements” about the incident and which provided significant detail about the reasons for the school district’s actions.\textsuperscript{2}

The student was later convicted of computer crimes and voyeurism. Predictably, a few weeks later, the teacher filed a lawsuit against the school district and the superintendent, both in his official capacity and individually, claiming slander, defamation, and breach of contract. In the complaint,\textsuperscript{3} the teacher alleges that school officials never identified any “law, regulation, guideline, policy, procedure, or administrative rule” that was violated by the teacher. The parties, presumably after having reached a settlement, stipulated to a dismissal of the lawsuit with prejudice.\textsuperscript{4}

This case highlights the need for password protection on devices containing potentially sensitive data, which would include most of today’s smartphones. It also highlights the need for carefully-developed procedures, employment mandates, and training related to technology and sensitive information.

\textsuperscript{1} There are conflicting reports as to whether the teacher was in the hallway performing her hall monitoring duties or in an adjoining classroom at the time.
\textsuperscript{2} The full text of the interim superintendent’s statement can be found here: \url{http://wjtv.com/2016/03/05/student-who-sent-nude-pics-of-fmr-union-teacher-arrested-say-police/}.
\textsuperscript{3} Which can be found at: \url{http://publicindex.sccourts.org/Union/PublicIndex/PImageDisplay.aspx?ctagency=44002&doctype=C&docid=CTOzXJ2ykUTIyMrVuCt9tA==}.
\textsuperscript{4} A copy of the Court’s Dismissal Order is available here: \url{http://publicindex.sccourts.org/Union/PublicIndex/PImageDisplay.aspx?ctagency=44002&doctype=C&docid=ONNKguOnbgWEipow4bvz31A==}.
The SC case highlights the importance of cell phone passwords, but it also provides schools with other valuable lessons. School administrators need to take steps to ensure that their staff members are trained with regards to electronic device security and privacy protections. Schools also need to establish and enforce clear, common-sense restrictions, protocols, and procedures regarding, among other issues, the use of personal cell phones in school; the use of personal devices for professional business; the maintenance of student data on cell phones; and required security measures, such as required password protection and mandatory periodic password changes, for cell phones and other electronic devices that do or may contain confidential student information.

In addition to those protections, schools should also establish protocols for providing notice if/when an employee device containing FERPA-protected student information is lost or stolen. Such protocols should include mandatory notice provided to a designated individual within a set period of time. It should also require, where possible, remote wiping of the device, so that confidential student information is not accessible to unauthorized 3rd parties. Schools should consider prohibiting employees from maintaining FERPA-protected student information on any portable electronic device that does not have a remote-wipe option.
RANSOMWARE AND DATA HACKING SCHEMES

Several districts recently learned valuable lessons about the importance of data security and data backups. Unfortunately, the lessons were learned the HARD way. Entrepreneurial criminals with tech expertise have developed a self-replicating computer virus that attacks networks and servers by encrypting all of the data that it finds, essentially making the data unreadable to anyone who does not possess the encryption key. The victim organizations then receive a ransom demand requiring a payout in the form of untraceable bitcoin in exchange for the decryption of the data. If payment is not made, the data is generally destroyed.

In all cases, such a cyber-attack can cause a significant loss of time and resources, as the data is reassembled from back-up servers. Even systems with the most sophisticated back-up servers are bound to experience at least some data loss. For schools with outdated back-up servers; districts with back-up servers that are not properly isolated from the network such that they, too, become affected by the virus; and districts that do not have any back-up data system, the potential loss can be devastating. In those districts, the administration may actually consider giving in to the ransomers’ demands.

In a survey of 540 organizations from the U.S., Germany, the U.K., and Canada, 50% of the organizations reported that they had been the victim of a ransomware attack. [6] Municipalities, schools, hospitals, and police departments are among the many U.S. entities that have been attacked – and have paid the ransom to restore their files. The U.S. Department of Justice reports that its Internet Crime Complaint Center (IC3) received almost 7,700 public ransomware complaints since 2005, totaling $57.6 million dollars in damages, which includes ransoms paid as well as costs related to lost data and data restoration. [7] In 2015 alone, the IC3 reports indicate that there 2,500 cases were reported, and that victims paid out over $24 million in ransom. [7]
In July of 2016, a group of particularly entrepreneurial Russian criminals launched Ransomware as a Service, or RaaS, which provides the software that would effectively enable any individual, regardless of tech expertise, to use and capitalize on these malicious ransomware programs. [8] Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI’s Cyber and Counterintelligence Program in its Boston office, warned that most ransomware programs are so good that, if an entity doesn’t have sufficient back up, there is little that can be done. “To be honest, we often advise people just to pay the ransom.” [9]

For school districts dealing with ransomware attacks, the cost can be heavy regardless of whether the ransom is paid. In the spring of 2016, Horry County School District in South Carolina paid $10,000 for the release of its data, opting for a quick resolution to a problem that otherwise would have resulted in a devastating loss of data. [10] Officials in Bigfork School District in Montana did not pay the ransom, since they had sufficient off-site backup data when their school’s network was compromised, but it took the district a week to get the system back up and running after the attack. For some institutions, the delay that these attacks can cause creates an impossible situation. One hospital in California paid $18,000 to get their systems back online after the malware imposed a two-week stranglehold on their network. [11] Statistics show that 72% of institutions affected by ransomware lost access to their files for at least two days, and 32% lost access for five days or more. In these technology-centered times, a multi-day, complete system loss is significant and can cause substantial disruptions in the educational program.

In 2015, the Swedesboro-Woolwich school district in New Jersey was compromised by ransomware in which the ransom demand was nearly $125,000. [12] Fortunately, in that instance, no student or employee files were breached, and the district was able to restore its system using backup files, but the process took a significant amount of time. In the spring of 2016, ransomware compromised the servers of the Region 11 Education Service Center in Texas, which affected data from
at least six Texas school districts. [13] Ransom was not paid in that case, but, as with
the other instances where backup restoration was used, the backup process took
valuable time. When Oxford School District in Missouri
suffered a ransomware attack, it took the district two
weeks to fully restore the system using backup data. [14]

A quick internet search will reveal story after
story of school districts being affected by ransomware,
and schools are weighing the costs of paying for speedy
recovery of the documents versus engaging in a time-
consuming data-recovery process. In January of
2017, the Los Angeles Community College School District paid $28,000 to
ransomware criminals. [15] In a January 6, 2017 letter, Erika Endrijonas, Ph.D., the
president of the college, issued a memo, which stated, in part:

In consultation with district and college leadership,
outside cybersecurity experts and law enforcement, a
payment was made by the District. It was the
assessment of our outside cybersecurity experts that
making a payment would offer an extremely high
probability of restoring access to the affected systems,
while failure to pay would virtually guarantee that data
would be lost. [16]

Ransomware is a form of data breach, and it is important for schools to
understand their obligations with regards to a breach of any of their systems that do
or may contain information regarding students, employees, volunteers, visitors, and
other individuals. From a legal perspective, schools need to be aware of what
information is maintained in their servers and whether
a breach of such systems would trigger legal mandates
regarding data breach. In January, 2017, NSBA
issued a wonderful resource for schools, entitled: “Data
Breach for Schools: A Legal and Policy Guide for
School Boards.” [17] In that resource, Attorney
Christine N. Czuprynski provides a thorough
discussion of data breach requirements for schools. That resource also provides a helpful chart of legal citations for each state’s data breach laws.

With so many employees, students, and guests connected to a district network at any given time, it is impossible to entirely prevent a ransomware attack. However, as with so many issues, just knowing the risks and being familiar with what ransomware is and how it works, as well as knowing whether the district must comply with data breach laws if such a breach occurs, is sufficient to enable schools to plan for potential attacks and take steps to minimize the effects of a ransomware attack, both from a technology perspective and from a legal perspective.

**What Schools Need to Do:**

There are a number of proactive steps that schools need to be taking in light of these types of attacks. First, be sure to have a good backup system that is separate from the primary network and protected from attacks such as these. Districts should do their homework regarding these systems. One of the most significant problems when there is a backup system in place is the time it takes to restore the backup. For instance, a backup program that restores data at a speed of 10 mbps can take up to 12 hours to upload just 50 GB of data. [53] At that rate, a full, district-wide system restore could take weeks. Investing in a data backup system with a capacity for higher restoration speeds can mean the difference between days and weeks of service disruption.

Schools should also have a plan for public notification if/when these types of attacks occur. At what point will the public be notified? Who will issue the release of information? What information will be provided? Transparency is key in building and maintaining community trust. Finally, schools need to consider legal and practical responses. Was data compromised such that state and/or federal data breach laws would apply? Should the insurance carrier be notified? How and when will law enforcement be involved? Will the DOJ’s CI3 and/or the FBI’s Cyber Crimes division be contacted? Proactively establishing clear and practical administrative regulations and/or protocols will inevitably result in a better response to the issue by the school.
As schools endeavor to integrate more technology into their programs, they are required to rely upon contracted services of technology companies, which may range from startups launching a single, educational app to well-established, global, high-value corporations. In some cases, schools may have the ability to negotiate contract terms, and, in others, they will need to determine whether the fixed terms of a click-wrap agreement are consistent with the school’s legal obligations, particularly with regards to student information privacy and FERPA compliance. Schools need to assume that tech companies do not have a working knowledge of FERPA, the Protection of Pupil Rights Act (PPRA), CIPA, or other school-specific laws. Because the companies do not deal with those laws in the private sector, it is also likely that their attorneys are not familiar with them, either. As a result, most tech contractor agreements do not include language that satisfies those important laws. Because of that, schools and school attorneys need to be hyper-vigilant when it comes to the terms of technology contracts.

In addition to ensuring that the contracts, themselves, pass legal muster, schools also need to be confident that the practices of the company are legitimate and trustworthy and that the technology will perform in the manner expected and will not incorporate undisclosed data-mining processes, tracking cookies, or other practices that may make the school's data vulnerable and/or otherwise compromise the integrity or legal-defensibility of the District’s practices. Analyzing and modifying contract language, in comparison, is a simple task.

---

5 A click-wrap agreement is an agreement with fixed terms to which a user must agree before gaining access to an app or technology product. Most appear in the form of a pop-up button in the app, which contains the language “I accept the terms,” or something similar, and which provides a link to the contractual terms.
Google Apps for Education / G-Suite

Nothing in this world is free. Many people can hear that phrase resounding in their heads as spoken by their parents or grandparents, sometimes as they are uttering the same phrase to their children. Most people inherently understand its wisdom, yet most also still feel the temptation. People simply don’t want it to be true. Still, now, more than ever, current events are reminders that it is a sound mantra for schools to keep in mind when making decisions regarding the use of apps and programs developed by 3rd-party providers. In 2012, Google made news when it was fined $22.6 million to settle FTC charges that it misrepresented privacy assurances. The FTC reported that it was the “largest penalty ever” for a violation of an FTC order. Now, Google has repeatedly come under fire for its Google Apps for Education product. (The name of that product, which bears the unfortunate acronym of “GAFE,” has recently been changed to GSuite.) Google Apps for Education, which was rolled out in 2006, is a free suite of productivity apps, which included apps such as Gmail, Google Drive, Google Docs and Google Calendar.

Several cases against Google regarding its data-mining practices in its Apps for Education suite have been filed. The first, which was originally filed in 2013, resulted in an undisclosed settlement with Google. As part of that case, in a motion to dismiss in the original case, Google acknowledged

---

that it had been scanning and data-mining GAFE users’ emails, a fact that it had not previously publicly disclosed. (EdWeek has published a through summary of that lawsuit, which is available online. [18]) On April 30, 2014, in its official blog, Google acknowledged the practice of data-mining and announced its formal cessation of the practice. “We’ve permanently removed all ads scanning in Gmail for Apps for Education, which means Google cannot collect or use student data in Apps for Education services for advertising purposes.” [19] In December of 2015, a complaint was filed with the FCC by Electronic Frontier Foundation, a nonprofit organization.

So far, at least at the time of the submission of this document for publication in early 2017, the FCC has remained silent on its investigation and has not released any findings with regards to the 2015 complaint. However, the filing prompted U.S. Senator Al Franken to demand some clear answers from Google on the issue. [20] In its response letter, [21] Google admitted to collecting information and data-mining from student accounts, stating that the information is not used within Apps for Education / G Suite, but that the information is used outside of the “core services.” The letter provides examples of non-core services that are excluded from the data privacy protections, which include such basic functions as Google Search, Google Maps, Google Earth, and YouTube.

In early 2016, another class action lawsuit was filed in a California federal court by three University of California, Berkley students, who alleged similar issues as were raised in the 2014 case.8 They attempted to join 876 additional plaintiffs to the lawsuit, as well. In August of 2016, the judge in that case, who was the same

50 YEARS OF SCHOOL TECHNOLOGY

judge that presided over the 2014 case, severed the cases of the 876 additional plaintiffs, allowing them leave to re-file without prejudice.

Along with the upgrade in name of the product, Google also changed the product’s privacy notice. The new privacy notice\(^9\) identifies the data that it collects from G Suite accounts, which includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number of the user;
- log information, including details of how a user used our service, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

The Privacy Notice also states: “We will share personal information with companies, organizations or individuals outside of Google when we have user consent or parents’ consent (as applicable).” Based upon this information, it does not appear that there is anything preventing Google from using the data that it is collecting for commercial purposes once Google obtains consent. Once a student leaves the “G Suite” universe and wishes to roll over his or her email account or other information into a regular Gmail account or other app, conceivably, all of that data that was collected during the student’s “G Suite” days will transfer, as well, this time with the consent necessary to share the information with a number of 3rd-party providers. Over the course of the next few months or even years, the public will likely learn more information, through litigation discovery procedures, if nowhere else, about how the product really works, but, until then, in light of Google’s history and the fact that nothing in life is free, schools should be wary.

\(^9\) Available at: https://gsuite.google.com/terms/education_privacy.html.

“When you're using free services, if you don't know what the product is, you are the product.”

Khaliah Barnes, Director of the Student Privacy Project of the Electronic Privacy Information Center (EPIC)
It remains true that the contract language between schools and 3rd-party tech providers is important, and school law attorneys should encourage schools to submit all such contracts for legal review, so that the attorneys can work with the companies to ensure that the language is compliant with FERPA, CIPA, and other applicable laws. The Google Apps for Education allegations, combined with its recent history of the 2012 FTC findings that the company was using tracking cookies in violation of its agreement with the FTC, brings to light a different moral to the story: a company’s past practices and litigation history matter and should be properly investigated. This is particularly true for large-scale or district-wide contracts, such as large-scale tech purchases and/or school-wide app use (see COPPA section, below) and contracts that may involve access to sensitive student data, such as student data management systems, student email and other electronic communication software, and student grade management software.

School attorneys can aid their clients in vetting potential tech contractors by researching pending and recent lawsuits against the companies. School administrators should be reminded that the fact that a company boasts about strict privacy policies and/or FERPA-compliant practices in its marketing materials and sales pitch does not guarantee that the contract language or company practices will follow suit. Recent experiences have taught us that contracts are not mere technical agreements but also investments of trust. While it is impossible to predict all future improper conduct by contractors, proper vetting is an important step in making a fully-informed decision.

In addition, school administrators also need to be wary of falling into the “neighbor trap.” Many schools enter into agreements with companies that a neighboring school district has used and either assume or are told that the other district’s attorneys have reviewed the contract. Often, school districts that do not have in-house counsel will look to the policies and contracts that have been approved by
school districts that do, assuming that the legal department of those schools has vetted the companies and reviewed the contracts. While collaboration and sharing of information among legal counsel can greatly reduce the amount of time spent on any task, it is never wise to assume that any issue or contract has been subject to legal review by another school’s legal counsel or that the matter has been given sufficient treatment and/or consideration.

Finally, now, more than ever, it is important for schools to have highly-trained IT departments that have the skills and the knowledge to vigilantly protect against security breaches, ensure proper compliance with laws such as CIPA and FERPA, and quickly isolate and address potential issues. A district’s technology director should be a highly-skilled, knowledgeable administrator who is able to not only review the technical aspects of the products and contracts, but who also has broad knowledge of available technology, current industry-specific issues. The technology director should receive regular training in current technology security issues as well as the laws affecting schools and school technology. This administrator should be able to understand the school’s legal obligations, proactively identify potential liability issues, and develop formal procedures and protocols designed to ensure legal compliance and enhance student information safeguards and system security.
Another trend that may cause schools unintended liability with regards to data privacy comes from an unlikely source – school security technology. Computerized systems known as “school visitor management systems” are designed to enable schools to keep track of visitors and prevent entry to those who may pose a risk to students. Some of these systems look like large, freestanding ATM machines standing in the entryway to a school. Visitors insert their state-issued driver’s license or ID, and, if approved, the machine spits out a pre-printed ID badge, often complete with the visitor’s picture. Alternatively, some visitor management systems are not stand-alone machines, but, rather, are purchased as a combination hardware/software package that may include a small, USB ID scanner, a USB badge printer, and the necessary software.

Depending upon the software and the school’s preferences, these products can check visitors’ identifications against state and/or national sex offender registries and other databases, which may include a list of individuals on a locally-compiled list, such as individuals who may be the subject of a protection from abuse order or similar legal prohibitive order. Some of the machines can even be electronically wired to trigger a door lock, allowing those who have provided the requisite information entry into the school’s reception area. These types of machines can be amazing time-savers, but, as with any technology, a little prophylactic legal scrutiny and some legal-defensibility tweaks to the protocols can prevent a great deal of liability. Since these products are not cheap, it is certainly preferable to determine any potential legal
issues before the school purchases a unit, when software modifications and other fixes can be negotiated into the price of the units.

So, what is the problem, exactly? A web search of the issue quickly reveals a multitude of sites singing the praises of these systems. (Of course, most of these are sales websites of companies advertising their version of visitor management systems, each claiming to have the best system on the market.) However, none of the sites, even those providing what appear to be unbiased reviews of the products, mentioned the one crucial legal issue that could make these systems significant: state data breach laws.

What many school administrators may not realize is that, in many states, the use of these systems may cause all of a district’s visitor information to fall within state data breach laws, which would not otherwise have been applicable to that district’s visitor information had the school reviewed it for the purposes of permitting entry and not maintained it or had tailored the types of information that the system retains to avoid falling within the data breach requirements. Data breach law compliance is not new for schools. In fact, most schools’ employee records already fall within those laws, due to the types of information that employers are required to collect and maintain for tax purposes. Depending upon the state, many schools fall within the boundaries of their data breach requirements due to the types of student data they

10 Protecting Personal Information: Managing and Preventing Data Security Breaches
August 2016 – Inquiry & Analysis – by Jill Greenfield [23]

© 2017 Erin D. Gilsbach, Esq.
retain, as well. An article in the August 2016 issue of COSA’s Inquiry and Analysis, “Protecting Personal Information: Managing and Preventing Data Security Breaches,” by Jill Greenfield, [23] provides an in-depth look at state data breach laws, how they work, the penalties for failure to comply with the legal requirements, and their more general implications for schools. The previously-referenced NSBA guide, “Data Breach for Schools: A Legal and Policy Guide for School Boards” [17] is also very helpful. Still, while many schools are already subject to these laws due to the information that they collect on employees and, sometimes, students, performing data-breach notifications for several hundred employees and students is significantly less costly and administratively burdensome than sending data-breach notices to the potentially tens of thousands of visitors that schools receive every year.

It is imperative for schools to be aware of the information that they are collecting regarding school visitors and, where it is possible to do so while still maintaining the primary benefits of the school visitor management system, tailor the information retained to avoid unnecessary and costly data breach law implications. That may mean using the system to permit entry, but not retaining the data on file. Alternatively, in some cases, negotiating an alteration of the software to black out the driver’s license or state ID may solve the problem. The bottom line with this technology is that schools should enter into contracts with these companies fully understanding the issue. If they do, they may be able to make smarter choices about which products to purchase, what add-ons/modifications to request, and how to use the technology in a manner that balances the school’s safety interests while being mindful of the costs associated with compliance with state and federal data breach laws.
The Children’s Online Privacy Protection Act (COPPA) has been drawing attention from the school attorney and school administration crowds lately. This is primarily due to the fact that the law, drafted by Congress before the turn of the century, does not anticipate the fact that students might be using the internet or other “online services” in school. This section attempts to analyze the issue and provide some guidance as to what schools need to do with regards to their use of online programs and apps that collect student information.

The Basics of the Law

The requirements of the law, itself, seem simple: operators of websites or web-based programs/applications must get informed consent before they are permitted to collect personal information of students. Here is the primary statutory requirement:

[COPPA’s implementing regulations must] require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child—

(1) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator’s disclosure practices for such information; and
(2) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

The relevant provision of COPPA’s implementing regulations state the following:

General requirements. It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a

---

11 The author strenuously emphasizes the word “attempts,” due to the fact that the entire issue is a nightmarish conflagration of statutory shortcomings and nonsensical bureaucratic interpretations and directives.
manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).\textsuperscript{12}

The term “verifiable parental consent” is important in the school analysis. In the regulations, the measures that are required to be taken to ensure “verifiable parental consent” are fairly onerous:

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

\textsuperscript{12} 16 CFR § 312.3. Subsections (d) and (e) appear to be significantly outside of the scope of the statute, and, therefore, are ripe for a legal challenge on that basis. The FTC’s overstepping of authority in this context is informative, these provisions are not directly related to the issue at hand, so they are not specifically addressed here.
(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) Provided that, an operator that does not “disclose” (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.13

**Does COPPA Apply to Schools?**

Before continuing further, it should be noted that neither COPPA, itself, or its implementing regulations, directly apply to schools. COPPA applies to operators of websites of commercial online services that collect or maintain personal information

---

13 16 CFR § 312.5(B).
from or about the users of such sites/services. In January of 2015, the FTC published an online article in its “Business Blog” that provided the following information, renewing concerns regarding the FTC’s view of COPPA and schools:

Schools – which are usually part of the local government – don’t fall within the legal definition of who’s covered by COPPA because they aren’t commercial “operators.” That said, schools sometimes allow, or even require, students to use sites and services that are covered by COPPA and which must provide notice and get verifiable parental consent. 

While not expressly stating that COPPA applies to schools, this renewed prior concerns regarding the interplay between COPPA and public schools, and the FTC’s expectations. Later that spring, on March 23, 2015, the FTC updated its FAQ on COPPA, which currently serves as the latest update to that guidance. That guidance document, which is discussed in detail, below, potentially entangles schools in an ambiguously complex, amorphous mass of non-statutory, non-regulatory expectations of the FTC despite the fact that the law is not directly applicable to them.

The Issue

The crux of the COPPA issue, for schools, is that none of COPPA’s provisions, or those of its implementing regulations, addresses the issue regarding what consent is required or what procedures should be followed when a school wishes to have students use a website or online service that is covered under COPPA. Schools often use online resources to monitor a student’s progress and even assess students; teachers are increasingly requiring students to use different types of social media in projects and assignments, specific apps and online programs are regularly used in special education programming to target specific needs; and bring-your-own-device and 1:1 technology programs (see discussion of that topic, below) are increasing the use of apps and online services in schools. Thus, the question arises: when the school

---

15 This practice poses potential legal defensibility issues that are outside of the scope of this discussion but should be carefully considered by schools and school attorneys.
wishes to use a program or service covered by COPPA, how do the COPPA-covered operators of those programs obtain the consent in these situations, when parents may not even be aware that the students are using the programs/apps?

A specific carve-out or exception for operators who contract with schools would have been a logical addition to this law, however, no such provision was added. This puts schools, operating with varying degrees of statutory and common law “in loco parentis” authority, in a difficult position. The collection of parental consent, under COPPA, is not the responsibility of the school and, in any case, would be too unwieldy for the school to accomplish in the statutorily-required manner set forth, above, for large numbers of students. COPPA’s definition of “parent” is vague (arguably not even meeting the basic requirements of being an actual definition), and it does not contain the “individual acting as a parent” language that makes FERPA’s definition so workable in a school setting. The definition reads: “Parent – The term ‘parent’ includes a legal guardian.” 16 This skeletal definition is repeated, verbatim, in the law’s implementing regulations. 17

So, to recap, there exists a law that requires operators of programs/apps to obtain express, regulatorily-specific (and burdensome) parental consent for programs/apps commonly used by schools to collect student information, but the program operators do not have access to the parents, since the programs/apps are being used in the schools. Further, the schools, who are not subject to and do not have any requirements under the law, are directly affected, since, without the consent, the operators cannot provide the programs that are needed by the schools. Indeed, the problem is better summed up as follows:

---

17 16 CFR § 32.2.
The FTC Weighs In

In the absence of applicable law or a legal theory that resolves the school problem in a manner that is supported by the actual language of COPPA, FTC officials have made a bold decision to take a novel approach to finding an interpretation of the law that would properly address the issue... they just made one up.

1. Can an educational institution consent to a website or app’s collection, use or disclosure of personal information from students?

Yes. Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. In these cases, the schools may act as the parent’s agent and can consent to the collection of kids’ information on the parent’s behalf. However, the school’s ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.

This answer, as well as the manner in which it is affirmatively stated, making no mention of the fact that it has absolutely no legal basis and is, indeed, contrary to the statutory and regulatory provisions, would surely have garnered a failing grade for a law student analyzing the issue on an exam or a pink slip for a young legal associate asked to provide a legal analysis of the question for a partner in a law firm. The FTC, however, answers the question as if it is plainly contained in the regulatory language, itself, and even provides exceptions based on the purpose of the collection of the information (commercial vs. non-commercial) to its completely fabricated ‘education exception’ to COPPA’s very clear parental consent requirement.

The January 2015 blog post provides some explanation as to the basis on which the FTC’s guidance is formed, but that is no less unsettling. The FTC’s answer comes

---

18 Or, perhaps more plausibly, a gaggle of unpaid summer interns...
from its own comments in the originally-issued 1999 version of the final regulations. Those comments read:

Numerous commenters raised concerns about how the Rule would apply to the use of the Internet in schools. Some commenters expressed concern that requiring parental consent for online information collection would interfere with classroom activities, especially if parental consent were not received for only one or two children. In response, the Commission notes that the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents’ agent in the process. For example, many schools already seek parental consent for in-school Internet access at the beginning of the school year. Thus, where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator’s collection, use, and disclosure practices, the operator can presume that the school’s authorization is based on the school’s having obtained the parent’s consent.

In other words, the FTC’s non-regulatory guidance is based, not on law, but on other FTC non-regulatory guidance. It is at this point that the faint-of-heart might greatly desire to simply ignore the issue entirely, but school attorneys are tasked with protecting the clients they serve and recommending the most legally-defensible solutions possible, so we press on.

The FTC’s 1999 comments demonstrate a few really important points: 1) even back in 1999, there was significant concern about the impact of the language of the COPPA regulations on schools; 2) the FTC, both then as well as now, does not appear to have a clear understanding of schools or their parental consent requirements; and 3) the FTC was aware that there was a need for a school exception, and they did not add one. The reasoning for the last point may be because the addition of a specific exception for schools would have exceeded the scope of the original statutory language, a well-established regulatory no-no, but that is unlikely, given the clear overstepping of their authority in other sections of the regulations. (See footnote,
above, in “The Basics of the Law” section regarding COPPA’s implementing consent regulations.  

It should concern schools and their legal counsel that, despite not including a specific exception or carve-out in the regulations, the FTC is now operating as if there is one. There is nothing in COPPA that would suggest that the use of an “intermediary” is permissible under the law, much less that the requirements for consent, if obtained by an intermediary, could be substantively modified to such an extent that a parent’s consent that their child be allowed to use the internet at school would satisfy the very specific informed consent that is required by COPPA and its regulations. The FAQ imposes burdens on schools that greatly exceed their obligations under the law (none), and, to make matters worse, they are not at all clear about their expectations regarding the specific responsibilities of schools in obtaining consent on behalf of the covered “operators.”

**Enforcement of COPPA**

If COPPA were enforced only by the FTC, the issue might be less significant and could even be looked upon as the equivalent of a federal policy statement on the FTC’s enforcement intentions. However, the FTC is not the sole entity tasked with enforcing or authorized to enforce COPPA. States and other federal agencies have jurisdiction over COPPA enforcement actions. Indeed, the FTC’s FAQ points out that Texas and New Jersey have already brought COPPA enforcement cases in their states. Under COPPA, there is no specific provision that would require these other enforcement entities to give deference to the FTC’s non-regulatory guidance, and since the guidance is contrary to the actual law, it is unlikely that they will.

**The Bottom Line:**

So, what are school attorneys to make of all of this information? The bottom line is that the law, as well as the FTC’s interpretation of it, is a mess, but there’s nothing

---

19 The author would love to point readers directly to this particular footnote, but she is tired of writing about COPPA, and her children are fighting, so the readers will just have to find it themselves.
50 YEARS OF SCHOOL TECHNOLOGY

the schools can do about that. What really matters is putting the guidance into context for legal and practical purposes and determining a course of action that affords schools the least amount of liability. Schools need to wade through the hype and truly assess the legal risks, which must be clearly identified before trying to craft viable mechanisms to protect the schools. Since school districts are not statutorily required to comply with COPPA, the monetary penalties in COPPA’s enforcement provisions are not directly an issue.

Since school districts are not statutorily required to comply with COPPA, the violation of COPPA by an online provider with which a district contracts poses little to no legal liability for the district. The FTC’s proposed solution, however, particularly because it has no identifiable legal basis, may pose some potential risk, since it imposes on schools’ responsibilities of obtaining parental consent that do not exist in the law and are legally beyond the scope of what the schools may lawfully do. Still, such risk is likely minimal or nonexistent in states with broad tort claims protections. This liability would necessarily stem from a claim by a parent that a child suffered harm as a result of the school’s improper assumption of parental authority under COPPA (which following the FTC’s guidance would inevitably cause schools to do), improper application of the FTC’s guidance with respect to the manner in which consent was provided, or other similar claims. Attorneys should review their states’ sovereign immunity protections to ascertain whether their schools would be protected from such claims. If they would not, schools will need to weigh the benefits of the convenience of being able to provide blanket notice and passive-consent to parents against the potential for liability in a related tort claim.

It is possible that the electronic services providers with which the districts might contract, who are legally obligated to obtain the parental signatures, may try to seek legal recourse from the districts if they are found to be in violation of COPPA based on what they believed the districts did or should have done. Thus, the contract language between the districts and the providers, in those cases, will be important. Districts should insist upon language that spells out specific expectations of both
parties with regards to what steps, if any, districts will take to provide passive notice. Having the districts obtain active, specific parental consent should never be on the table since they are not legally required to do so and their collection, maintenance, and enforcement would be too onerous. Districts should strike any COPPA-related indemnification language that would make the districts legally liable for any loss on the part of the contracted service/program provider (“operator”) for COPPA-related judgements or enforcement actions. Districts may wish to insist on specific language that relieves them from any COPPA-related liability.

**The True Risk:**

While COPPA issues should be considered and addressed by schools, they should also be focused on two issues that *DO* directly apply to these types of services – compliance with FERPA and the Protection of Pupil Rights Act (PPRA). Entities that are subject to COPPA are, by definition, collecting information from students. Where the districts are entering into relationships with these entities, they need to ensure that such collection of information is done in a manner that is consistent with FERPA and the PPRA.

Schools need to be aware of COPPA and its related risks, but they need not lose sleep over potential liability issues. The law is simply not workable, but the FTC’s fixes are not sufficient, either. Schools should establish procedures to provided notice to parents regarding the apps, websites, and/or online services that fall under COPPA and for which they have entered into an agreement with the service providers. Schools should also, however, protect themselves by not permitting any language in such contracts that would implicate them in any COPPA-related liability.

Most importantly, since schools know that these apps, websites, and online services that fall under COPPA involve the collection of student information, they need to be sure that the information collected is in compliance, first and foremost, with the Protection of Pupil Rights Act (PPRA) and with FERPA, since those are the laws that *DO* apply directly to the schools.
BIOMETRICS

USE OF BIOMETRICS IN PUBLIC SCHOOLS

Most people are unaware that biometric scanning in public schools has been around for well over a decade. In 2003, one vendor stated that the company had fingerprint-scanning systems in 45 school districts in the U.S., which scanned approximately 250,000 individuals daily. [25] By November of 2010, another vendor reported that 2,758 school cafeterias in 27 states were using their systems, including 112 of the school systems in North Carolina. [25] In fact, fingerprint scanning technology continues to be a high-profit area for EdTech vendors.

The use of biometric technology in schools is not limited to the lunch line. At the Bais Yaakov School for Girls in West Hollywood, CA, a private school educating 300 high schoolers in an affluent neighborhood, the main school doors automatically open for students who are authenticated through state-of-the-art facial-recognition and body-movement-recognition technology accessed by cameras placed above the front doors. [26] While this may seem like high-tech science reserved for the elite and sci-fi movies, as early as the 2002/2003 school year, a handful of New Jersey public schools, through a grant from the National Institute of Justice, tested – and liked – iris scan technology to control access for parents, teachers, and staff members. [27]
Computer companies have also integrated biometric readers into their technology, offering fingerprint reader technology on common items like the computer mouse and laptop touchpad. iPhone users now use this technology daily when accessing the information stored on their phones.

**DATA PRIVACY CONCERNS AND STATE LEGISLATIVE RESPONSES**

Parents and lawmakers, alike, have raised data privacy concerns with the use of biometric technology in schools. In fact, several states have passed laws regarding biometric data and schoolchildren. In Florida, Governor Rick Scott signed into law the “Education Data Privacy Act” on May 12, 2014, that would prohibit any K-12 institutions from “collecting or retaining ... biometric information of a student, parent, or sibling of a student.”[20] [28]

Examples of biometric information in that law include fingerprint scans, palm scans, retina or iris scans, facial geometry scans, and voiceprints. The law allowed for a one-year grace period.

---

for schools that were then using hand scanners in their cafeterias, but all other biometric data collection was required to immediately cease. [28] It is unclear whether this language will prevent some of the current fingerprint identification technology that does not result in the collection of actual fingerprint information but, rather, converts information from a fingerprint into a series of data points that are then linked to the student’s records but allegedly, according to the tech companies that sell them, cannot be turned back into or reveal information about the student’s actual fingerprint (discussed further in the next section).

Illinois has a law, SB1702,\(^{21}\) which requires school districts to have a policy before collecting any biometric information from students, prohibits the sale or disclosure of biometric information, and requires parental consent before any children are scanned. Officials from District 304 in Illinois indicated that they have approximately 6,000 students using biometric fingerprint scanners in the district’s cafeterias and that they have had no complaints from parents. [29] Despite the legal protections, the practice still concerns many. Ed Yohnka, spokesperson for the ACLU-Chicago, stated: “I think it undermines the notion of really thinking about the importance of biometrics as a matter of privacy. I think in this age, when so much is available and so much is accessible online about us and there is all this information that floats out there, to begin to include in this one’s biometrics, it really does raise some legitimate concerns.” [29]

Several other states, including New Hampshire\(^{22}\); Louisiana\(^{23}\); and Arizona\(^{24}\), have enacted data privacy laws that specifically address biometric data. In Louisiana, Arizona, and Illinois, parents must consent prior to the collection or use of biometric data. The New Hampshire law completely bars the collection of biometric data of students.

\(^{21}\) 105 ILL. COMP. STAT. ANN. 5/34-18.34(b)(1)
\(^{22}\) N.H. REV. STAT. ANN. § 189.68(I)
\(^{23}\) LA. STAT. ANN. § 17:100.8(B)(2)
\(^{24}\) ARIZ. REV. STAT. ANN. § 15-109
INFORMING THE SCHOOL COMMUNITY OF USE OF BIOMETRIC TECHNOLOGY

Of course, the manner in which schools roll out this technology matters, as well. The Florida Senator who introduced the initial “Education Data Privacy Act” bill discussed, above, stated that she did so when she discovered that Polk County was scanning children’s irises before allowing them onto school busses without notifying parents or obtaining parental consent before doing so. In September of 2016 in Oregon City, OR, parents were shocked and angry to find that their local school district had recorded their children’s fingerprints and were requiring the children to scan their fingerprints to pay for their lunches.

In that district, however, the children’s fingerprints were not actually being recorded or maintained. The district was using a technology that protects the individual privacy of the student while allowing the District to use fingerprints to establish a reliable data point for schools to use to verify identity. The District’s website stated: “The scanner examines a few points of a fingerprint and generates unique numbers based on those points to create a secure key called a ‘string.’ Only the string value is retained for reference back to the student. These numbers cannot be converted into an actual fingerprint image; fingerprints cannot be regenerated or reproduced for any purpose.” If this is the case, then theft or disclosure (intended or unintended) of a student’s actual biometric data – his fingerprint pattern – appears to be impossible.

This seems to be the type of system that could ease the mind of even the most staunch privacy advocates. So, why didn’t it? Perhaps it is because the district simply did not adequately prepare the public for this new technology. In the news video associated with the article, the concerned parents had one thing in common: all of them appear to have discovered the district’s use of the technology through their children. With so many legitimate privacy concerns being raised,
schools need to tread lightly around these issues and implement new biometric technology only after a prolonged period of conditioning of the public and after putting all of the necessary safety and data privacy safeguards into place through the implementation of proper policies and protocols designed to protect the privacy of the students.

Another problem could be that although the school was trying to assure the public that it was using, but not actually collecting, fingerprints, that is a difficult concept to understand without sufficient background information. Any claim that the fingerprints are used, but not collected, and that fingerprint data is obtained, but cannot be used to regenerate a whole fingerprint, will need to be explained in detail in a manner that parents can take home to review and process. Even that, however, may still not be enough. A quick internet search can produce what appears to be legitimate data refuting the proposition that the data cannot be used to regenerate a fingerprint. Schools will need to provide assurances regarding how they are keeping the information, what else they may be using it for, and how and when it will be destroyed when it is no longer necessary. Claims that the data collected could not be useful to a 3rd party, without assurances that the data will, nonetheless, be safeguarded, may actually make the public more wary of the initiative. Such over-confidence in the technology being used makes the district sound too cavalier about the data it collects.

**Right to Opt Out a Good Idea, Even When Not Legally Mandated**

The Akron School District in Ohio has been using fingerprint scanners in their cafeterias since the 2003/2004 school year. When that district rolled out the program, it offered the parents the option to opt out of the program. The District reports that almost all of the parents chose to continue in the program. That appears to be fundamentally different from the approach taken in Oregon City. Parents were not given the chance to opt out prior to the roll-out of the program (or, at least, the option to opt out was not widely publicized among the parents).
Indeed, the message is only as effective as the mechanism that presents it, but, in cases like this, with significant data privacy concerns, getting the right message across can mean the difference between a community that is comfortable with the district’s plan and on-board with an idea or a community that lashes out against the district for acting without full transparency and consideration on an issue that has potentially serious privacy ramifications. It is the latter community in which a district will find itself wading in the mire of legal challenges and compliance complaints.

School administrators and attorneys need to work together on this issue. School administrators need to be aware of state privacy laws that may affect or even prohibit a school’s use of biometric technology in schools, and they need to work with their attorneys prior to any collection or use of biometric data to ensure that their processes and procedures are legally sound, paying close attention to any applicable state mandates.

Notice is important, as well. Neither parents nor school attorneys should be made aware of a biometric data collection initiative after it happens. School attorneys can assist with legal compliance regarding the data collection, ensure that any necessary policy changes are made, and confirm that parental notification is done in a manner that is consistent with any applicable state laws.

Districts should be wary of sales pitches by tech companies that sound too good to be true – especially on the important issue of student privacy. School administrators should be fully aware of what is being collected, how it is being collected, where and how it is being maintained, and how it will be used. The technology should be properly vetted to ensure that the administrators’ expectations and understanding are in line with the way that the technology actually works. In addition, all such processes, once they have been confirmed from a technology standpoint, should be vetted by the school’s attorney to ensure full compliance with all applicable laws. Administrators
need to fully understand the technical process involved to such an extent that they are able to accurately explain it to parents and provide meaningful reassurance that the technology is not violating a student’s privacy rights.

School districts also need to be deliberate and careful about the time and manner in which the initiative is rolled out and when and how the parents will be notified. Schools should include their attorneys in this process. Because parents may need time to understand the technology, and a written explanation of the system and processes being used may be very helpful in alleviating fears. Explanations and information that is provided to the parents, whether in writing or through some other means, should be thoroughly reviewed to ensure that it is consistent with the technology and technological processes being used as well as compliant with federal and state privacy and student data collection laws.
In today’s world, digital technology has made video and audio recording so simple and accessible, it is easy to overlook some of the most basic legal and practical digital recording issues until there is a big problem. Such recordings, however, are causing some big stirs and, in this era of YouTube stardom and predatory media outlets waiting to find their next “shocking” or “heart-wrenching” story, digital recordings can be extraordinarily powerful and, in many cases, damaging. Recording technology issues have been making their way to the forefront of the special education law scene, as well, with parents demanding the right to record IEP meetings; attempting to use illicit classroom video or audio recordings as FAPE violations; and utilizing devices with audio broadcasting capabilities, like AngelSense and similar devices, to record communications within the school and/or monitor their child’s education.

**Student Recordings in School**

Due to today’s technology, more events are being captured on video than ever before, and school is no exception. A simple YouTube search reveals a seemingly-endless supply of videos recorded by students with such titles as ‘raging teacher’ and ‘teacher flips out.’ There are even video compilations – some complete with background music and screen graphics. Can schools that permit the possession of electronic devices lawfully curtail recording on school grounds? If so, to what extent? Do schools have any recourse when student-filmed videos of employees and/or other students get uploaded to YouTube and other media sites? These are the questions that administrators are asking, and school attorneys need to understand the factual issues as well as the answers.

In Florida, an 11-year-old 5th grade girl was suspended for recording a teacher who was allegedly harassing another student. [33] The student was suspended for
recording the event in violation of “the law” and board policy, and the teacher was dismissed. The story caught fire with TV news media and subsequently grew even further in the blogosphere, and a very public discussion of the District’s policy and its erroneous interpretation of Florida’s wiretap law (see further discussion regarding wiretap laws, below) ensued. By the time the District reversed course and lifted the student’s suspension, the public damage had been done.

In North Carolina, a parent purchased a recording device online and sent it to school with her child on the specific advice of her son’s psychiatrist. Her son had been upset about his special education class, particularly his special education teacher. He recorded 4 hours’ worth of the school day, on which the teacher can be heard yelling things like ““You want something to happen! But I’m tired! So, somebody might just get hurt and I just might go to jail!” In that case, the local CBS station repeatedly contacted the District, which refused to discuss the matter, citing confidentiality in personnel matters. The specific formal action that was taken against the teacher, if any, is not publicly available, but it can be confirmed that the teacher was not dismissed as a result of the incident. The news station was, however, able to find another parent of a child in the same classroom, whose shocked and disgusted reaction was described in the news article. The next sentence stated that “[a]fter a fight in the classroom her son came home with a gash in his head.” There does not appear to be any correlation between the two incidents, and there is no further discussion with regards to the other child or the fight, but the reader is left with the distinct impression that this is just another one of the many horrors children are being subjected to in their classrooms that is being kept from parents and other authorities. Once again, the public image damage has been done, and administrators following the story take steps to curtail recording in the classrooms.

While most student-recorded videos are created for non-legal purposes, there have been instances where students, often with the knowledge and, in some cases, encouragement of their parents, have recorded videos expressly for the purpose of obtaining evidence for a lawsuit. In 2011, a 15-year-old sophomore boy in a California
public high school began making hours of unauthorized audio recordings of his AP History class. The student, who was a conservative Christian from a conservative Christian family, was recording the classes to gather evidence that his teacher was using his classroom to promote his anti-Christian views. Once he felt he had enough evidence, his family filed a federal lawsuit.

The complaint asserted that the student’s rights under the Establishment Clause have been violated by a practice and policy hostile toward religion and favoring irreligion over religion. The student argued that the teacher’s "only purpose in making these statements is to make sure that the students who sit before him as a captive audience understand that religion is irrational." The plaintiff’s case cited 22 statements made by the teacher that he believed showed the teacher’s anti-Christian teaching. Many did appear to be inflammatory when considered alone and out of context, such as “[w]hat was it that Mark Twain said? ‘Religion was invented when the first con man met the first fool’; and "when you put on your Jesus glasses, you can't see the truth." However, the court evaluated each one in context and found that only one violated the Establishment Clause. Even in making that determination, the court stated, in an unusual “afterword” section at the end of the opinion, that it sought to protect both the student’s and the teacher’s rights.

It seems clear that the Court felt that the teacher’s purpose in making such incendiary remarks was to get the students thinking. In fact, the 9th Circuit appellate decision, which upheld the lower Court’s decision but found that the teacher was not liable under the legal theory of qualified immunity, noted that this purpose was admitted by the teacher in a letter sent home over the summer, prior to the start of the school year, to all students enrolled in the class. The 9th Circuit opinion,

26 In a discussion with his class regarding another teacher in the school who aggressively espoused and taught creationism, he recounted a conversation with his administration where he said “‘I will not leave [the other teacher] alone to propagandize kids with this religious, superstitious nonsense.” It was this statement that failed all 3 of the prongs of the Lemon test. (See Lemon v. Kurtzman, 403 U.S. 602, 91 S.Ct. 2105, 29 L.Ed.2d 745 (1971)). The Mark Twain and “Jesus glasses” quotes were determined to be academic studies of religion being used as a mechanism of societal manipulation, not necessarily the teacher’s personally-espoused views of religion.
27 C.F. ex rel. Farnan v. Capistrano Unified Sch. Dist., 654 F.3d 975, 985-86 (9th Cir. 2011).
quoting directly from the letter, pointed out that the teacher was up front in stating that “[h]is pedagogy is intentionally provocative in order to elicit responses from his students and to help them develop critical thinking skills.” The Court went on to state (again quoting directly from the teacher’s own words to his students):

> He encourages students to ‘question and try to come up with a[n] analysis of what is true [and] is not true, from [a] historical perspective.’ Corbett told his AP Euro students that, “it is completely safe, in here anyway, to disagree with me, make a comment, whatever you want to say. I don’t care. The only thing you’ll get from me in response is, ‘On what basis . . . have you come up with this particular perspective?’ . . . I mean, there’s almost always more than one point of view on stuff.”

In short, the student was in possession of recordings that contained a number of incendiary comments that, on their face, when taken out of context, sound incredibly anti-Christian. The teacher’s saving grace, in this case, appears to have been the court’s deliberate consideration of each comment in context. What would have happened, though, if the student had not maintained all of the original recordings, but, instead, edited the recording to compile only the series of the most inflammatory statements, not the contextual discussions? What if, instead of audio, the student had video?

The recordings, in this case, subjected this teacher’s practice to a scrutiny that would not have been possible twenty or thirty years ago. In 2007, when this student made his recordings, the iPhone had just made its debut, but it did not have any type of video recording capabilities. Today, the student would have been able to edit the video right on his phone and, if he so desired, make a YouTube compilation of the clips set to music with graphic effects. Would the result have been different if the court had only a video like that to review? It is very possible that, in that case, the decision would have come out very differently.

The court gave the teacher a great deal of deference when it heard the actual lessons. It is clear that both courts were convinced that this was a good teacher who
was trying to get his college-bound students to think critically. The district court inserted large sections of the transcript into the opinion, itself, to justify its decision. Many of the arguments that the court made regarding the context of the statements would not have been available, had the student recorded clips of conversations or electronically modified the recordings to reveal only snippets of quotes and what might, out of context, sound like exceptionally inappropriate remarks. With so many inflammatory, boundary-pushing statements, had the court not heard the teacher’s effective methods for itself, i.e., the rest of the recordings it would have been very possible for the court to fail to fully understand that there may be a context in which all of those facially inappropriate and biased comments could have passed any prong of the *Lemon* test, let alone all three.

**Policy Issues**

As a result of these and many other similar incidents, schools are rightfully looking for ways to curb and/or eliminate recording in the classrooms. However, this can be extremely difficult, particularly for schools that have a difficult time enforcing existing no-cell-phone policies and, in particular, for schools that have 1:1 and Bring-Your-Own-Device programs (see more detailed discussion, below). In the late 1990s, when smaller, affordable personal cell phones became widely available on the market, most schools banned them outright, and several states even made it unlawful for students to have them in schools. [35] Then came Columbine, followed by 9/11. The panic of not being able to reach a child during a time of national crisis, and the possibility that a student with a cell phone during an active shooter attack might save lives, led to great public pressure to allow phones on campus – pressure which still exists to this day. Schools gradually moved from complete cell phone bans to “in the locker” or “powered off and out of sight” policies. As cell phone use has become increasingly common, those policies have had a tendency to become very loosely enforced. Some schools left it up to the classroom teachers, with some teachers strictly prohibiting them and others more lackadaisical in their approach.
Today, a close investigation of the cell phone policies of any particular district is likely to expose significant fluctuation in cell phone rules and enforcement of existing rules and policies from building to building, classroom to classroom. A comparison of any school’s policy language and the actual practices with regards to cell phones is highly likely to reveal vast inconsistencies. This, then, becomes a day-to-day headache for administrators, who are tasked with enforcing rules that don’t always exist and commonly end up establishing a variable record of enforcement, with different standards applying to different students, based upon a variety of undocumented factors and variables. (Did anyone get hurt? Does this teacher let them do this all the time? Is that teacher being overly strict? Is this a “good kid” who just couldn’t resist the urge to text? etc.) From a legal perspective, this approach could ultimately lead to liability in the form of a discrimination lawsuit, with parents/students claiming the disparity in treatment was based on race, disability, gender, etc.

This approach, however, sets the stage nicely for serious legal and public image problems in high-stakes situations. For instance, in the case of the Florida 5th grader who videoed misconduct by her teacher, the school’s administration immediately sought to enforce their school’s video policy, despite the fact that it was based upon a wiretap law that was plainly not applicable to the situation (see the “Wiretap Law” discussion in the next section). This is a foreseeable reaction for a school, regardless of how justified this video may have been. Even where policy language is not directly applicable to a situation or does not exist to address the issue, administrators know that students video teacher behavior all day with the intent of hoping to catch something that they, in turn, can take to the district’s administration and use to get their teacher reprimanded. That type of atmosphere would result in an extraordinarily negative working environment for teachers, which may, in turn, result in employment conflicts, union issues, collective bargaining issues, etc.

There is a solution, however. Schools need to have policies and procedures that do apply to these situations and that are legally defensible. Schools may lawfully
establish no-recording policies, provided that they leave open an exception in cases where such recording may be required by law in order to ensure parental access to meetings and/or school information (see “Prohibiting Recording at IEP Meetings” section, below). Where such a policy exists though, schools need to be careful to enforce it uniformly and accurately. School administrators are opening the door to potential liability when they are discretionary in their enforcement of recording laws. Still, enforcing strict “no recording” policies in today’s world of ever-present personal electronic devices is no easy task.

**Wiretap Laws**

In the Florida case, as districts do in many such cases, the district clung tightly to the state wiretap law as justification for its discipline of the 12-year-old. State wiretap laws vary significantly from state to state. The chart found in Appendix A of this Document provides the legal citation for each state’s wiretap law as well as information regarding whether each state requires the consent of “one party” or “all parties.” In “one party” states, consent need only be obtained from one of the participants in a conversation or other communication. In contrast, “all parties” states, consent needs to be obtained by all parties involved. (This is sometimes referred to as two-party consent, due to the fact that both parties in a conversation between two parties would need to consent, but the term “all parties” is more accurate in cases where more than two people are communicating.) If a state has a “one party” wiretap law, using that law as justification for a no-recording policy is tenuous, at best, since the individual making the recording generally serves as being one of the “parties” at issue under the law. Thus, the consent requirement is satisfied.

In addition, there is another reason why state wiretap laws may not be helpful. That is because most of them only apply to situations in which there is a reasonable expectation of privacy. In the case of a student making a recording of something going on across the room in a classroom full of students, it is highly unlikely that the subject being recorded has any reasonable expectation of privacy, due to the fact that
their actions are taking place in a very public setting. In the Florida case, where the 12-year-old student recorded her teacher’s comments, she was recording comments that were being made aloud to the entire class. There was no expectation of privacy with regards to the teacher’s comments. Thus, the wiretap laws would not have even applied to the recording at issue.

That is not to say, however, that state wiretap laws are never implicated, however, or that references to wiretap laws should be removed from policies entirely. For instance, if the student is making a recording of something happening across the room, but, in the process of doing that, the student’s ultra-sensitive microphone catches part of a whispered conversation that he or she may not otherwise have overheard, there may be wiretap law implications. In such a case, there may be a violation of the state wiretap laws. Likewise, if the teacher leaned down to whisper something to that student only, and the microphone caught what was said, but the rest of the class did not, the teacher would have likely had a reasonable expectation of privacy in that situation, and the recording would have been a violation of the law.

It is not the reference to a wiretap law within a policy that is inappropriate. References to wiretap laws can prove to be a meaningful deterrent to surreptitious recordings. Despite the fact that the school is not tasked, under the law, with enforcing the wiretap statutes, a parent or student is more likely to think twice about recording if their actions may have criminal repercussions. For this reason, referencing wiretap laws, as well as emphasizing their criminal penalties and consequences, in policies and notices may be an important deterrent tool. Schools need to be careful, however, to avoid language that states or implies that it is the school, itself, that enforces state wiretap laws. Likewise, schools also need to ensure that their policies ensure a potential for a legally necessary exception to the recording prohibition, such as for a parent who requires recording as a necessary accommodation under the IDEA (see “Prohibiting Recording at IEP Meetings” section, below).
References to wiretap laws in school policy may have a deterrent effect on those seeking to privately record school conversations without permission, but school officials need to understand that they do not have the authority to enforce wiretap laws. References to wiretap laws should be made in policies and parent and student notices should not give the impression otherwise. Schools should review such documents to make sure that their references are correct, that they are not providing misinformation, and that they do not rely exclusively on the wiretap law for prohibiting conduct where those laws may not even apply, such as in a circumstance where there is no expectation of privacy. References to wiretap laws should be a tool that schools can and should use, where appropriate, for its deterrent effect, not the exclusive authority to be used by schools as a “catch-all” excuse for disciplining and prohibiting all unsanctioned recording.
**Prohibiting Recording at IEP Meetings**

Many of the recording issues arise in the context of IEP meetings. Parents make a request to record a meeting, a school employee knows/suspects that a parent is secretly recording an IEP meeting, etc. In these cases, districts all too frequently rely on poorly-phrased board policies (that were all-too-often not submitted for legal review) in order to deny parents the right to record. In most cases, the denial can often be made lawfully pursuant to the IDEA itself, but schools need to understand what parents’ rights are under the IDEA regarding recording and how to properly consider and make a determination regarding a parent’s request for permission to record.

The school’s legal jurisdiction is important, too. States may grant parents the right to record IEP meetings, so schools need to be careful about the policies that they establish with regards to general prohibitions on audio recording. For instance, in California, parents/guardians have the right to record the meetings as long as they provide 24 hours’ notice of the intent to record. Under that same law, schools are also permitted to record if they provide the requisite 24 hours’ notice, unless the parent objects. In states with similar laws that require advance notice, the U.S. Department of Education’s Office of Special Education Programs (OSEP) reminds schools to be cognizant of this additional time requirement and be sure to schedule meetings with sufficient advanced notice to permit the parents the full allotment of time afforded to them in which they may object. In that same letter, OSEP re-affirms its previous guidance on the subject, which was based on Appendix A of the 1999 IDEA federal regulations, confirming that, although the language is from the prior regulations, it still carries weight with the Department.

Part B does not address the use of audio or video recording devices at IEP meetings, and no other Federal statute either authorizes or prohibits the recording of an IEP.

---

28 California Education Code §56341.1.(g).
29 Letter to Savit, 67 IDELR 216 (OSEP 2016).
meeting by either a parent or a school official. Therefore, an SEA or public agency has the option to require, prohibit, limit, or otherwise regulate the use of recording devices at IEP meetings.

If a public agency has a policy that prohibits or limits the use of recording devices at IEP meetings, that policy must provide for exceptions if they are necessary to ensure that the parent understands the IEP or the IEP process or to implement other parental rights guaranteed under Part B. An SEA or school district that adopts a rule regulating the tape recording of IEP meetings also should ensure that it is uniformly applied.30

While states and districts are, pursuant to the above language and the lack of applicable law, permitted to establish rules regarding the recording of IEP team meetings, the 1991 OSEP memorandum31 cited by the 2016 OSEP letter, references section 300.345(e) of the IDEA regulations, which states:

> The public agency shall take whatever action is necessary to ensure that the parent understands the proceedings at the IEP meeting, including arranging for an interpreter for parents with deafness or whose native language is other than English.

It is important to point out that, in order to be eligible for an accommodation to help the parent understand the meeting, the parent must be able to point to a language deficit, memory problems, difficulty understanding what is being said at an IEP meeting, or another deficit or disability.32 There is also some caselaw to suggest that parents are not entitled to a recording of a meeting for the sole purpose of being able to use it as evidence in a due process hearing.

"The right of tape recording must be exercised in good faith by all parties. ... The parties are advised,

---

30 Letter to Anonymous dated June 4, 2003 and in Appendix A to the 1999 IDEA Part B regulations (64 Fed. Reg. 12406, 12477 (Mar. 12, 1999)).
31 Letter to Anonymous, 40 IDELR 70 (OSEP 2003).
32 Jackson County Sch. Dist., 61 IDELR 120 (SEA FL 2013).
however, that taping is to be used exclusively as an aid for understanding the CSE proceedings and for assistance in making informed decisions. It is not to be used as a weapon or as a shield, and upon evidence that a party is abusing its right, that party may forfeit its right to tape record future proceedings."33

Schools should note, however, that "[i]f a public agency uses an alternative means of meeting participation that results in additional costs, the public agency is responsible for paying the additional costs."34

There are a number of different ways that schools can ensure that a parent is able to fully participate in and understand the IEP process without recording, and, while recording should never be precluded as a potential option, it is likely that schools will be able to find an alternative mechanism to assist a parent’s understanding in almost every case. If a school is able to find an alternative method of accommodating a parent that is reasonable and serves the purpose of enabling the parent to understand the proceedings, the school is not required to permit recording.35 Such alternatives may include:

• Arranging for an interpreter to be present with a parent who has language difficulties or does not speak English;

• Paying a staff member or advocate to take thorough notes at the meeting, explain IEP team members’ discussions, and answer questions;36

• Using videoconferencing and/or conference calls for parents who are not able to attend participate in meetings;37 and

33 Warrensburg Cent. Sch. Dist., 17 IDELR 371 (SEA NY 1990). See also Santa Monica-Malibu Unified Sch. Dist., 2 ECLPR 112 (SEA CA 1995).


36 Belvidere Cmty. Unit Sch. Dist. No. 100, 112 LRP 12955 (SEA IL 02/27/12)

37 20 USC 1414(f); 34 CFR 300.328. See also Dep’t of Educ., State of Hawaii, 58 IDELR 240 (SEA HI 2012). While conference calls are certainly best practice, at least one case has indicated that using a non-conference telephone,
• Providing a transcript of an IEP meeting.\textsuperscript{38}

There are rarely instances when none of the above accommodations could be considered appropriate for a particular disability or deficit. Schools should be aware, however, that regardless of the method chosen, it is the school’s responsibility to bear the cost of such accommodation.

\textbf{WHAT SCHOOLS NEED TO DO:}

While schools may permit recording, there are certainly many other available options for accommodating parents’ needs. School recording policies should never preclude the recording of IEP meetings as a matter of policy, but, instead, should leave it as an available option of last resort only when no other appropriate accommodation is available. Schools should note that they are responsible for bearing the cost of any such accommodation. Finally, if parents are permitted to record, schools should make and maintain their own recording, or should establish a policy or procedure that requires that, where a recording is permitted to be made, it is the school personnel who will make the recording and provide a copy to the parent. This will ensure that the school has a full and unedited version of the recording, in the event that the parent does attempt to use the recording against the school in litigation.

IEP team members should be familiar with the school’s general policy regarding recording in school, so that, if they observe a parent attempting to record a meeting without first requesting permission, the IEP team members can cite the policy as an initial response and can then inquire as to the reasons that the parent feels it necessary

\textsuperscript{38}Jefferson County Sch. Dist. R-1, 104 LRP 30613 (SEA CO 04/13/04).
to record the discussion. At that point, the school personnel may inquire further, if necessary, to determine whether the parent requires an accommodation to fully understand and participate in the meeting. If so, it is up to the school to determine what accommodation would be appropriate.

Most school administrators are well aware that permitting parents to record sensitive meetings that may have significant legal implications could elicit a negative response from staff members, as discussed above, so it is extremely important that schools are proactive in their approach to requests for recording IEP meetings to ensure legal-defensibility while also ensuring that recording is a measure of last resort. IEP teams, then, in conjunction with school administration, should be properly trained to understand their legal obligations, suitable alternatives for recording, and cases in which recording may be the only option. Most importantly, they should be trained to seek legal advice in cases where recording appears to be the only option or the parents are refusing to settle for any accommodation other than recording. This type of measured, proactive approach will undoubtedly benefit schools that are dealing with this difficult issue.
PORNOGRAPHIC CONTENT IN SCHOOL ONLINE LIBRARIES

On February 22, 2017, the National Center on Sexual Exploitation (NCOSE) announced its 2017 “Dirty Dozen” list [36] – a highly-influential list intended to “name and shame the bad corporate actors in America that perpetuate sexual exploitation—whether that be through pornography, prostitution, and sex trafficking.” The “Dirty Dozen” list highlights companies that pose the greatest risk and pressures them to change their policies and practices. This year, the list highlighted the issue of widespread access to online pornography in schools by naming one very surprising company – EBSCO Information Services. EBSCO Information Services is a widely-used resource database that provides online library resources to thousands of public and private schools (K-12), colleges and universities, and public libraries nationwide. Its parent company, EBSCO Industries, brings in almost $2 billion in annual sales. EBSCO Information Services describes its K-12 school databases on its website as follows:

The high-quality, curriculum-appropriate content in EBSCO’s school databases not only assists with classroom instruction and student research, but also promotes multimodal literacy, encourages student inquiry, develops critical thinking skills, and integrates 21st century information technologies into the curriculum. [37]

However, the NCOSE found that EBSCO’s Explora, Science Reference Center, Literary Reference Center, and other products, “provide easy access to hardcore pornography sites and extremely graphic sexual content. To make matters worse, innocent searches provide pornographic results. Via a system that bypasses school
Internet filters, EBSCO brings the dark world of XXX to America’s elementary, middle, and high school children.” [38] NCOSE’s Executive Director, Dawn Hawkins, provided this description of EBSCO’s search results system:

Innocent searches lead to sites that normalize sexual violence, such as a link to a story depicting the rape of a woman using the barrel of a gun, as well as sites that normalize risky sexual behaviors such as public, anal, and group sex. These toxic sexual messages are being provided to young students under the guise of an authoritative academic resource. [38]

When reading this information in the “Dirty Dozen” report, this author was skeptical. I did a search for the word “sex,” which yielded 5,092,797 results. Among the top 20 were resources such as: “The Hottest Sex in the World,” “The Hers Guide to Great Sex,” “Is Everyone Having Anal without Me?,” and “Does Your Sex Life include Bondage Play?”

Rather than filtering or blocking inappropriate content, EBSCO Information Services not only provides access to such content by school children, but actually increases the likelihood that inappropriate results will be found in searches by younger users. EBSCO uses a technology known as Lexile, a scale that evaluates the reading level of written materials by using quantitative methods based on individual words and sentence lengths rather than using more qualitative factors, such as maturity of themes or the meaning of words. Lower Lexile scores indicate a lower reading level, and, therefore, are highlighted as more appropriate for lower-level readers. Because pornography has statistically lower Lexile scores than other types of materials, pornographic content shows up with more regularity than other types of content in searches by lower level readers. Information on NCOSE’s “Dirty Dozen” website provides the following description of its experience with the search filtering system:

© 2017 Erin D. Gilsbach, Esq.
The most simple, innocent searches (we tried “7th grade biology” and “6th grade respiration”) are yielding dozens of explicit, even unrelated, articles as the most relevant and first suggestions. [38]

Another significant problem with potentially wide-ranging political and legal ramifications for school districts is that parents and students are not provided with the same access to EBSCO products. Due to licensing costs, schools typically provide students with full-access, password-protected accounts, while parents are provided with simply an overview of the service that does not allow the full search access that students have. In most schools, parents are unaware of this discrepancy and in many cases, school administrators may not be aware of it, either. This problem may result in schools engaging in an unknowing violation of their own policies regarding parent access to and review of curricular and materials content.

NCOSE highlights the experience of two concerned parents in the Cherry Creek School District in Colorado:

In September 2016, concerned parents, Robin and Drew Paterson from Colorado, realized that the Cherry Creek School District and EBSCO were providing access to hardcore pornography, softcore pornography and glamorizing risky sexual behavior to students as young as elementary school when they first found what they felt was obscene material available through their daughter's middle school portal. Their initial complaints to school officials at both Fox Ridge Middle School, and for the county dismissed their claims. On 9/14/16, Dr. John Kenney, the CCSD Director of Middle Schools even demanded that they stop contacting other people about the pornography and said the resource links were district mandated. On 9/23/16, the Patersons received a letter from CCSD that defended material on several grounds, including as an “appropriate use” of “sensitive and controversial” material.

The Patersons continued to reach out to many officials with the school, often meeting with great resistance and refusal to meet or communicate. Through February 20, 2017 the Patersons have attended and spoken at four school district
meetings and officials, while deeply offended at hearing the explicit language printed from EBSCO’s portal at the local middle school, have refused to do much about this problem, other than remove a couple of the more egregious articles.

On the same website, NCOSE published two letters from the school district’s administration. In both letters, but particularly the second, dated October 27, 2016, the school goes to great lengths to justify its actions and even some of the content contained on EBSCO that the parents found to be objectionable, at times giving the impression that the district approved of the pornographic content at issue.

To reinforce its point regarding how truly concerning this issue is, in addition to describing their experiences with EBSCO, NCOSE has made available videos demonstrating the ease with which pornography can be accessed from student accounts – even in cases where a student may not be looking for it. The videos also show the types of inappropriate content that is accessible to students, including erotic fiction and shockingly lewd and inappropriate material.

39 The letters provide excellent “teachable moments” for school district clients. It is unlikely, when the letters were written, that the authoring administrators had any idea that the letters would garner national attention and be posted, publicly, in a such a national forum. The first letter, dated September 23, 2016, gives the impression of blaming the parents for failing to adequately filter their own internet and supervise their child online, despite the fact that it appears that the parents’ primary concerns were regarding the information that the students were able to access at school. The parents’ own communications are not published, so it is impossible to comment on the content of their specific communication with the school, but their email correspondence with EBSCO is published and appears to be very professional and courteous. The tone of the school’s 9/23 response, however, suggests that the authoring administrators felt that the parents’ objections were motivated by a discriminatory objection to the LGBT community, not simply related to their child’s access to explicit pornography in the school setting. The second letter, dated October 27, 2016, from the Associate Superintendent, provides an elaborate blame-deflection analysis and repeatedly emphasizes that the district has little to no control due to the fact that the content is being hosted by a 3rd-party provider.
CIPA Concerns

The sexually explicit content available in schools through EBSCO may violate the Children’s Internet Protection Act (“CIPA”), which requires all school districts that receive eRate funding to utilize filters to block images that constitute obscenity, child pornography, and material that is “harmful to minors.” CIPA defines “harmful to minors” as:

Any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The materials available on EBSCO, as demonstrated by the National Council on Sexual Exploitation, certainly meet this definition. EBSCO products can potentially remain available despite internet filters because they are self-contained within EBSCO in areas that filters do not typically search.

A school or library that knowingly fails to ensure the use of computers in accordance with the certifications required by this section, must reimburse any funds and discounts received under the federal universal service support mechanism for schools and libraries for the period in which there was noncompliance.

41 Id.
42 Links in the “Proof” section of the EBSCO page of NCOSE’s website provide screenshots as well as video explorations of what is available on EBSCO’s student portal. The materials that are accessible on that site certainly do appear to fall under this definition. See http://endsexualexploration.org/ebSCO/.
43 34 CFR 54.520(3)(1).
EBSCO reached out to NCOSE on the day that the 2017 Dirty Dozen list was released. The company expressed concern over the issue and informed NCOSE that it is working to develop better filters and algorithms. There was no indication of what types of filters EBSCO may be considering, whether those filters would comply with CIPA, and whether more content would be blocked instead of just being subject to different algorithms to establish age differences. Until substantial changes are made, however, schools need to carefully consider whether they can lawfully continue to permit students to use EBSCO without jeopardizing the school’s eRate funding.

Keeping in mind that student passwords may permit access to different resources than those available in parent or other accounts, schools should investigate whether inappropriate content is available through any of their internet-based subscriptions, providers, or services, such as EBSCO, and they should immediately take steps to block inappropriate content. If the investigation or the process of filtering/blocking will take time, schools should consider temporarily disabling EBSCO.

In addition to taking action to correct the issue, district-level administrators should be prepared to respond to parent concerns regarding EBSCO’s content, since parental awareness may be heightened now that the issue has been receiving public attention. School administrators and school boards should prepare for public discussions regarding the issue by having someone from the district who should be knowledgeable about the issue available to discuss specific concerns and provide important answers to parent’s questions.

---

44 See the “Update” at the top of NCOSE’s EBSCO page, available at: http://endsexualexploitation.org/ebsco/.
The McAllen Independent School District, in McAllen, Texas, has committed to spending $10,000 on a drone to conduct surveillance on school grounds. [39] Conversely, the Fort Lee and East Rutherford school districts in New Jersey have declared a prohibition on launching, flying, and/or landing drones on school property. [39] Due to the increasingly complex nature of federal and state drone laws, the legal constraints on both practices are elusive. COSA’s Inquiry and Analysis from March of 2016, written by this author, provided a detailed discussion of the state of drone laws at the time and how they impacted public K-12 schools and school policymaking. [40] That article discussed a 2015 FAA Fact Sheet, [41] that states that all regulation related to airspace use, management and efficiency, or safety lies within the exclusive jurisdiction of the FAA. The FAA’s assertions in that Fact Sheet do not have the full force and effect of law, but they may provide guidance as the FAA is adjudicatory authority for all unmanned aircraft systems (UASs).

In June, additional FAA regulations, relating to the operation of UAS, were issued but they did not provide any additional deference or flexibility to schools or other property owners to regulate the use of drones over school or private property. Nonetheless, school districts may be able to regulate conduct that occurs on school property in a manner that effectively

---

45 A copy of East Rutherford’s drone policy is available here: [http://www.straussesmay.com/seportal/Public/DistrictPolicy.aspx?id=8123269e120b4bd38bfd33f99750a769&PolicyID=7481](http://www.straussesmay.com/seportal/Public/DistrictPolicy.aspx?id=8123269e120b4bd38bfd33f99750a769&PolicyID=7481).
controls most drone use above school property. For instance, schools may prohibit individuals from operating a drone without permission while they are on school property and/or regulate the time, place, and manner in which drones may be operated.

Under such a system, a student whose teacher takes a class outside to learn about engineering, aerodynamics, and/or technology may be permitted to operate a drone while a student, acting independently, may not. Even more restrictions may be placed on third-party contractors through specifically-tailored contract language. For example, schools may wish to insert language into construction contracts with building contractors that limit the use of drones by the construction companies. An example of when that might be important is in contractual relationships with building contractors. Construction companies are increasingly being used in the construction industry to assist with surveying, landmapping, inspecting for quality control, and many other uses. [42]

In May of 2016, the FAA issued guidance for schools that clarified that use of drones by students for educational/curricular purposes would fall within the “hobby or recreational use” definition of the FAA regulations, not the more restrictive and regulated “commercial use” section. [43] The guidance permits only limited assistance by teachers, however, and emphasizes that teacher use of drones would not qualify as “hobby or recreational use.” The guidance does not, however, address the use of drones on school grounds for other non-commercial purposes, such as the surveillance uses being contemplated in McAllen, Texas.
Schools that use drones for instructional purposes need to be aware of the FAA’s specific requirements regarding such instructional programs, including the limitations placed on educators. Educators using drones in their classrooms should be trained on the FAA requirements to ensure compliance.

Neither the FAA regulations nor the school guidance address the non-commercial use of drones for safety/security purposes. Where such use is being contemplated, schools will need to work closely with legal counsel to become informed about the issue and properly understand and weigh the risks associated with operating the drones in a manner that significantly lacks clarity of law.

In addition, as pointed out in COSA’s March 2016 I&A article, referenced, above, schools should be carefully apprised of potential insurance issues and risks, as most insurance carriers do not cover drone-related incidents due to the uncertainty and ambiguity of the law. Depending upon the size and the nature of the drones in use, this factor, alone, may cause some schools to decide to temporarily discontinue the use of drones in the educational curriculum until such time as coverage becomes available.
1:1 AND BYOD (BRING YOUR OWN DEVICE) INITIATIVES

Most public schools have at least considered a 1:1 or BYOD program; are in the process of developing one; or already have one in place. While the terminology may vary slightly, a 1:1 program is a program wherein a school district issues a laptop or other electronic device to every student in a particular grade, class, or building. In a BYOD, or “Bring Your Own Device” program (sometimes called “BYOT”– Bring Your Own Technology), a district permits students to bring their own technological devices to use in school, subject to specific conditions and requirements. This section discusses legal issues regarding those initiatives.

The “Free Public Education” Challenge

Both BYOD and 1:1 initiatives have been challenged on the basis that they are inconsistent with the basic premise of public school education: that it is to be available to all children free of cost. All states currently offer a free public education system. Such systems were designed to ensure that all students have an equal right to a K-12 education regardless of socioeconomic status.

Each state establishes this right in a slightly different manner, but the underlying premise is generally the same: all students are entitled to equal K-12 education advantages. For instance, Pennsylvania school law states that:

“Most state constitutions provide for an equal access to a quality education, so if we're saying we're delivering ... educational material through mobile devices, that would imply to me that every kid should have equal access to that content.”

- Scott Himelstein, director of the University of San Diego’s Mobile Technology Learning Center [56]
The board of school directors of each school district shall purchase all necessary furniture, equipment, textbooks, school supplies, and other appliances for the use of the public schools, or any department thereof, in their respective districts, and furnish the same free of cost for use in the schools of the district, subject to such rules and regulations regarding the use and safe-keeping thereof as the board of school directors may adopt.46

[Emphasis added.] Georgia’s language is even stronger and more pointed:

No local unit of administration shall require any pupil or parent to purchase any textbook, library book, or media material except in cases where the pupil damages, loses, or defaces such item either through willful intent or neglect.47

BYOD programs are regularly criticized in public board meetings as contrary to the notion of equal access to education for all students. Even in schools where classroom technology is available to those who cannot afford to meet the district’s BYOD requirements, questions still exist regarding the true equality of opportunities for students who do not bring their own devices. Districts proposing 1:1 initiatives have not been immune to these types of challenges, either. Many schools have required parents to pay a portion of the cost of a 1:1 device, while others have opted to require parents to pay an insurance premium. Most districts exercising these options have instituted exceptions based on socio-economic status, the statutory rights to free education are not generally based upon socio-economic status, and, thus, even programs with generous carve-outs are potentially subject to legal scrutiny.

46 24 PA. STAT. ANN. § 8-801.
So, what are schools to do in the face of these challenges? Challenges (legal and otherwise) based on the “free public education” laws are almost inevitable, but, in order for BYOD and/or 1:1 programs to have a fighting chance, districts need to carefully consider the impact on students who do not have the financial means to participate in such programs as well as those who simply choose not to do so. Will they be provided with the same level of education as those who have the devices? This will ultimately be the crux of any legal challenge based on a free public education theory.

For 1:1 programs, administrators and their attorneys need to carefully review state legal requirements regarding the provision of a free public education and the materials provided for such purposes. Schools need to consider whether having parents supplement the cost is ultimately worth the potential legal challenges (not to mention administrative headache) that such measures may spark. As with the Georgia law, most laws do permit schools to seek recompense for lost/damaged items. Schools should consider whether it makes more sense to focus on shoring up their loss-recoupment procedures instead of requiring parents to shell out money up front.

A Fundamental Difference: Fourth Amendment Protections in 1:1 vs. BYOD Programs

With BYOD programs, one of the fundamental issues will always be the expectation of privacy. Because the devices in BYOD initiatives are personally-owned, users will always have a heightened expectation of privacy. When students use school-issued devices through programs that are commonly called 1:1 programs – one device to one student – there is not the same legal expectation of privacy,

---

48 COSA has a number of great resources related to 4th Amendment protections and student electronic devices. For those seeking a primer on the law regarding that topic, COSA’s Inquiry and Analysis regarding “Student Searches in the Age of Wireless Communications” is a great place to start. http://www.ns.ba.org/student-searches-age-wireless-communications.
Any expectation of privacy on a school-issued device can effectively be reduced to zero through carefully-worded user agreements signed by the student and parents and clear policy language. While schools may have limitations on their ability to search a privately-owned device, due to 4th Amendment protections, schools have complete authority to search school-owned devices, provided that they have taken the necessary steps, as described above.

**The Fourth Amendment vs. Stored Communications Act**

While school administrators often study the 4th Amendment’s search and seizure rules extensively in their graduate courses and professional development trainings, they are rarely, if ever, exposed to the Stored Communications Act and its state-law equivalents. This gap in knowledge could ultimately lead to potential additional liability for schools with regards to email content on In 1967, the Supreme Court held, in *Katz v. United States* that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”49 This rule became widely known as the “third-party rule” based upon a second U.S. Supreme Court case, *Smith v. Maryland*,50 which held that “that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

The Stored Communications Act (“SCA”), 18 U.S.C. § 2701, *et seq.*, sought to fill that gap in privacy protection. The SCA, which was passed by Congress in 1986, is a federal law that prohibits the examination of communication stored in an electronic storage system, such as a public internet-based email server51 or cloud-based voicemail storage system. The Act was intended to provide protection, that was not available under Fourth Amendment, to communications in electronic

51 Note: Not all states agree on what is protected under the SCA. In *Jennings v. Jennings (Jennings I)*, 736 S.E.2d 242 (S.C. 2012), South Carolina diverged from the reasoning adopted by most other jurisdictions when the S.C. Supreme Court determined that an internet-based email system does not qualify for protections under the SCA.
storage. Because the user has shared the information with a third-party ISP or other provider and, therefore, arguably has no expectation of privacy.

Schools should be aware of the SCA when attempting to search a cell phone, since many applications on the phone may contain communications that are covered under the SCA, and, thus, are statutorily assigned heightened privacy. A district court in New Jersey found that the SCA even applies to Facebook communications, when such communications take place among an individual’s Facebook “friends” only and are not readily viewable by the public.52

Policy Language

Too often, schools launch into initiatives such as 1:1/BYOD without taking the necessary steps to ensure that the district’s policies are in sync with the new program. In a district that has recently unveiled a highly-anticipated BYOD program that will allow the use of smartphones53 for academic purposes in the classroom may have an old cell phone use policy from the late 90’s that bans all cell phones from the campus.54 Likewise, buried deep within the murk and mire of a school’s acceptable use policy might lie a general prohibition of student-owned devices in schools. Schools need to scour their policy manuals and perform a “technology upgrade” to address any outdated information55 and make sure that their policy manual, at the very least,

53 Note: Most BYOD programs do not include smartphones on their lists of approved devices. In an age where cyberbullying and sexting have become pervasive, this is likely wise. Schools should be specific in what devices will be permitted. Limiting devices to netbooks and laptop computers only seems to result in the fewest device-related misconduct issues, although with new technology, the lines between laptop and tablet or other devices can sometimes be blurred.
54 In the late 1990’s and early 2000’s, prior to 9/11/01 and the Columbine shootings a year and a half earlier, there was an almost unanimous consensus among education leaders that cell phones should be banned completely, and several states even enacted legislation to that effect. After 9/11, parents became concerned about being able to reach their children in the event of an emergency, and public pressure outweighed the educational considerations. Most school administrators, even where formal policy remained unchanged, began to permit students to have cell phones in schools as a result. Even today, many of those old general-prohibition policies remain on the books.
55 As recently as 2017, our office has stumbled across whole policies dedicated to restricting student possession and use of pagers on school grounds.
does not conflict with any new 1:1 or BYOD initiative, and, more importantly, serves to institute carefully-crafted language that will serve to protect the students and the schools with regards to the new, extensive use of electronics on school grounds.

**CIPA and the Cellular Data Problem**

Policy drafters should be particularly cognizant of the requirements of the Children’s Internet Protection Act (“CIPA”) when making changes to board policy to accommodate 1:1 or BYOD initiatives. Many devices, including many eReaders, tablets, and, smartphones, have cellular connectivity (3G, 4G, LTE, etc.) that does not restrict the users to WiFi networks. This is problematic, since schools are required to ensure that they have a policy that ensures that the online activities of minors are monitored and that technology protection measures are in place to protect students from online activity that is obscene, harmful to minors, or contains pornography, as defined by CIPA.

**The “Free and Reduced Lunch” Problem**

In order to curtail some of the costs of a school-issued 1:1 program, some schools have required a $50 or $100 deposit in order for students to be permitted to take the devices home at night. If the students do not pay the deposit, which usually is intended partly to off-set the costs of the additional insurance the schools generally need to take out to cover the devices and partly to instill some sense of personally responsibility in the student and families. In an effort to ensure socioeconomic fairness, however, many schools waive this cost for low-income students. To determine who qualifies for such a waiver, some schools have turned to the “free and reduced lunch” lists compiled pursuant to the National School Lunch Act (NSLA). Using the free and reduced lunch lists for this purpose without first obtaining written

---

permission from the parents to do so, however, is a violation of federal law. The NSLA prohibits disclosure of such information to individuals and programs not expressly authorized under the NSLA.

In order to lawfully obtain consent, the district must obtain written consent that identifies the information that is to be shared and describes how the information must be used.\textsuperscript{57} The consent statement must be signed and dated by the parent or guardian of the applicant household.\textsuperscript{58} The consent form must also disclose that failing to sign the consent statement will not affect eligibility or participation in the program and that the information will not be shared by the receiving program with any other program.\textsuperscript{59} Disclosure of NSLA information is a criminal offense and bears the penalty of up to $1,000 in fines and up to one year in prison.\textsuperscript{60}

Most schools do have a form that is provided to eligible parents at the beginning of the school year, which allows them to delineate which programs to which they do and do not consent to releasing their information.\textsuperscript{61} These forms, however, are generally well-established and were created, researched, and legally-reviewed by prior administrations. It is common for new initiatives, such as 1:1 tech programs, to be inadvertently left off the list. Administrators may become so accustomed to using the information from the free-and-reduced-lunch lists that they forget or do not realize that written consent is necessary. Thus, while appropriate written consent may be obtained for some purposes, it is often overlooked for newer programs and purposes.

\textsuperscript{57} 42 U.S.C. § 7258.
\textsuperscript{58} Note that this is different than the requirement for applications for free and reduced price meals, which permits any adult household member to sign.
\textsuperscript{59} Id.
\textsuperscript{60} The language of the law is unclear as to whether this penalty would be applied per incident/program or per student. If calculated per student in a program that routinely misused NSLA information of students without proper consent, the potential penalty could increase significantly.
\textsuperscript{61} The ability to selectively give consent regarding some programs and not others is required by law.
School attorneys should periodically remind their districts, for this and other purposes, of the consent requirement. All schools should update their National School Lunch Act disclosure/consent forms at least annually as well as whenever a new program is developed that seeks to use the information from the free-and-reduced-lunch list.

**Schools that are considering a 1:1 technology program need to thoroughly research and investigate the differences between school-issued 1:1 devices and BYOD initiatives. There are many practical and legal implications involved, and the Fourth Amendment issues should be given great weight. With either program, however, schools should be counseled on the applicability of the Stored Communications Act, and administrators should have a thorough understanding of potential SCA issues with regards to search and seizure practices.**

**School attorneys should be an integral part of the planning of any BYOD initiative, from the development of waiver forms to ensuring that the proper liability riders are purchased from the insurance carriers to developing legally-defensible procedures for the program. School attorneys should also play a role in training administrators on such topics as the Fourteenth Amendment, the SCA, CIPA basics, etc.**

**Finally, the launch of a school-issued 1:1 or a BYOD program should coincide with a thorough review and update of the district’s acceptable use policies and other related policies, including cell phone use and personally-owned device policies, and school administrators need to ensure that any use of the National School Lunch Act’s free and reduced lunch list is being done with the appropriate consent.**
TECHNOLOGY AND SCHOOL HEALTH

Telehealth

On June 8, 2016, the Governor of Missouri signed into law SB579, which established the framework for a system of telehealth medicine that can be used in the schools. The law permits schools to bill Missouri’s Medicaid program, HealthNet, for telehealth services, and it also opens the door for specialized disability-related services, such as speech, physical therapy, and mental health therapy, to be provided, and reimbursed, through the telehealth system. The idea of telehealth in schools is not new, however, more and more schools are using it to provide much-needed health-related services to their students. The Los Angeles Unified School District, which is the nation’s 2nd largest school district, unveiled a pilot telehealth program with an initial 5 telehealth carts costing anywhere between $20,000 and $60,000 per cart. [44] The carts are equipped with videoconferencing equipment and electronic health record access. One of the primary incentives for the school district is the cost. It’s free. The telehealth company, Florida-based LifeMD, is picking up the entire tab and will bill student insurers and health plans for the cost of the services. LifeMD will cover the entire cost for students who do not have healthcare. LifeMD has provided telehealth services in health systems, urgent care centers, and prisons, but it had never contracted with a school. With the new school contract, however, the company stands to double the company’s $10.6 million in

revenues in 2016 alone. [45] If the project is successful, the L.A. school district will phase the telehealth services into more of its 900 schools over the next few years.

These projects, and the many like them nationwide, offer many apparent incentives to schools as well as enormous profit potential for telehealth providers, but the introduction of telehealth services into school systems comes with a significant amount of legal complexity related to the applicability of HIPAA to the provider schools. These services clearly place schools within the “covered entity” definition. Thus, HIPAA is applicable to schools that offer telehealth services. HIPAA’s privacy rule provides a specific exemption for student records. Under HIPAA, records that fall within FERPA’s “education records” definition do not constitute “protected health information” under HIPAA. In short, if FERPA can apply to a record, then FERPA’s privacy rule, not HIPAA’s, is the applicable law. Likewise, HIPAA’s security rule is equally inapplicable because the security rule is a subset of HIPAA’s privacy rule, which is not applicable to student records.

With telehealth services, such as those provided by LifeMD and the L.A. school district, however, the telehealth providers would fall within the definition of “health care providers” under HIPAA, and the services, because they would be billed to insurance providers, would be considered covered “transactions” under HIPAA.

As a “covered entity” the school must comply with the HIPAA Administrative Simplification Rules for Transactions, Code Sets and Identifiers with respect to its transactions. If a school district

---

63 See 45 CFR § 160.103.
64 See the exception at paragraph (2)(i) and (2)(ii) to what is considered “protected health information” (PHI) at 45 CFR § 160.103.
65 Id.
66 See 45 CFR § 160.103 (definitions of “health care provider” and “transaction”) and 45 CFR Part 162, Subparts K–R.
contracts with a telehealth provider that is fully HIPAA compliant out of necessity due to its own legal obligations and/or the legal obligations of its other clients, this should be not a significant burden, as long as the telehealth provider will be completing all transactional tasks that may implicate HIPAA, such as billing to insurance companies. School districts will need to be careful, however, that the companies with which they contract are, indeed, HIPAA-compliant, at least with regards to the transactional activities. Schools investigating telehealth options may wish to have an attorney who has expertise in the area of HIPAA compliance review the contract and perform a preliminary investigation into the provider to ascertain whether there are any HIPAA-related issues with the provider. School attorneys can also ensure that the HIPAA-compliance burden falls squarely on the shoulders of the telehealth provider by insisting on highly-protective indemnification language in the contract between the school and the provider.

**Telehealth and IDEA/Section 504 Compliance**

Another one of the key issues with respect to telehealth providers is ensuring compliance with the IDEA and Section 504. Consider this scenario: An 8-year-old child visits the telehealth cart on several occasions due to shortness of breath and a sensation of tightness in his chest. The telehealth provider notes in the child’s telehealth medical records that the child should see an allergist and pulmonologist due to the possible presence of asthma. The telehealth provider is responsible for communicating medical findings directly to the parents. The school nurse is aware of the potential diagnosis but does not share the information with anyone in the school due to confidentiality concerns. A year and a half later, the child has a severe asthma attack in school and suffers significant medical complications as a result of the time it took for the school to recognize the issue and call 911. The treating emergency physician indicates that, had the school reacted more quickly to the student’s condition, many, if not all, of the complications could have been avoided. When the building principal investigates the matter, she finds that the child did not
have a Section 504 plan for the asthma, but the nurse confides that she was aware of the high likelihood that the student had asthma, based upon the telehealth provider information. Would the school be liable under Section 504 for child find and FAPE violations?

What if the nurse had not been aware of the telehealth physician’s observations and recommendations? Would the telehealth physician’s knowledge of the potential disability have been enough to impose child find and/or failure to provide FAPE liability due to the fact that the physician is performing a service for the district as a contracted provider? The answer to this question is less clear, and it revolves, at least in part, around whether the district should have known or had reason to know of the child's potential disability. If it did not and could not have known, then the district would likely be off the hook for a FAPE violation (unless there were other signs that the district missed with regards to the student’s asthma). Indeed, the answer may at least partially depend upon whether the records were subject to FERPA, such that the information could have been shared with a district employee who had a “legitimate educational interest” in the information.

It is clear that the telehealth provider is providing a service for the district in that scenario. There is little doubt about that, particularly if the district, as was the case in L.A., is clear that the reason it has engaged in the relationship with the telehealth provider is to keep kids in school, reduce absenteeism due to simple, treatable minor health conditions, and to reduce the amount of time that a student needs to be out of school for physician appointments. In most schools, particularly those that issue press-releases and multi-platform public comments extolling the benefits of the telehealth program regarding the children’s education, the school-based purpose is clear. However, it is not necessarily clear that these services are services that would otherwise have been provided by the district if they were not being provided by the telehealth entity. Indeed, these are new, novel services that are only being provided because there is an entity that can provide them in a cost-efficient manner.
If the services would not have been provided, then, under FERPA, the telehealth provider would not have qualified as a “school official.” Because of that, the records, including the information about the potential asthma, would not be subject to FERPA. Thus, HIPAA would apply, but to the healthcare provider (the telehealth company) only. In such case, the telehealth physician would have been legally prohibited from disclosing the information about the potential asthma. In such case, not only would the school not have known, it would not have been legally permitted to know (again, presuming that the school employees had no other independent reason to know of the child’s condition). Parents may not be aware of these legal distinctions, however, and they may be assuming that the school has access to and is using the information for educational accommodation purposes as well as the medical/health-related purposes that the telehealth provider offers. Where a child’s telehealth history includes information that may be relevant or even necessary for the school to consider in order to identify or properly accommodate a child’s IDEA and/or Section 504-eligible disability, the parents may be presuming that the school has access to the information in order to make such a determination or accommodations.

Because of this, schools need to consider carefully their procedures and protocols regarding the implementation of telehealth services and their communication with parents. Schools participating in telehealth programs should provide written notice to families addressing and explaining these issues, clearly identifying what the information will be used for, what it will not be used for, who will have access to it, and who will not. Schools offering telehealth services should also consider whether they wish to require a FERPA release from all parents whose children use the telehealth services, just in case the telehealth providers do not constitute “school officials” under FERPA and access to the information is precluded without valid written consent.
Because the legal issues and potential for liability vary dramatically, depending upon the type of telehealth program involved, the nature and source of the providers, whether insurance will be accepted/billed, the extent of involvement by school nurses, and many other factors, schools that are exploring telehealth options need to make sure that they are working very closely with an attorney who has sophisticated knowledge of both the relevant school laws as well as HIPPA and medical liability issues. Since these specialty areas do not often intersect, more than one legal expert may be necessary to provide counsel to schools and assist with developing procedures and regulations as well as establishing boundaries for the program and making sure that the program does not extend beyond what has been determined to be an appropriate amount of legal risk. Districts that are particularly risk-averse should be cautious about this and any type of program that may potentially extend the district’s services into other fields, such as healthcare.

An important consideration for schools, and one that should factor into any decision regarding offering telehealth or similar program is that of insurance coverage. It is likely that the district’s current policies would not extend to such a program. Thus, schools need to consider what coverage is available for telehealth and related programs and should factor the cost of such policies into their decision-making. An important but potentially separate coverage issue is that related to the district’s school nurses. If a nurse, due to telehealth services, will or may be working closely with telehealth providers and providing services outside of the scope of those that they would normally provide in the education setting, additional (or initial, for some districts) malpractice insurance may be necessary. These insurance issues are particularly important since state tort claims immunity may not be applicable to the provision of healthcare in schools that is outside the scope of what is required by state law. Attorneys need to analyze all of these issues and provide school clients with risk-assessment and potential liability information so that they can identify the types of insurance products that may be necessary/beneficial and make fully-informed decisions regarding whether to proceed with telehealth services, and develop policies, procedures, and protocols that are designed to protect schools from liability.
Requests for livestreaming in the classroom are becoming more frequent due to significant advances in technology. Most of the legal issues that could arise as a result of livestreaming classroom instruction can be eliminated with careful planning and legally-defensible policies and procedures. The following paragraphs highlight a few of the issues that could arise and provide potential solutions.

Wiretap Law Violations

First, school districts need to be careful not to violate state wiretap laws. Most wiretap laws cover live-streaming, as well as recording, conversations. Therefore, school districts need to take precautions to make certain that they do not violate wiretap laws when they live-stream in the classroom. As discussed above, most wiretap laws apply only in contexts where the speakers have a reasonable expectation of privacy. Thus, most conversations that take place in a classroom full of students would not be protected under those laws. However, if two individuals are speaking in a low voice to each other in a manner that is clearly designed to ensure the privacy of the conversation, those individuals may be deemed to have a reasonable expectation of privacy in those conversations. Similarly, individuals might also have a reasonable expectation of privacy if they are having a conversation in a classroom, after class has ended, and they believe that they are the only people present in the classroom. If the microphone of a live stream device picks up those conversations, there may be a wiretap violation.

Depending upon the specifics of the state law, however, schools can generally eliminate the wiretap issues. In many states, schools can eliminate the wiretap issues by eliminating the expectation of privacy. School attorneys should research their state’s law to determine what actions, if any, can effectively eliminate a speaker’s expectation of privacy in a live-streamed classroom.
**FERPA / Student Records Policy**

Perhaps a more significant issue, however, is the issue of student data privacy. Regardless of whether there is an expectation of privacy in any given environment, student records are protected by FERPA, and FERPA’s confidentiality mandates apply. School districts need to establish protocols and provide proper training to employees to ensure that the livestreaming of classroom content will not result in a violation of privacy rights through streaming or publishing confidential student information protected by FERPA, that would require parental written permission to share with the livestream viewer(s).

**WHAT SCHOOLS NEED TO DO:**

**WIRETAP LAW VIOLATION CONCERNS:**

Generally, prominent posting of signs, clearly warning of the presence of recording or live-streaming devices in that classroom are sufficient. Such signs should indicate that the recording and/or live-streaming may occur even when class is not in session. In addition, written notices could be sent home to all parents and students, letting them know that some classes are being live-streamed and how to recognize a classroom in which live-streaming may be taking place. Schools may wish to provide a copy of the signs that will be present in live-streamed classrooms, so that parents and/or students can identify live-streamed classrooms. Additionally, signage could be prominently placed in the main office that provides basic information about live-streaming and informs visitors that classrooms may be live-streamed.
FERPA PRIVACY VIOLATION CONCERNS:

In classrooms where live-streaming is or may be taking place, school employees will need to be particularly cautious about what information they discuss within proximity of the live-streaming device’s microphone. In addition, employees must be careful to remove any FERPA-protected information that may be viewable from the lens of the live-stream device. For instance, if a teachers desk is within view of the device, the teacher would need to be particularly cautious not to place confidential student information on his/her desk while the device is streaming. Specialized training in these areas, as well as a refresher course in FERPA’s protections, is a good idea.

ESTABLISHING RULES AND EXPECTATIONS FOR STUDENTS/USERS

Finally, schools should also establish clear, written rules and expectations pertaining to the recipient of the live-streamed content and make the student’s right to participate via livestream contingent upon the student and parents’ compliance with the established rules. For instance, for privacy protections, schools may wish to prohibit the remote recording or screen-grabbing of live video content without prior district permission. While, from a practical purpose, this may be difficult, if not impossible to enforce, it will establish a clear right to immediately revoke the student’s permission to participate via livestream if a video of the transmission suddenly ends up on YouTube. The establishment of a set of written rules and protocols eliminates any argument of ambiguity or ignorance.
Livestreaming of School Events

Interscholastic Athletics Association ("IAA") Policies and Restrictions

In most states, schools have the inherent right to broadcast their own events, subject, of course, to intellectual property laws, which are discussed, below. Since most secondary athletic events are governed by the state athletic association, in which a particular school district participates, districts should check their athletic association policies and restrictions to determine whether there are any restrictions on live broadcasting of interscholastic events. In most of the states where the IAAs do specifically address broadcasting rights, the IAA only restricts schools from broadcasting tournament games. However, districts should check to be sure live-streaming broadcasts will not violate their state IAA rules.

Music Rights

When live-streaming any event, schools need to be aware that any musical work being streamed, from the songs played by the marching band to the music being played through the loudspeakers during player warm-ups, must be properly licensed to avoid copyright infringement. This includes even partial songs and song clips. Where music is not licensed, the sound of any live stream must be muted whenever the music plays.

In lieu of obtaining copyright permissions for everything that airs, schools could opt to "white out" or silence songs when they come on, having your announcer fill in those sections. Many schools have found a happy

---

68 See Oklahoma Sports Properties, Inc. v. ISD No. 11 of Tulsa County, 1998 OK CIV APP 40, 957 P.2d 137.
69 In Wisconsin, the Seventh Circuit expressly upheld the right of the Wisconsin Interscholastic Athletics Association to exclusively license the right to broadcast tournament games played by its member schools over the 1st Amendment objections of a local news media outlet. See Wis. Interscholastic Athletic Ass’n v. Gannett Co., Inc., No. 10-2627 (7th Cir. Aug. 24, 2011).
medium in obtaining the necessary copyrights for the music they play all the time at the games, if it's not too cost-prohibitive. That way, the school would not be required to white out everything, but it could still keep costs relatively low.

Copyright infringement claims can become extremely costly because a single event can result in multiple types of liability. For example, failure to properly license a musical work that is played on a livestream video feed, which is then made available as a recorded, on-demand program for a period of time after the work was initially live-streamed, could result in multiple counts of infringement. With the recent increase in the popularity and ease of live-streamed content, performance rights organizations have become vigilant in spotting copyright infringement and enforcing copyright laws through legal action.

**What is Protected by Copyright and What is Free?**

There are two types of songs: those in the public domain, and those that are protected by copyright. Much of the older music that is played over livestream, such as songs played by a marching band, is in the public domain and would not be protected by copyright laws if it was written prior to 1923 (the year that copyright laws were first enacted). Thus, if school districts stick to what’s in the public domain, there are no copyright issues. However, since there’s only so much John Phillip Sousa that a school can take (and since that’s not usually a high school football player’s warm-up music of choice), schools should be aware of the legal music licensing requirements for songs that are not in the public domain.

The general period of copyright protection lasts for the creator’s life plus 70 years.⁷⁰ “Works for hire,” however, have a copyright protection lifespan of 95 years from the date of first publication or 120 years from the date of creation, whichever

---

⁷⁰ 17 U.S.C. §302(a). Note: If there is more than one composer/author, the 70 years begins upon the death of the last living composer/author.
expires first. It is very possible - if not probable - that there will be another extension of the 95-year timeframe due to everybody's favorite rodent, Mickey Mouse. The "works for hire" expiration period has only been extended twice since 1928 - both times were to prevent Mickey from falling into the public domain. Under the current law, Mickey becomes public in 2023, but since he is his own multi-billion-dollar industry, it is reasonably certain that Disney will do everything in its power over the next few years, including throwing a significant sum of money at high-powered lobbyists, to once again extend that protection.

Because of these lengthy copyright protection periods, schools can reasonably count on the fact that the vast majority of music that they will be playing at live-streamed events

71 17 U.S.C. §302(c)
is protected by copyright law. Therefore, schools will need to obtain the rights to the music prior to streaming the content live.

**Sovereign Immunity and Copyright Liability**

Sovereign immunity has long been upheld by the courts in copyright actions. In 1990, Congress passed the “Copyright Remedy Clarification Act (“CRCA”),”72 which specifically says that state sovereign immunity shall not apply to copyright infringement actions.73 Shortly thereafter, Congress passed similar laws for trademark and patent infringement actions.74 Soon after the CRCA was passed, the U.S. Supreme Court decided several cases that, although they were not cases specific to the CRCA or other intellectual property laws, made clear that Congress’s powers under Article I did not give it the authority to abrogate state immunity and that the attempt to do so was a violation of the 14th Amendment.75 Thus, where it exists, these cases suggest that the sovereign immunity that protected government entities prior to the CRCA continues to apply in copyright cases. Many school districts are political subdivisions that are not protected by sovereign immunity. Additionally, states vary in the breadth of their sovereign immunity rights, so school attorneys need to make certain that they know the law in their jurisdictions before they rely on sovereign immunity as a defense to a copyright action.

Even in situations where a school district might be protected by sovereign immunity, it should be very careful in its use of copyrighted material for a number of reasons. First, even though the districts might be immune from copyright infringement liability, the individual actors involved may not be immune, depending

upon the nature of their involvement with the infringement and the specific language of the governmental immunity laws. The individuals within a school who personally handle the tasks that result in copyright infringement could potentially be held legally responsible. Depending upon the sophistication of the livestreaming, there could be many individuals involved in the process who may be vulnerable to potential liability in their personal capacities. In addition, while damages and similar types of relief may not be available due to governmental immunity, injunctive relief is likely still available, and individual actors can be sued for injunctive relief as well as potential money damages under the legal theory of *ex parte Young.*

An event, such as a livestreamed graduation ceremony, the livestreaming of which may have taken months to plan and may have cost a significant amount of money to produce, could be foiled mere hours before the event by a court-issued injunction. In such a case, many hours of work and a potentially large financial investment in equipment, software, training, and personnel would be wasted.

Finally, if the school is using a 3rd-party site, such as YouTube Live, Facebook Live, or Periscope, the provider might prohibit the streaming of copyrighted content without prior notification of the legal right to do so. (See the “Notifying 3rd Party Streaming Video Providers” and “Platform” sections, below.) As with an injunction, the endeavor would result in a great deal of wasted time, money, and energy if it is prepared for livestreaming but not accepted by the hosting site. Thus, despite any available governmental immunity protections, it is still in the school’s best interests to comply with applicable copyright law as ignoring such laws could be detrimental.

**Performance Rights**

Live streaming music requires a “performance license.” Performance rights organizations (PROs) are companies that contract with individual artists and composers to handle the licensing of their music. Most entities seeking a performance license

---

76 *Ex parte Young*, 209 U.S. 123 (1908). See also *Board of Trustees of the University of Alabama v. Garrett*, 531 U.S. 356, 374 n.9 (2001)
opt for what is known as a “blanket license,” which gives licensees the performing rights for the PRO’s entire catalog for either a percentage of the gross revenues of an establishment (which is generally not applicable for school districts), or a fixed, flat fee, which is typically paid annually.

A less common option, but one that may be appropriate for schools that intend to use advertisements during their live stream event, is a “per-program” or “per segment” option. With this type of option, the licensee negotiates a fee for the license that is based upon a percentage of the ad revenue. (Note: Schools considering an ad-based structure for their live-streaming of events or other revenue-building mechanism need to be wary of the potential eRate issues that such action may raise, which is discussed, below.) This type of percentage-based system is generally more cumbersome than the flat-fee arrangement due to the necessary fee calculations involved. It is also more difficult for schools to budget due to the fact that revenue from ads may not be consistent from year to year or even event to event. It is important to note that, even if a school decides to use an ad-based program for its event streaming, it may still utilize the more easily-manageable “blanket license” option.

Finally, “per-song” licenses are also available, but they are generally impractical for events, such as sporting events or graduation ceremonies, that typically have a large number of songs and/or musical clips being played throughout each event. Pre-planning each individual song would likely require more time and energy than a school district has available to dedicate to the task. Thus, “per-song” licenses are rarely used in live-streaming situations.

As indicated, above, there are only four major PROs that deal with performing rights. They are: ASCAP, BMI, SESAC, and GMR. ASCAP and BMI have been

---

77 Meredith Corp., 1 F. Supp. 3d at 190; BMI v. CBS, 441 U.S. at 5.
subject to federal antitrust consent decrees since 1941, due to alleged price-fixing, unlawful “tying,” and other nefarious business practices.

**Synch Rights**

Synch rights are different from mechanical or performance rights in that they permit a musical work to be layered on top of other visual effects. These types of compilations are common on YouTube, and many software programs now make it easy to create a professional-looking synched video in minutes. It is important for schools to remember, though, that the use of any musical work in this manner, particularly if it is utilized during a public event or performance, requires proper licensing. If the school will be using video editing techniques to create a synched video, specialized rights may need to be obtained.

**Notifying 3rd-Party Streaming Video Providers**

Schools that have obtained the rights to the music should notify the 3rd-party provider (such as YouTube and Facebook Live) in advance and provide them with a copy of the contract. Many of these entities have strict rules about copyrighted content, and they may curtail the school’s program in order to protect themselves from copyright infringement lawsuits. For instance, YouTube Live has been known to take down content for a 15-second music clip that is playing in the background. To avoid this type of disruption, provide any and all music licensing information to the 3rd-party program in advance.

---

79 “Tying,” in a nutshell, is the practice of selling/licensing one item only if the buyer/licensee agrees to by another item. Courts are lightening up restrictions on tying, with cases now examining the competitive effect of the tying rather than just prohibiting it outright as a violation of antitrust laws. See “Tying the Sale of Two Products,” FTC, http://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/tying-sale-two-products (last visited Jan. 26, 2015).

ADA Accessibility (“Closed Captioning”)

Despite the fact that Federal Communication Commission (FCC) regulations specifically state that channels/streams producing annual revenue of less than $3 million and locally produced educational programming are both exempt from FCC requirements for providing closed captioning for its broadcasts, entities that are recipients of federal funding, such as public school districts, have a legal obligation to ensure that its web-based content, including streaming videos, are accessible to individuals with disabilities. For streaming videos, this primarily deals with closed captioning for the hearing impaired. Closed captioning is, in short, a necessary ADA accommodation that schools need to make, akin to installing ramps for visitors in wheelchairs to use to get down to the field to view the event live. If a district is live-streaming the event, it needs to be just as accessible in the live stream. With so much web and technology-based content being used by schools, the federal government has prioritized this issue. Over the past year, the federal Office of Civil Rights has had a significant increase in active enforcement cases. As of July 2016, OCR had 227 open investigations involving the issue of accessibility of online courses, distance learning, websites and remote applications. [46]

Closed captioning used to involve selecting from a number of different cumbersome and expensive hardware options that added closed captioning to videos after the fact. However, due to the fantastic technological advances in voice recognition software as well as the recent emergence of real-time, cloud-based captioning options on the market, providing captioning for live-streamed events is now readily available and much more affordable for school districts.

Platforms

Not all live-streaming platforms are equal, and schools need to be careful to select a platform that meets their needs. Platforms like YouTube and Facebook Live are convenient from a technical perspective, but they have their own issues. Facebook Live has a 90-minute time limit, so that is not generally a workable

81 47 C.F.R. §79.1(12) and (13)
solution for high school football games or graduation ceremonies. Twitter recently released a live stream option called Periscope, but users currently have no ability to turn off the associated public comments (it is Twitter, after all), so schools would have limited ability to protect against real-time cyber-bullying and negative, nasty, or inappropriate comments. At a minimum, schools will need a platform on which they can control (read: block) the live interaction. In addition, all of the free sites are ad-based. Schools will need to consider what ads are being promoted and whether such ads are in violation of any of the school’s advertising policies.

With any platform, the school will need to make sure, first and foremost, that it will retain the exclusive intellectual property rights to the video being streamed. As discussed in the “Student Data Privacy” section, above, be wary of “free” services. When using a “free” service, always ascertain what benefit or value the service is obtaining from facilitating the livestream video. Are they requiring the school to fully or partially relinquish intellectual property rights? Are they making money on advertisements to which the school’s viewers will be subject?

One solution that eliminates many issues involved with “free” services is for a school to purchase a software package, such as Wirecast Pro or Ustream Producer, and stream the content directly from the school’s website. This is increasingly an ideal option for schools that are concerned with turning over the content to a 3rd-party site and/or taking responsibility for what a user sees on the 3rd-party platform. This method has the added benefit of allowing the school full control over when a video is taken down. With 3rd-party sites, schools have little to no control over when a video is taken down and does not have the ability to ensure that a video is permanently deleted from the servers of the 3rd-party site, which may be important if the school later finds that the video contained objectionable content.

82 Plus, as I have been told repeatedly by my 6, 8, and 10-year-old daughters, “Facebook is for old people.”
Finally, for those districts that are truly tech-savvy and want to get ahead of the game, there are also a lot of products out there that allow schools to create their own SmartTV channel, which will be compatible for devices such as Roku, GoogleTV, etc. SmartTV content is gaining increasing popularity, and it's really easy for users to download the app and watch. Similarly, there are a number of products available that will allow schools to create a streaming iOS or Android app. This is not something that should be endeavored without copious amounts of research, however. Schools should be aware of what they are purchasing and using, and they should know the pros, cons, and potential issues of whatever software/platform they choose. As discussed elsewhere in this paper, schools should always be wary of things that are "free," because there may be potential legal liability lurking beneath the surface of many of these no-cost options.

**Delay**

Another factor that schools should consider with regard to live-streaming of events is the amount of delay that they wish to impose. Depending upon the platform upon which the district chooses to stream, it may not have much (if any) discretion in how much lead-time delay a streaming video will have, but, with most of the purchased software, delay time is a variable setting. The delay will enable the school to have more time to censor and/or stop the live stream if necessary, and, depending upon the functionality of the closed captioning program being used, a longer delay may enhance the performance of the closed captioning. Finally, and very importantly, it will allow for more lead-time to “white out” the sound when unexpected music is played for which the district does not have a license.

**Livestreaming Policy**

Schools should have formal policies and procedures in place for their live-streaming activity. Board policies and applicable administrative regulations/procedures should address the items discussed, above.
In short, live-streaming is becoming quite commonplace within today’s schools, and schools (and their attorneys) need not be afraid of embracing it. However, a careful, calculated approach to the development of live-streaming policies and procedures will, without a doubt, prevent liability and ensure a better experience for the school and the community. Schools should follow the basic checklist, below, using the information, above, to guide them as they implement livestreaming initiatives:

- Identify the events/types of events for which livestreaming may be used.
- Research and select a platform to be used, taking into consideration the factors and options discussed, in the “Platform” section, above.
- Ascertain whether a formal board policy should be implemented prior to engaging in livestreaming of district events. The policy should designate a specific district-level administrator who will be responsible for ensuring proper implementation and developing written procedures/administrative guidelines and who may receive specialized training in copyright requirements and procedures and other legal issues.
- Establish formal procedures or administrative regulations that must be followed, which are designed to ensure a uniform and predetermined approach to livestreaming that is designed protect the school against liability. The regulations, at a minimum, should specify an individual in each building who will be responsible for ensuring successful implementation of the applicable policies and procedures at the building level.
- Obtain a thorough legal review of all policies, procedures, and administrative regulations.
- Research available “blanket licenses” (see “Performance Rights” section, above) and determine whether it is in the school’s best interests to secure such a license.
- If the events are athletic events, check with PIAA and/or other groups with which the athletic event is affiliated to ascertain what restrictions on livestreaming, if any, may apply.
- If the events are artistic events, such as plays, musicals, concerts, etc., check the school’s permissions to make sure that the school has the rights for public dissemination (unless they made specific arrangements, they likely do not).
- On an event-by-event basis, ascertain whether any copyrighted musical or video works will be seen/heard on the livestream video, and ensure that the school either has legal permission to livestream the works or is prepared to use a white-out or other technique to prevent such works from appearing/being heard on the livestream.
Although this author briefly addressed the issue of school district cyber options in her 2016 COSA presentation and paper entitled “Creative Revenue Streaming and Public Schools: A Legal Discussion Regarding Non-Traditional, New and Creative Revenue Streaming Trends in Public Schools Nationwide,” [47] the issue has increased in significance and bears mention once again in this year’s materials. As with many other edtech products, the operation of cyberschools has proven to be an extremely lucrative business. The company K12 Inc. brought in over $700 billion in revenue from the schools it managed, and other big-name education resource companies, such as Pearson, have thrown their hat into the cyberschool game. Research, however, is beginning to show what public schools have been saying for a long time – that cyber charters and full-time online options are not working.

In 2015, Stanford University’s Center for Research on Educational Outcomes did a study that highlighted the appalling performance of full-time cyberschool programs. That study found that the math scores of cyber students were comparable to the scores of the students if they had not attended school at all. The typical academic gains for students in math were -.25 deviations below that of those attending brick-and-mortar schools. That’s the equivalent of 180 fewer days of instruction. [48] In other words, the math scores of the cyber students were the same as if they had not attended an entire year’s worth of school. Reading scores were not much better.
With such abysmal performance ratings, especially from companies that have purportedly researched their practices and are solely dedicated to successful online learning, it has become clear, at the very least, that no provider or online education theory has been successful in duplicating, in an online format, the educational results of brick-and-mortar schools. Despite that, many brick-and-mortar school districts are adopting online options in an effort to compete with online charter schools. In June of 2010, the Michigan Department of Education compiled a summary of states with full-time, statewide, online schools. This chart summary showed that the majority of states have at least one statewide online school wherein the state funding leaves the student’s district of residence and follows the student to the applicable online school. Virtual schools typically have a lower per-pupil expenditure rate than traditional brick-and-mortar schools, but few states compensate for that difference. Thus, many school districts are turning to cyber-option versions of their own curriculums to keep students enrolled. In Pennsylvania, schools can save up to $4,000 per student by opening their own cyber-school options. Indeed, cyber-learning businesses have sprouted up with the goal of helping schools retain students in cyber-options who might otherwise attend a statewide virtual charter school.

---

84 This resource is available publically at: [http://www.doe.mass.edu/boe/docs/FY2010/0610/item4_FTvirtualschools.pdf](http://www.doe.mass.edu/boe/docs/FY2010/0610/item4_FTvirtualschools.pdf).

Cyber programming in public schools does not have to be exclusively online. Hybrid programs, such as the Denver Public Schools’ “Click and Brick” program, offer online programming, which can be completed on or off campus, for some subjects and allow students to participate in the general learning environment during other portions of their schooling. Some market-savvy schools have not only developed successful cyber-options within their public schools, but have also worked to develop marketing platforms on their district websites to garner attention for their online and/or hybrid programs.

**Special Concerns Regarding Cyber-Options and Students with Special Needs**

Cyber-options for public school districts can become challenging with regards to special needs students. Schools must walk a fine line between the true provision of FAPE and non-discrimination. What is the “least restrictive environment” when it comes to a school that offers both a cyber and traditional brick-and-mortar option? Where a parent wishes to have a student attend a cyber option, but the IEP team determines that the brick-and-mortar option is more appropriate, which option should the school choose? Is the school obligated to first try to create an appropriate cyber program or hybrid program for the child to avoid a disability discrimination lawsuit? These questions have yet to be answered, but as more schools embrace the cyber-option as a way to recoup increasingly needed costs, the caselaw will surely follow.

---

Schools that already have or are seeking to create a cyber-option should proceed with caution and should obtain the advice of their legal counsel. Written cyber-option rules should be provided to parents and the student upon enrollment in the school’s cyber program. Such rules should, most importantly, specify what circumstances would trigger a child’s ineligibility for further online services. These situations would be where a student is displaying a pattern of nonattendance/non-activity in the cyber program, a specifically-designated level of poor grade performance, etc. This will help the district to ensure that, where a cyber program is not successful for a particular student, the student can be returned to the regular school environment before the student has fallen too far behind, academically. There are many different laws that apply to public schools that would likewise apply to their cyber-options. Simple mandates, such as mandatory attendance laws, become tricky when applying them to a cyber-option. How is attendance measured? What is a “full day” in cyber-school? Which mandates can be contracted out to 3rd-party online service providers, and which cannot be transferred? Schools should have clear, written answers to these and other important questions, both in their own administrative regulations regarding cyber-option implementation and, where appropriate, parents and students should be informed of these requirements. Enrollment in a district cyber-option by a special needs student should be carefully addressed by the schools, and, at least until specific guidance is issued by the courts, schools may wish to have their legal counsel review their cyber-option protocols and procedures with regards to IDEA-eligible students to help ensure legal defensibility.

SCHOOL DISTRICT CYBER OPTIONS

The above pages set forth only a few of the many education technology issues that do or may present legal issues for school clients. When representing public school clients, it is important to be knowledgeable about the technology programs
and initiatives that are being offered by the client. Many times, in an effort to keep a step ahead of the ever-changing arena of educational technology, administrators who are focused on bringing the latest in technology and high-tech programming to their schools often forget that having a legal review of EdTech programs and initiatives, even if it temporarily slows down the process, will help the schools, in the long run, as such review will allow schools to assess the potential for liability and recommend procedures and protocols that can minimize that potential. EdTech initiatives can be brought to a screeching halt by litigation and can end up costing districts far more in legal fees than the districts ever anticipated.

School attorneys need to keep up with changing and newly-emerging areas of educational technology as well as the legal issues that they may present. They also need to keep alert and recognize EdTech initiatives that may be going on in their client districts that may cause problems or require careful planning. Finally, they need to counsel clients, generally, that EdTech issues should be discussed and raised proactively with counsel on a regular basis, just to make sure that any potential problems can be addressed proactively and steps can be taken early in the process to limit potential liability. In many cases, administrators may not have recognized that the initiatives might pose liability, and, therefore, may not have proactively sought legal counsel.

Armed with knowledge about the potential risks, attorneys can help their clients proactively build better programs. This will ultimately benefit the students, the parents, district personnel, board members, and taxpayers.
REFERENCES


lucie-county/fort-pierce/student-suspended-after-she-says-she-recorded-video-of-teacher-bullying-student.


50 YEARS OF SCHOOL TECHNOLOGY


## Appendix A: State Wiretap Law Chart

<table>
<thead>
<tr>
<th>STATE</th>
<th>Who Must Consent?</th>
<th>Legal Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEDERAL</strong></td>
<td>One Party</td>
<td>18 USC § 2511(2)(d)</td>
</tr>
<tr>
<td><strong>ALABAMA</strong></td>
<td>One Party</td>
<td>13A-11-30(1) and § 13A-11-31</td>
</tr>
<tr>
<td><strong>ARKANSAS</strong></td>
<td>One Party</td>
<td>Ark. Code Ann. § 5-60-120</td>
</tr>
<tr>
<td><strong>DISTRICT OF COLUMBIA</strong></td>
<td>One Party</td>
<td>D.C. Code § 23-542(b)(3)</td>
</tr>
<tr>
<td><strong>FLORIDA</strong></td>
<td>All Parties</td>
<td>Fla. Stat. Ann. § 934.03(3)(d)</td>
</tr>
<tr>
<td><strong>HAWAII</strong></td>
<td>One Party</td>
<td>Haw. Rev. Stat. § 803-42(3)(A)</td>
</tr>
<tr>
<td><strong>IDAHO</strong></td>
<td>One Party</td>
<td>Idaho Code Ann. § 18-6702(2)(d)</td>
</tr>
<tr>
<td><strong>INDIANA</strong></td>
<td>One Party</td>
<td>Ind. Code Ann. § 35-31.5-2-176</td>
</tr>
<tr>
<td><strong>IOWA</strong></td>
<td>One Party</td>
<td>Iowa Code Ann. § 808B.2 (2)(c); Iowa Code Ann. § 727.8</td>
</tr>
</tbody>
</table>
## Appendix A: State Wiretap Law Chart

<table>
<thead>
<tr>
<th>State</th>
<th>One Party</th>
<th>All Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minnesota</td>
<td>Minn. Stat. Ann. § 626A.02(d)</td>
<td></td>
</tr>
<tr>
<td>Mississippi</td>
<td>Miss. Code. Ann. § 41-29-531(e)</td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>Mont. Code Ann. § 45-8-213</td>
<td></td>
</tr>
<tr>
<td>New Mexico</td>
<td>N.M. Stat. Ann. § 30-12-1(C)</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>N.Y. Penal Law § 250.00(1); N.Y. Penal Law § 250.05</td>
<td></td>
</tr>
<tr>
<td>North Dakota</td>
<td>N.D. Cent. Code § 12.1-15-02</td>
<td></td>
</tr>
<tr>
<td>Ohio</td>
<td>Ohio Rev. Code Ann. § 2933.52(B)(4); Ohio Rev. Code Ann. § 2933.51</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Party Type</td>
<td>Law References</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>UTAH</strong></td>
<td>One Party</td>
<td>Utah Code Ann. § 77-23a-4; Utah Code Ann. § 77-23a-3</td>
</tr>
<tr>
<td><strong>WASHINGTON</strong></td>
<td>All Parties</td>
<td>Wash. Rev. Code Ann. § 9.73.030</td>
</tr>
<tr>
<td>** WYOMING**</td>
<td>One Party</td>
<td>Wyo. Stat. Ann. § 7-3-702</td>
</tr>
</tbody>
</table>