Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy

April 1, 2015
This study was conducted by the Center for Education Policy and Law (CEPAL), an Institute for Entrepreneurship in Education (IEE) research entity operating under the auspices of the School of Leadership and Education Sciences (SOLES) and the School of Law at the University of San Diego (USD).

Established by a grant from the William D. Lynch Foundation in 2007, CEPAL’s mission is to foster better linkage between educational research, policymaking, and practice. To this end, CEPAL undertakes empirical and legal research on educational policy issues, enhances communication between education leaders and state-level policymakers, and facilitates understanding among USD law students and education graduate students about the policymaking process through courses, internships, and research opportunities. Additional information about CEPAL is available at www.sandiego.edu/cepal.
LEGAL DISCLAIMER

This document was prepared by CEPAL at USD’s SOLES. This document does not convey or constitute legal advice. This information is not provided in the course of and does not create or constitute an attorney-client relationship. CEPAL does not provide legal advice on behalf of USD or any other entity, and any statements or analysis performed in the course of this research are that of CEPAL and its researchers and do not necessarily reflect the views or opinions of USD.
This report is a condensed version of a much more comprehensive report, published in the *Journal of Law and Education*. It discusses some of the privacy implications that arise when students use digital technology in public schools. The report identifies three entities that are most likely to breach student privacy: advertisers, criminals, and the government. Using these areas as three separate lenses through which to examine California and federal law, the report looks at student and parent expectations of privacy and where school districts and the law are falling short of those expectations. Throughout, the report highlights areas of concern for school districts that are using digital technology and offers some guidance as schools navigate digital waters. A more detailed legal discussion of the points addressed in this report can be found in the *Journal of Law and Education*, (Volume 44, Summer Issue).

**Author**

Joanna Tudor, JD, Legal Research Associate

Table of Contents

Overview of Relevant Law Affecting Student Privacy ................................................................. 2
Who is Collecting Data, How is it Being Collected, and Why Does it Matter? .......................... 5
Advertisers ........................................................................................................................................ 5
Criminals ......................................................................................................................................... 17
The Government ............................................................................................................................. 20
Conclusion ...................................................................................................................................... 24
Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy

April 1, 2015

Policymakers have been attempting to improve our education system and student achievement for decades. With encouragement from recent legislation such as the America Competes Act, which places an emphasis on Science, Technology, Engineering, and Math (STEM) education, school districts across the country are incorporating technology into academics in sweeping strides. As technology is integrated into academic instruction for use at school and at home, student interaction with digital technology has been propelled to exceptional levels. Meanwhile, the efficiency of digital technology has made it easier for school districts and other entities to collect, organize, and store large databases of information. For instance, Apple’s iTunes has a behavior-monitoring application (app) available to teachers that allows them to compile information about which students have behavior problems and which students are helpful in the classroom. Sometimes districts contract with outside service providers who deliver services to students, and often these service providers also collect and use personally identifiable student information to help them improve their services. For example, some school cafeterias are now using a biometric identification system to allow students to pay for lunch by scanning their fingerprint at the checkout line.1

The ease and convenience of collecting, organizing, and storing data through the use of technology means that most, if not all, of these data are in digital form. However, the convenience and insight allowed by unprecedented access to technology comes at a cost, which frequently manifests as invasions of student privacy. Districts may not realize the extent to which student privacy is at risk, particularly because technology is constantly evolving to create new or expanded risks. However, understanding the risks involved are only half the battle. Districts must also navigate the multitude of federal and state laws currently in place that are designed to protect student privacy. In the last several decades, privacy laws in general have morphed as advances in technology have challenged well-established concepts in privacy law.2 Compounding the matter, student expectations in privacy has

---

2 For example, in U.S. v. Jones, the United States Supreme Court ruled that the attachment of a Global-Positioning-System (GPS) to a car was a considered a search for purposes of Fourth Amendment protections, and thus may not be used by government officials without a warrant. 132 S.Ct. 945 (2012).
always been a vague concept and is only further complicated by the challenges digital technology has introduced to privacy law.

This report discusses the potential risks to students when districts incorporate technology by considering who is collecting data and why it is problematic. The report focuses on privacy violations that are likely to occur due to a district’s increased use of technology and explores questions such as, “What are students’ expectations of privacy in digital technology?” and “What is a district’s duty to protect students from privacy invasions?” Where answers are not yet available, the report provides relevant information that districts need to contemplate as they implement technology devices and programs in their schools. The report begins with an overview of federal and California privacy laws and other laws that regulate technology use. Then it takes a look at how student privacy is compromised and who are the biggest contributors to student privacy invasions and why. Based on the law described in the first two sections, the report then discusses students’ privacy expectations in digital technology, and the implications for school districts.

For those desiring a more detailed legal analysis, a longer version of this report can be found in the *Journal of Law and Education*, (Volume 44, Summer Issue). That article gives a lengthier discussion of the laws that affect student privacy as well as the ways in which technology is used to extract data from users. The *Journal of Law and Education* article also provides more examples as well as a deeper analysis of some of the privacy concerns that are emerging in the public school system.

**Overview of Relevant Law Affecting Student Privacy**

The United States Constitution does not guarantee privacy specifically, but there are constitutional limits to how far the government can intrude into an individual’s private life. The Fourth Amendment establishes some of those limits by ensuring the right to be free from unreasonable search and seizure of body, house, papers, and effects. In addition to the Fourth Amendment, the First and Fourteenth Amendments also protect personal autonomy. The First Amendment safeguards personal autonomy by protecting the right to speak freely and peaceably assemble, while the Fourteenth Amendment ensures substantive due process. The Ninth Amendment protects privacy indirectly because it holds that even if a right is not explicitly mentioned in the Constitution, the government may not infringe upon that right if it has been granted through other means.

Unlike the Constitution, there are many federal statutes that directly address privacy concerns such as the Privacy Act of 1974. Some statutes specifically concern digital privacy, like the Electronic Communications Privacy Act, while others are even more specific and address the digital privacy of students or minors. Additionally, there is a significant amount of California law that complements federal law and sometimes even extends beyond federal protections.
Though not comprehensive, the tables below gives a synopsis of much of the relevant federal and California laws that currently affect student privacy. The reader is advised to look through the table before reading further so that the federal and California laws that are referenced in the ensuing discussion are understood.

<table>
<thead>
<tr>
<th>Federal Law:</th>
<th>What It Says:</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Const. amend. IV</td>
<td>Ensures freedom from unreasonable searches and seizure of body, house, papers, and effects.</td>
</tr>
<tr>
<td>U.S. Const. amend. I</td>
<td>Protects the right to speak freely and peaceably assemble.</td>
</tr>
<tr>
<td>U.S. Const. amend. XIV</td>
<td>Ensures substantive due process.</td>
</tr>
<tr>
<td>U.S. Const. amend. IX</td>
<td>Recognizes that inalienable rights exist beyond what is enumerated in the Bill of Rights. The Ninth Amendment holds that even if a right is not explicitly mentioned in the Constitution, the government may not infringe upon that right if it has been granted through other means.</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g (2013); AND Code of Federal Regulations, CFR 34 C.F.R. §99.3</td>
<td>Prevents unauthorized sharing of information in education records. However, the School Official Exception allows schools to disclose personally identifiable student information to other school officials, teachers, or vendors who perform functions for the school that would otherwise be performed by a school employee. The school must maintain direct control of the data in order to provide parents with access to the records when requested. FERPA doesn’t define “personally identifiable information” (PII) but the Code of Federal Regulations defines the term as including student’s name, names of family members, addresses, “personal identifiers” such as social security numbers and biometric records, other indirect identifiers such as date or place of birth, mother’s maiden name, or any other information that “alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.”</td>
</tr>
<tr>
<td>Children’s Internet Protection Act (CIPA), 20 U.S.C. §9134(f) (2010); Neighborhood Children’s Internet Protection Act (NCIPA), 47 U.S.C. §254(h) (2008)</td>
<td>CIPA requires public libraries and schools receiving federal funds under the E-Rate program or the Library Services and Technology Act to implement Internet safety policies for minors that block access to visually inappropriate material. NCIPA requires schools and libraries to implement Internet safety policies addressing the accessibility of inappropriate material on the Internet, the safety and security of minors while using email and other forms of Internet communication, and the unauthorized disclosure of PII.</td>
</tr>
<tr>
<td>Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§6501-6506; 16 C.F.R. §312.2</td>
<td>Prohibits certain commercial website operators from collecting PII from children under age thirteen without first obtaining “verifiable parental consent.” Affected website operators must provide notice of their data collection policies. Parents may review personal information collected from a child and may refuse permission for further use at any time. Personal information may only be retained for as long as is necessary to fulfill the purpose for which the information was collected. Once that purpose has been fulfilled, the information must be deleted. PII includes: first and last name, physical address including street name and name of a city or town, online contact information [such as email address], screen or user names, telephone number, social security number, any persistent identifier that can identify a user over time and across different websites or online services, a photograph, video or audio file where such files contain a child’s image or voice, geolocation information, or information concerning the child or the parents of the child that the operator collects online from the child and combines with an identifier described above.</td>
</tr>
<tr>
<td>Protection of Pupil Rights Amendment of 1978 (PPRA), 20 U.S.C. §1232h (2002)</td>
<td>Governs the administration of surveys soliciting specific categories of information, and imposes certain requirements regarding the collection and use of student information for marketing purposes. Schools must give notice to obtain written consent from and provide an opt-out opportunity to parents before students can participate in commercial activities that involve the collection, disclosure, or use of personal information for marketing purposes, unless the vendor is using student data solely for the purpose of developing, evaluating, or providing educational products or services to students or schools. PPRA defines PII as individually identifiable information including a student or parent’s first and last name, a physical address, a telephone number, or a social security number.</td>
</tr>
</tbody>
</table>
### California Law:

<table>
<thead>
<tr>
<th>What It Says:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ca. Const. art. 1, §1</strong></td>
</tr>
<tr>
<td><strong>Cal. Civ. Code §1798.29 (2014)</strong></td>
</tr>
<tr>
<td><strong>Privacy of Pupil Records, Cal. Educ. Code §§49073, et. seq. (2014).</strong></td>
</tr>
<tr>
<td><strong>NEW LEGISLATION Cal. Bus. &amp; Prof. Code §22580 (2015)</strong></td>
</tr>
<tr>
<td><strong>California Online Privacy Act, Cal. Bus. &amp; Prof. Code §§22575 et. seq. (2014)</strong></td>
</tr>
<tr>
<td><strong>NEW LEGISLATION Student Online Personal Information Protection Act (SOPIPA), SB 1177, Steinberg (2014), will become Cal. Bus. &amp; Prof. Code §§22584-22585</strong></td>
</tr>
<tr>
<td><strong>Cal. Educ. Code §49062</strong></td>
</tr>
<tr>
<td><strong>Cal. Educ. Code §36182.5 (2014)</strong></td>
</tr>
<tr>
<td><strong>NEW LEGISLATION Cal. Educ. Code §49073.6</strong></td>
</tr>
<tr>
<td><strong>Cal. Educ. Code §49073.1</strong></td>
</tr>
</tbody>
</table>
Who is Collecting Data, How is it Being Collected, and Why Does it Matter?

As districts begin to incorporate technology into their schools, especially where one-to-one programs are in place, it is imperative that they understand the actions that expose students to risk and why. There are three main groups that are interested in data collection. These include advertisers, criminals, and the government. Each group wants different information for varying reasons, but they are all using technology to access the information they are seeking and are jeopardizing students’ privacy in the process. Of course, as individual consumers, we are all at risk of privacy invasion when using the Internet, but students in particular are a vulnerable group because of their exposure to online dealings both at home and at school as well as their maturity level and their lack of inhibition with regard to sharing personal information online. The following sections will discuss how each of the three main data collectors (advertisers, criminals, and government) uses technology to infiltrate technology users’ lives and gather private data.

Advertisers

Advertisers want to reach large audiences efficiently and effectively. They do this using a process called “targeted advertising,” which allows marketers to place advertisements in front of groups of consumers based on various traits such as demographics and other behavioral variables. This kind of behavioral targeting uses information gathered about individual consumers’ habits so as to gain insights about the types of products and services that an individual is likely to purchase. Marketers can then strategically place advertisements in front of an individual that are specifically tailored to that individual. One of the most efficient ways to collect data about individual consumers is by tracking their activity online. As a result, data mining has become a lucrative business.

The Data Collection Process

Data miners are able to collect information about Internet users and their behavior through many means—some of which are very familiar to the public, such as tracking activity through the use of cookies, while others are less familiar, like a process called fingerprinting.

In the past, every digital device was designed to have its own Internet Protocol (IP) address, which could be used to identify the web activities of each device by recording the websites the IP address had visited. Data miners have now maneuvered away from this approach. Because of the proliferation of devices, the average American owns four devices.

---

3 Mary Graw Leary, Reasonable Expectations of Privacy for Youth in a Digital Age, 80 Miss. L.J. 1035 (2011).
more connected devices than there are unique public IP addresses⁵ and advertisers want to be able to create a user profile even if the user has access to multiple devices. Thus, data miners are now using a process called “householding” to track users’ online activity. This process is also sometimes referred to as “multi-screen” or “cross-device” identification, and it has the ability to track across multiple devices so that each device is associated with one user or household. The information gathered across devices can be layered and compiled into one user profile. This means that unique identifiers that were once linked to individual computers are now more closely tied to the individual using a device.

More than any other tracking method, householding has major implications for school districts with one-to-one technology programs regardless of whether the program is supplied through district-owned devices or through a Bring-Your-Own-Device (BYOD) program. Householding allows data collection to occur across devices regardless of whether or not they are owned by a district or owned privately by a student. It creates potential for any activity that a student engages in at home on a personal device to be linked to activity conducted by that student at school on a district-owned device. Householding is able to identify every device the student uses, regardless of who the owner is, where that device is used, and for what purpose. Therefore the line between data collected from the student on the student’s own device on his or her own time, and data collected from the student while using a district device at school is virtually eliminated. Data miners are not likely to distinguish between data collected at school from data collected at home. Nor are they likely to distinguish between data collected on a district device and data collected on a personal device. All devices are capable of being linked to one individual and all data collected across devices can be compounded and cross-referenced to create a broader image of who an individual user is.

Other methods of data mining include using search engines such as Google or Yahoo! to collect user information. Search engines have the ability to track IP addresses, but they can also track any terms that were used in the search, the time that the search occurred, as well as other data.⁶ This has implications for students who may be using district devices to search personal information about themselves or others. For example, if a student ran a Google search of her name and social security number, Google would have a record of that data, and it would be linked to the device that was used in the search. Additionally, when an individual uses the same entity for a search engine and an email account, such as Google and gmail, the search engine can then tie the email login to the searches as well.⁷ As this occurs, data collection becomes no longer tied to the registered owner of the device, but rather is tied to the individual user.

---

⁷ Id.
Smartphones and tablets, like computers, have their own IP address, and thus can be tracked in the same manner that a computer can be tracked. However, service providers for smartphones are also able to collect information about incoming and outgoing calls (including phone numbers and duration), how frequently users check email or access the Internet from the phone, and the user’s location. Most individuals who use smartphones and tablets use mobile applications (apps) rather than an Internet browser, to access the Internet and its features. Apps can provide a wide variety of functions ranging from mapping services, to games, to flashlights – all of which make them attractive to users. The apps often have a dual function however. Naturally, they deliver the content or service they are designed to provide, but they are also advertising gold mines. Particularly where an app is free to download, developers make money either by selling space within the app to advertisers who can market to a captive audience or by collecting data from the unsuspecting user and then selling it to marketing agencies. Generally, the type of data collected includes phone and email contacts, call logs, Internet data, calendar data, data about the device’s location, the device’s unique IDs, and information about how the user engages with the app itself. Some apps have a user agreement alerting users to their data collection policies, but the privacy policy (if it exists at all) does not always identify what data are being collected, how long the data are being stored, where the data are being stored, and who may ultimately end up receiving the data. Thus, these policies are often unleashed on users who are unaware their data are being harvested. For example, Angry Birds, which was one of the first games made for a smart phone, collects from users personal information (such as location data) that is unnecessary to run the game. In fact, a recent Wall Street Journal investigation of 101 smartphone apps found that almost half were tracking the phone’s location, fifty-six shared the phone’s unique ID number, forty-seven transmitted the phone’s location, and five shared the user’s age, gender, and other personal details such as contacts list.

Victims of this kind of privacy invasion extend beyond just the users of mobile apps. Any of the users’ contacts are also at risk of having information collected. Of course, contact information such as phone number and email address will be collected if the users’ address book is accessed, but any information offered in an email or text message may be intercepted and collected as well. Districts with one-to-one technology programs need to be careful where students download and use apps for classroom or homework assignments. The Family

---

11 Cheryl Conner, Your Privacy has Gone to the [Angry] Birds, Forbes (Dec. 05, 2012), http://www.forbes.com/sites/cherlysnapconner/2012/12/05/your-privacy-has-gone-to-the-angry-birds/.
Educational Rights and Privacy Act (FERPA) does not appear to cover any information collected by a third-party app operator. While the Protection of Pupil Rights Amendment (PPRA) recognizes the need for policies addressing the protection of personal student information, it does not actually offer any such policy. Rather, it places the responsibility of drafting these policies on school districts and leaves to their discretion what the policies entail. The Children’s Online Privacy Protection Act (COPPA) only protects students up to age 13, so student information accessed in this manner can be easily collected without federal violation.

Thus, the question arises, whose responsibility is it to protect students from exposure to data collection in this situation? Do parents or students have the right to opt out of an assignment that requires the use of a mobile app? How can students who wish to maintain anonymity protect themselves? What rights do they have? The answers to these questions remain unresolved. However, as more legislation is introduced and as case law on the subject develops, answers will surely begin to emerge.

As technology advances, the trend is to move information storage and hosting from tangible dedicated servers to cloud computing. In general, cloud-computing platforms allow users to access software applications through web browsers which enable them to store files and email on the Internet. Cloud computing is attractive to school districts because it requires less maintenance, and it is cheaper and more efficient. Cloud storage allows users to access files from any device that has Internet access, thus the cloud can be used to increase student access to learning activities and enhance the ability of students to collaborate with each other or receive feedback from teachers. However, the cloud has also opened the door to advertisers looking to access personal information.

One of the problems with cloud computing is that most cloud providers who do not charge for their services are funding their services through advertising to their clients or through data mining. For example, Google, Yahoo, and Hotmail are all email providers that use the cloud, but they are able to provide free services because of the money they make by selling user information to data collectors and by selling targeted advertisements created from the collected data. The major problem with this is that even though most companies promise to remove identifying information from data when they mine them, once the data have been transferred to a marketer, data aggregators can recombine information to re-identify an individual. Most people are aware that marketers have the ability to track online interactions.

13 This may be changing in the future. Early in 2015, the House of Representatives heard testimony from several experts regarding the ways in which FERPA is falling short of protecting student privacy. This is an indication that the House is considering updating FERPA. Technology And Student Privacy: Before the H. Comm. on Education and the Workforce 114th Cong. (2015) (statement of Todd Rokita, Chairman Subcomm. on Early Childhood, Elementary, and Secondary Education).
15 Id. at 885.
However, the aggregation of data compiled from pieces collected creates a substantial issue: it can turn non-personally identifiable information (non-PII) into personally identifiable information (PII), virtually eliminating the distinction. There is a wide misperception that if specific identifiable information, such as name, address, or social security number, is not voluntarily given, an individual can operate online anonymously.16

Unfortunately, the problem is not unique to cloud computing and exists any time data collection is occurring. For example, the combination of three seemingly innocuous, and relatively available pieces of information—gender, zip code, and date of birth—are sufficient to accurately identify 87% of individuals in the United States.17 When this concept is applied to data mining through the collection of a student’s web search terms and other text from messages and online documents, the aggregation of data can combine to form a well-developed profile of the individual. There is no sense of anonymity by the time the information is sold to an advertiser.

The Problems With PII
The ability to aggregate data to compile a portrait of an identifiable individual is particularly problematic for schools because of the restrictions on PII in federal legislation. As noted in the table above, many laws, including FERPA, PPRA, and COPPA, center on the concept of what constitutes personally identifiable information. Under FERPA, PII cannot be shared without parental consent; under PPRA, proper notification must be given before PII may be collected for commercial purposes; COPPA prevents the collection of PII without consent from children under the age 13. Therefore, whenever a student’s personal information is at issue, some law is likely to apply. Identifying which laws apply can be difficult, especially when the collected information might not become PII until after the transaction at issue has occurred. Some of the laws have broadened their definitions of PII to include data that are not traditionally linkable to a student, such as geolocation. However, each law has its own definition of PII, making it harder to keep track of when a transaction might trigger federal or California law.

Although the definitions of PII used in FERPA, PPRA, and COPPA now cover a lot of personal information that in the past would not have been considered PII, they cannot protect student identities if student information exists elsewhere. The collection of a seemingly harmless piece of information, such as a movie review, can be enough to identify an individual if there is relevant information available elsewhere. Although FERPA specifically declares that its list of items that can be defined as PII is not exhaustive, and COPPA’s list is even more extensive than FERPA’s (it includes identifiers such as photographs, video and audio files containing a

child’s image or voice, and geolocation information), as seen above, even these protections may not be enough to protect student privacy.

**What is a District’s Responsibility to Protect Student Privacy?**

As made apparent in the discussion above, it is safe to assume that in today’s technological climate, almost every digital interaction is at risk of being monitored. Information is collected from online interactions done on every type of device—from computers to tablets to smartphones and everything in between. When a district requires students to use digital technology in the course of their academic work, whether the device is personally owned by the student, as in a BYOD program, or the district issues the device, what kind of responsibility does the district bear for protecting the student’s digital interactions? If the district is responsible for protecting student privacy, does that responsibility vary depending on whether the digital interaction is completed in furtherance of course work or simply done for the student’s recreation?

Schools must comply with the Children’s Internet Protection Act\(^\text{18}\) (CIPA) and the Neighborhood Children’s Internet Protection Act\(^\text{19}\) (NCIPA), which are designed to protect students from exposure to inappropriate visual content through web filtering and from other harmful interactions such as unauthorized data collection through an Internet safety policy. The key components of these laws are set forth in the table at the start of this study. These are valuable laws, but they merely protect students from those precise interactions. They do nothing to protect student privacy. This is because CIPA is designed to protect minors from exposure to pornography, but it is not designed to protect against other non-visual communications on the Internet. Consequently, CIPA leaves minors unprotected from other forms of inappropriate or harmful interactions on the Internet, including data mining and exposure to cyberbullying. NCIPA tackles this problem in part by requiring schools to adopt and implement an Internet safety policy that addresses the accessibility of inappropriate material on the Internet, the safety and security of minors while using email and other forms of Internet communication, and the unauthorized disclosure of personally identifiable information. However, these policies do not address data collection by advertisers.

Schools also must comply with FERPA, which protects student records from being released to unauthorized parties. However, this is also inadequate to protect student privacy in all of the ways in which invasion occurs. One of the most pervasive problems associated with student privacy is the collection of data based on an individual’s digital interactions. Information is collected with every interaction, but even where precautions are taken to eliminate personally identifying information, data may become identifiable and all the more so

---


revealing when the data are pieced together with other personal information that has been collected and stored.

**Problems Arising Under FERPA**

Under FERPA, schools are required to protect any information that is held in the student record, but when third parties are collecting data, FERPA not only falls short of protecting student privacy, but it also creates some rather onerous responsibilities for school districts.

FERPA potentially fails to protect student privacy because even though it prohibits school districts from sharing information held in the “education record (or personally identifiable information contained therein…)” the education record is defined as those documents, records and files that are *maintained by an educational agency.* Critics have argued that FERPA may not cover situations where students are using digital devices to directly interact with websites or apps that collect information because the website or app operator may be collecting information from the student that was never a part of the educational record. Of course, some students may be protected from this type of data collection under PPRA and COPPA, but even these protections are limited at best. PPRA appears to only focus on data collected from students through direct questioning such as through surveys, analysis or evaluation, and does not seem to address many of the ways in which data are collected via engagement with the Internet and mobile apps. COPPA, on the other hand, deals directly with data collected from student interactions on the Internet, but its protections only extend to students up to age 13, essentially leaving out almost half of K-12 students. Furthermore, many of the website and app providers who market to schools have found ways to work around these restrictions as discussed in the “Problems Arising Under COPPA” section below.

Another weak point in FERPA’s language comes from the “directory information” exception, which allows information such as students’ names, addresses, and telephone numbers to be released unless parents are given the opportunity of opting out at the beginning of the school year. Given the routine use of this type of information in class lists, athletic rosters, and the like, many parents choose not to opt out. Because directory information may be shared without violating FERPA, this creates an opportunity for advertisers to use directed marketing to students. Additionally, as described in earlier sections, access to seemingly harmless pieces of information can be combined with other data collected elsewhere to create a much more encompassing picture of an individual. Thus, marketers who are in the business of aggregating data may look to schools’ directories for easy access to information that can be combined with other data at a later point.

In addition to FERPA’s weaknesses when it comes to protecting student privacy, the responsibilities that are placed on school districts can be quite burdensome because federal

---

regulations further defining FERPA, as well as California law,²¹ carve out a “school official” exception that allows student data to be shared with vendors who contract with a school to perform a function that would otherwise be performed by a school employee.²² This exception attempts to maintain protections for student privacy because under the regulation, the vendor must have a legitimate educational interest in the information and the vendor is prohibited from re-disclosing the information without consent from the school and written permission from the parent.²³ However, the school must be in direct control of the vendor’s use and maintenance of the data.²⁴ This is also true under a new section of the California Education Code.²⁵ This means that the district must be able to provide access to such data to any parent who requests it.²⁶ Districts should keep this in mind when contracting with vendors. Their agreements must include provisions that allow for either direct or indirect parental access. It also means that for every vendor that collects and maintains student data on behalf of a school or district (for example a biometric identification system), the district must keep a record of who has accessed the data and what information was shared.²⁷ This task can become arduous, especially for districts that have hired third party vendors to help reduce some of the time commitment, manpower, and resources necessary to perform the original function.

Furthermore, districts need to be cautious when entering into what are commonly known as “click-wrap” agreements, which offer licenses for software and are extremely easy to accept. Such software licenses are frequently available through simple Internet downloads. While the software terms may vary widely, a user confirms acceptance of the terms by clicking an “accept” button in a pop-up window or dialog box. Typically, these agreements are not negotiable and may not be compliant with FERPA and other California law. These are enforceable agreements, and if the terms allow third-party access to FERPA-protected information but do not allow a district to maintain “direct control” over the use and maintenance of that information, this could create problems for the district.²⁸ Thus, districts are wise to discuss ahead of time which employees have the authority to enter into such agreements so as to avoid the potential situation where an unsuspecting employee unwittingly obligates the district to a software license agreement that is not FERPA compliant.

Additionally, not all companies are forthcoming with how they use consumer information, or even intentionally misrepresent how they use it. A U.S. Government Accountability Office report pointed out that “some web filtering systems used in schools that block student access

---

to certain [websites] also allow the company that maintains that software to measure and analyze how children use the Internet by tracking which websites they visit and how long they stay there."29 Understandably, this can create problems for a district that thinks it is purchasing a system to protect its students from harmful or inappropriate web content, only to be unintentionally handing over student data directly to the company that is supposed to be protecting them. As mentioned above, under FERPA, a district must maintain control over any student data that are shared with third-parties. If the district is not even aware the information is being shared, how can it ensure control over that data? To complicate matters further, if a vendor does share student data without the requisite permission, the district will not only be prohibited from allowing that vendor to access student data for at least five years, if not more, but the district can also potentially lose funding.30 Therefore, not only must a school or district carefully monitor third party vendors who are collecting student data, but also if a violation does occur, that school or district will be unable to benefit from the services for which the vendor was hired.

There is a strong likelihood that FERPA will be amended in the near future. In February 2015, Congress held hearings to obtain testimony from industry experts on the ways in which FERPA no longer adequately protects student privacy in the 21st century. These hearings suggest Congress is preparing to introduce legislation to amend FERPA.

Problems Arising Under the Children’s Online Privacy Protection Act (COPPA)

Although COPPA does not obligate schools directly, it does pose some of its own issues for school districts that are using applications and programs that allow third parties to collect student data for those up to age 13. Under COPPA, upon obtaining parental permission to collect student data, website operators must provide a privacy policy explaining their collection practices. These privacy policies can include an option to unilaterally amend the policies, leaving to parents the task of regularly monitoring the policies to ensure their children are not unknowingly subjected to unacceptable privacy exposures. While COPPA does grant parents the right to refuse permission to store or use a child’s personal information at any time after permission has been granted, when continued data collection is the default it only furthers the parental burden of monitoring which websites are collecting what information. Although this is not necessarily a burden for school districts, they should be aware of this potential because of the ways in which website operators and mobile app providers have managed to shift responsibility from themselves to schools.

---

A perfect example of this comes from one of the more popular providers, Google. A cheaper option than the popular iPad, Google Chromebooks are being used in schools across the country, and now Google is offering schools an educational suite package called “Google Apps for Education” which includes services for email, calendar, and chat among many others. Google is advertising their product so as to be particularly attractive to schools, including the fact that K-12 Google Apps for Education users will not see ads when using their school account.  

Google Apps for Education is governed by COPPA because it is an online service that is directed to children. Google’s user agreement recognizes the need to comply with COPPA. However, it explicitly states that the “customer acknowledges…that it is solely responsible for compliance with” COPPA (emphasis added). Thus, through the terms of its user agreement, it appears Google has shifted the responsibility of obtaining parental consent from itself (as the vendor, obligated under the statute) to the school district (as “the customer” in the user agreement). Therefore, under the user agreement, Google can (and does) collect student data, but districts must do their part to ensure compliance with the law by obtaining the requisite parental consent. This has the potential to place parents in a difficult position of having to choose between consenting to Google’s privacy policies or refusing to allow their child to participate in the educational activities associated with the Google Education App. If the district does not obtain consent from a parent, then the district is left with the problem of providing alternative instruction for that student, or declining the Google package. This may also raise legal concerns regarding equal educational access for all students.

Because Google’s privacy policy is the same for all users, districts have little say in ensuring student privacy even where parents agree to the terms. This is particularly true because Google reserves the right to unilaterally amend its privacy policy, which essentially renders the policy meaningless. Google does not directly notify individuals of policy changes, but rather posts updates to the Google Privacy Policy page. This can create an onerous task for districts and parents who must continuously monitor privacy policies to ensure private

---

33 Id.
34 This practice landed Google in the middle of a lawsuit in 2013. 2013 WL 5423918; Benjamin Herold, Google Under Fire for Data-Mining Student Email Messages, Education Week (Mar. 26, 2014) http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html?cmp=ENL-EU-NEWS2; Additionally, HISD declined to incorporate Google Apps for Education due to the controversy surrounding how Google handles student information.
information is not being collected and shared.\textsuperscript{36} The bottom line is that the burden is on schools to investigate the services that providers offer. Schools should think about whether they are trading the electronic privacy of staff and students in order to access technology, though at this point in time there does not appear to be a legal responsibility to do so as long as FERPA and PPRA requirements are being met.\textsuperscript{37}

Another problem with the Google model is that it combines data collected from students using the Education Apps with information gathered from other Google services.\textsuperscript{38} This means that Google may elect to use data aggregation to combine student information from the Education Apps with other information gathered from personal use of Google applications. Google states that they require opting in for sharing of sensitive information,\textsuperscript{39} which refers to only a small grouping of highly personal information including "confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality."\textsuperscript{39} Thus, there is a large range of information that can be collected outside of this narrow definition, and consequently shared with user consent. Of course, as already explained, user consent is somewhat illusory because of the ephemerality of the privacy agreement.

There has been movement in Congress indicating that new legislation addressing student privacy will be introduced in the near future. U.S. Representatives Jared Polis and Luke Messer have sponsored a bill known as the Student Digital Privacy and Parental Rights Act. As of the time of this writing, the bill has not yet been formally introduced to Congress, however if it is introduced and passed into law, it may address some of the gaps in student privacy rights that COPPA does not cover. Introduction of the bill was originally slated for March 2015, but was postponed due to criticism from both privacy advocates (who feel the bill is not restrictive enough to address growing privacy concerns) and technology groups (who

\textsuperscript{36} This predicament seems to have been somewhat alleviated in 2015 when Google joined several other technology companies in signing the Student Privacy Pledge. However, critics still feel more is required to ensure student privacy. As part of the pledge, the companies promise to “not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.” studentprivacypledge.org/?page_id=45 (last visited Mar. 5, 2015).

\textsuperscript{37} Google Apps for Education also creates a burden for school districts to comply with FERPA requirements. The Apps for Education user agreement explicitly asserts that Google is considered a “school official” for purposes of applying the school official exception created under FERPA. As mentioned earlier, the school official exception allows a district to give student information to a third-party vendor provided the district remains in direct control of the student information. This may have the potential to create a substantial burden for a district that is tasked with maintaining direct control over data collected by Google. Although the user agreement states that Google will comply with FERPA, districts must be careful to ensure that compliance in fact is occurring. This is because unlike COPPA, the district is the only party liable for a FERPA violation.

\textsuperscript{38} Id.

prefer self-regulation). At this time, one can only speculate whether the bill will get passed as it currently exists, but the reader should be aware of the potential for new federal legislation on the subject.

Considerations for Districts When Contracting with Service Providers

Data mining is a highly lucrative business, and so many service providers that engage in data collection can afford to offer their services free of charge to their clients in exchange for information. Most districts are on tight budgets and the financial burden of having to pay for technology software and other applications can be daunting, making free services very appealing. Section 35182.5 of the California Education Code prohibits schools from entering into a contract for electronic products or services if the contract requires the dissemination of advertising to students unless the product or service would be integral to education and the product is not affordable without contracting to permit the dissemination of advertising.

Under new California law going into effect in 2016, service providers will be prohibited from knowingly engaging in targeted advertising to students when the advertising is based upon information that the provider has collected from a student’s use of his or her website or mobile app. Under the new law, the parties will not be able to contract around such prohibitions. Furthermore, service providers are prohibited from using information to amass a profile of a K-12 student, except in furtherance of school purposes. Service providers are also prohibited from selling or disclosing any personally identifiable information. Even though these requirements only obligate service providers, districts may want to look out for terms in a contract that might violate such requirements.

Even when districts can afford to contract for products that do not advertise, there are other factors to consider when selecting service providers. Newly added California Education Code Section 49073.1 allows schools to contract with third parties to provide digital storage, management, and data retrieval of student records as long as the contract affirms that student records will remain the property of, and under the control of, the district. Such contracts also must describe the manner in which the third party will secure the confidentiality of student records, as well as the manner in which the district will maintain compliance with FERPA.

Other aspects of a contract a district might keep in mind when contracting with service providers:44

- **Marketing and Advertising:** Terms of service agreements should be clear that data may not be used to create user profiles for the purpose of targeting students or their parents for advertising and marketing, which could violate privacy laws.
- **Data Collection:** Agreements should include a provision that limits data to only what is necessary to fulfill the terms.
- **Data Use:** Schools and districts should restrict data use to only the purposes outlined in the agreement.
- **Data Sharing:** While providers can use subcontractors, schools and districts should be made aware of these arrangements, and subcontractors should be bound by the limitations in the terms of service.
- **Access:** Federal student records laws require schools and districts to make education records accessible to parents. A good contract will acknowledge the need to share student security controls. Failure to provide adequate security could lead to a violation of FERPA.

#### Criminals

Criminals access personal information in order to commit identity fraud or harass or stalk victims. Technologically savvy criminals are able to use information called geotags to track movements or identify where victims live. Geotagging is the process of adding geographical information to photographs, video, websites, and text messages. Many digital devices, including smartphones and tablets, have the capability to add geotags to content. Often these metadata are embedded unbeknownst to the user. With a simple downloadable piece of technology, the geotag can be viewed by anyone who has access to the image. When an image with a geotag is posted to the Internet along with text giving context clues, just like data miners using aggregation, criminals can easily construct broader spectrum information about their victims. For example, a student might post a picture of a college acceptance letter with the caption, “Look what came in the mail today!” In this example, anyone with access to the geotag technology will know where the student lives, that the student is a senior in high school and therefore between the ages of seventeen and eighteen, what college that student may be attending in the fall, and any other contextual clues in the image. Furthermore, geotags have the capability of establishing patterns of a particular individual. If that individual posts photos on a regular basis, it is easy to determine common locations (e.g., home, school) and the time of day when the individual is expected to be there.

---

Facebook apparently does take precautions to limit geotag information from photographs that are posted on its site.\textsuperscript{45} However, Facebook is not the only social networking website that allows photos to be posted. Privacy policies on such sites are in a constant state of flux, and new sites are popping up all the time. Many people, students included, also have their own personal blog or website, and it is not uncommon for owners of blogs or websites to post photographs or other content that might have geotags attached. Moreover, technology is constantly evolving in ways that allow for circumvention of security measures that were designed to address outdated technology.

Hackers can access entire databases of information to steal identities of their victims. More and more, schools are becoming targets for hackers looking to access names, birthdates, and social security numbers.\textsuperscript{46} At this point in time there is little information indicating what a school or district’s liability would be to students when their private information is compromised. FERPA has no bearing in such cases because FERPA only deals with intentional sharing of student information and not unintentional data breaches.

Although only tangentially related to privacy, schools and districts that are distributing expensive pieces of mobile technology for students to use both in the classroom and at home need to be aware that this practice can cause the school or student to be a target for theft and violence. In 2012, the Cleveland Heights University School District in northeastern Ohio distributed 1,300 iPads to middle school students, but “less than a week after the tablets were

\textsuperscript{45} In a 2011 Security Blog article on WindowsITPro, Jeff James claims that when he contacted Facebook about the way it handles geotagging the response he received was “we make limited use of camera EXIF/IPTC [meta] data. EXIF rotation information is no longer ignored. Photo comments are automatically populated with the IPTC title and caption….we’re looking into more deeply integrating other EXIF/IPTC data into the product, but want to do so in a way that’s reliable and respects the privacy of people on Facebook.” Jeff James, \textit{How Facebook Handles Image EXIF Data}, Security Blog, WindowsITPro, (Dec. 7, 2011) http://windowsitpro.com/blog/how-facebook-handles-image-exif-data.

\textsuperscript{46} For example, the University of Maryland had one of its databases hacked, which compromised the personal information of over 300,000 students, staff and faculty members. In 2010, Ohio State University was the victim of a data breach that exposed the names, birth dates and social security numbers of 750,000 people. Eyder Peralta, \textit{Data Breach At University of Maryland Exposes 309,000 Records}, the two-way (Feb. 20, 2014) http://www.npr.org/blogs/thetwo-way/2014/02/20/280195882/data-breach-at-university-of-maryland-exposes-309-000-records; 300,000 students, faculty and employees at Florida Panhandle college had personal information compromised in 2012, when 200,000 records were stolen by hackers. Associated Press, \textit{200K Students’ Information Stolen in Massive Computer Hacking At FL College}, CBS Miami (Oct. 10, 2012 7:36 PM) http://miami.cbslocal.com/2012/10/10/200k-students-information-stolen-in-massive-computer-hacking-at-fl-college/; Iowa State University students were victimized earlier this year when records containing social security and university ID numbers were hacked. The documents included students who were enrolled between 1995 and 2012. Sharyn Jackson, \textit{Data breach could affect 30,000 Iowa State students}, The Des Moines Register, (Apr. 22, 2014, 12:04 PM) http://www.desmoinesregister.com/story/news/education/2014/04/22/isu-servers-hacked-social-security-numbers-exposed/8006303/.
handed out, more than a dozen students had been mugged on the way home from school.”\(^47\) Eventually the district stopped allowing students to take the iPads home, which frustrated the purpose of obtaining the devices in the first place. In response to this, other districts around the country are taking precautions. But, what is a district’s responsibility to protect students from harm when the district has distributed valuable technology to each student to carry from school to home?

Students are entitled to a safe school environment under both the California Constitution and the California Education Code, but “school districts and their employers have never been considered insurers of the physical safety of their students.”\(^48\) Generally, a school district is not responsible for student safety once a student has left school property. However, there are a few exceptions to this. Section 44808 of the Education Code specifically states that a district will not be responsible or liable for the conduct or safety of a pupil “at any time when such pupil is not on school property, unless…[the district] has otherwise specifically assumed such responsibility or liability or has failed to exercise reasonable care under the circumstances.”\(^49\)

Whether a district assumes responsibility by issuing valuable technology to its students thereby causing the student to be a target for violence is not known at this time.\(^50\) Until the legislature or a court of law rules on this issue, it will remain unknown.

The purpose of Section 44808 is to limit a school district’s liability for injuries to pupils before or after school hours while they are going to or coming home from school. Under the case law of one California court, a district bears no liability for injuries caused to students outside of school property when the district has not specifically assumed responsibility to do so.\(^51\) A court could find that in a situation where students are attacked because of expensive devices they carry, the district has assumed no responsibility and therefore is not liable for any injury. Alternatively, a different California court suggests that where a district can reasonably foresee a substantial risk of injury, the district must take measures to reduce that risk.\(^52\) Under this concept, if a district is aware of the danger posed to students who are carrying technological devices to and from school, a district may be liable for any injury imposed on a student if the district does not take measures to protect him or her. In either case, a district would be remiss


\(^{50}\) The language in the statute is ambiguous. No school district is liable for the safety of pupils not on school property “unless such district…has undertaken to provide transportation for such pupil to and from the school premises, has undertaken a school-sponsored activity off the premises of such school, has other wise specifically assumed such…liability or has failed to exercise reasonable care under the circumstances.” Cal. Educ. Code 544808 (italics added). “The portion of section 44808 that refers to failing to exercise reasonable care does not create a common law form of general negligence; it refers to the failure to exercise reasonable care during one of the mentioned undertakings.” Bassett v. Lakeside Inn, Inc., 140 Cal.App.4\(^{th}\) 863, 871 (2006).


to not consider the conditions of the surrounding community when sending students home with highly valuable equipment.

At this point, it is worth considering that students may be the perpetrators of theft or violence. California Education Code Section 44807 dictates that districts will hold students “to a strict account for their conduct on the way to and from school” as well as while on campus. Teachers and school administrators may use physical control that is “reasonably necessary to maintain order, protect property, or protect the health and safety of pupils, or to maintain proper and appropriate conditions conducive to learning.” Although it is unclear to what extent a district must go to protect students from violence, if the perpetrator is another student, the district assumes responsibility for disciplinary measures.

The Government

When it comes to governmental privacy invasions, violations may be intentional or unintentional. School districts hold stores of student information, which make them susceptible to unintentional data breaches. Unintentional breaches occur when information is inadvertently shared because documents are not properly secured or when sensitive information is shared with an unauthorized recipient. Of course, government records are also susceptible to theft or hacking incidents. While legal guidance in all of these circumstances is lacking, under California law an agency that owns or licenses or maintains computerized data that includes PII must notify any potential victim when a data breach has occurred. Under what circumstances, and to what extent, a school district will be liable to students for a data breach remains unclear. Thus, the focus of this section will be what rights are extended to students for intentional digital privacy invasions by school districts.

There are many reasons a district might intrude on a student’s digital privacy, particularly when it comes to ensuring student safety and enforcing school policies. Districts are charged with maintaining a safe school environment, but with the prevalence of cyberbullying and other inappropriate digital interactions occurring among students, districts are often left unsure about how to address such problems without violating student privacy rights. There is increased pressure for district officials to search electronic devices such as cell phones or

53 Such was the case in June of this year, when Riverside Community College District enrollment information was emailed to the wrong recipient, exposing sensitive information of 35,212 students. Dayna Straehley, Colleges: RCC, Moreno Valley, Norco students’ personal data breached, The Press Enterprise (June 17, 2014) http://www.pe.com/articles/district-696343-students-credit.html.

54 Three computers in the Student Health Center at the University of California Irvine were compromised when a keylogging virus captured keystrokes as information was entered into the computers. The hackers were able to gain information from mid-February 2014 through to the end of March 2014. The information the hackers obtained included names, unencrypted medical information, student ID numbers, mailing addresses, telephone numbers, and payment information such as bank names and check numbers. J Price, U.C. Irvine Student Health Data Breach Hits 1,800, News & Stories, id RADAR (May, 15, 2014, 2:24 PM) https://www.idradar.com/news-stories/identity-protection/UC-Irvine-Student-Health-Data-Breach-Hits-Thousands; https://www.privacyrights.org/data-breach/new.

laptops, or to access a student’s social media accounts and other digital interactions like text messages or blog posts, in an effort to monitor student behavior. Law enforcement agencies in general often use the Internet and social media sites to uncover evidence and identify suspects in a crime. The implication of using social media in this way is that law enforcement and school officials may be able to search and obtain personal information without the need for procedure, and data searches may be initiated without any requisite level of suspicion.

New legislation in California, AB 1442, which went into effect on January 1, 2015, allows school officials to consider using social media to obtain information about students. Under the new law, parents must be informed when a school is considering implementing a program that would allow the school to gather information about a student through social media websites, and then maintain that information in the education record. Under this law, such information would have to be destroyed after the student leaves the district or upon turning nineteen. The law says nothing of a district’s liability for any privacy invasion occurring in contravention of the law.

**Student Expectations of Privacy in Digital Devices**

The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizure of their private effects, papers, homes, and bodies. This is a well-established doctrine within the general public that has been extended to students through case law. The key to Fourth Amendment protection, however, is that it only protects individuals from searches where there is a reasonable expectation of privacy. Moreover, although students are entitled to Fourth Amendment protections, the protection is limited compared to that of the general public. Rather than using the general standard of “probable cause” to justify a search, school administrators may simply rely on the reasonableness of the search given the circumstances under which it takes place. But, how does this diminished standard apply to searches of digital devices? As technology has shifted the traditional limits to where information is kept and how it is accessed, the definition of reasonable privacy expectations has become rather murky. Even the U.S. Supreme Court agrees that “it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” Every time a new piece of technology is invented, there is a paradigm shift regarding what constitutes a reasonable expectation of privacy. Recently, courts have had to contend with applying outdated privacy expectations to the computer, and more recently, the smartphone. Courts are still in debate over how much protection such devices should be afforded, but generally, they are accorded more protection than other items typically found on a person.

---

In general, students have a reasonable expectation of privacy in their personal belongings, and there are even a few cases that address students’ expectation of privacy in digital devices specifically. Unsurprisingly, courts are divided on the issue, thus leaving clear guidance on the subject elusive. In an unreported case arising out of Mississippi, *J.W. v. Desoto County School District,* a student, R.W., was expelled from school after school employees discovered photographs on his phone implicating him in gang activity. Even though possessing a phone on school grounds was against school policy, R.W. opened his cell phone while in class to retrieve a text message from his father. The cell phone was confiscated as a result of the violation, and then three school officials and one police sergeant reviewed the phone’s contents. The court used a common two-part reasonableness test to determine if the search was reasonable under the circumstances: 1) was the search justified at its inception, and 2) was it reasonably related in scope? In light of these questions, the court determined that it was reasonable for school officials to search the phone. The court said the search was justified at its inception because the phone was not permitted on campus and R.W. “greatly increased his chances of being caught with that contraband, and of being suspected of further misconduct, when he elected to use it on school grounds.” The court thought it was “reasonable for a school official to seek to determine to what end the student was improperly using that phone.” The court also found that “the search itself was ‘reasonably related in scope to the circumstances which justified the interference in the first place,’” though it did not articulate why.

Another case, *G.C. v. Owensboro Public Schools,* offers a strong juxtaposition to the *J.W.* case. In *G.C.*, when a student, G.C., was caught sending text messages in class, a school official confiscated his phone and read his text messages. The school official testified that she had looked at the text messages because G.C. had a history of drug use and suicidal thoughts, and she was concerned for his safety. The court expounded on the two-part reasonableness test mentioned above and further defined what it means for a search to be “justified in its inception.” A search is “justified in its inception,” the court said, “when there are reasonable grounds for suspecting that the search will garner evidence that a student has violated or is violating the law or the rules of the school, or is in imminent danger of injury on school premises.” Continuing with its elaboration, the court said, “a search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.” Furthermore, “[i]n determining whether a search is excessive in its scope, the nature and immediacy of the governmental concern that prompted the search is considered.”

Using this explanation, the court disagreed with the way the *J.W.* court had applied the legal standard of evaluating the reasonableness of the search. It rejected the *J.W.* court’s logic that

---

60 This is an unreported case, and thus not binding authority. 2010 WL 4394059.
61 711 F.3d 623 (6th Cir. 2013).
simply because a student is caught using his cell phone, the school is justified in searching his phone. Instead, the court felt that a “search is justified at its inception if there is reasonable suspicion that a search will uncover evidence of further wrongdoing or of injury to the student or another.” It then emphasized that “[n]ot all infractions involving cell phones will present such indications.” Ultimately, the court applied this logic to the facts before it and determined that the search was not justified in its inception. Even though G.C. had a history of drug abuse and depressive tendencies, this fact without more, was not sufficient to justify a search. There was no evidence to suggest that G.C. was engaging in unlawful activity or contemplating injury to himself or to others. Rather, the evidence indicated that G.C. was sitting in class when his teacher caught him using the phone. The court felt this did not indicate that a search would reveal evidence of criminal activity or potential to harm anyone in the school. Thus, while J.W. stands for the likelihood that searches of student cell phones are reasonable, G.C. stands for the likelihood that they are not.

J.W. and G.C. provide opposing viewpoints on a district’s authority to conduct a search of a student’s digital device, and as such these cases do not offer much guidance to school administrators who engage in searches of student devices. Moreover, these cases do not give any insight into a school’s ability to search a device that has been issued to a student by the district under a BYOD digital policy. With many districts implementing, or looking to implement a one-to-one technology program, this question remains problematic. Neither J.W. nor G.C. gives insight into Fourth Amendment concerns arising from school searches of a district-issued device, which would presumably be the target of a search where students are using such devices. Arguably, a student may have a further diminished expectation of privacy in a district-owned device than in his or her own personal cell phone or computer, but this has yet to be determined. This is due in part to the fact that presumably, a district’s responsible use policy governing student use of district devices would address the scope of a reasonable search. However, a responsible use policy does not guarantee that a district’s actions are constitutional.

Although it is not a school law case, U.S. v. Finley does offer a little insight into this particular aspect. In Finley, Finley was arrested after driving another man to a truck stop for the purpose of conducting a drug deal. Finley did not take part in the deal, other than to provide transportation. Upon arrest, Finley’s phone was seized and searched. The phone belonged to Finley’s employer and had been issued to Finley for work, but Finely was allowed to use the phone for personal business as well. In determining whether Finley had a reasonable expectation of privacy, the court discussed the distinction between a property interest and a possessory interest in the device targeted in the search. Finley had a possessory interest while his employer had a property interest. The court did not believe that this affected Finley’s expectation of privacy in the device when concerning a government search. “That Finely’s employer could have read the text messages once he returned the phone does not

62 477 F.3d 250 (5th Cir. 2007).
imply that a person in Finley’s position should not have reasonably expected to be free from intrusion from both the government and the general public.” In reaching this conclusion, the court also focused on whether Finley had a right to exclude others from the item or place being searched. Where a person does not have a right to exclude others, his expectation of privacy is diminished.

This case is important because it suggests that even where another party has a property interest in a device, the user of the device may still have a reasonable expectation of privacy in that device. Under this premise, a student may still have an expectation of privacy in a device that is owned by the district. However, in Finley, the entity with a property interest in the phone and the entity searching the phone were distinct from one another. In the case of a district-issued device, the entity searching the device and the entity owning the device would be one and the same. Therefore, the principles established in this case do not necessarily translate to a situation where a school wishes to search a district-owned device that has been issued to a student. It would be reasonable to assume that in such a situation, the school would have more authority to search the contents of a device. Presumably, a school’s authority to search one of its own devices issued to a student would be established in the school’s responsible use policy.

Ultimately, it seems that the two-part test mentioned above in the J.W. and G.C. cases is the standard for student searches. If a school administrator conducts a search that is justified at its inception and the scope of the search is reasonably related to the circumstances that justified it, then this is sufficient to at least provide qualified immunity from liability to the official conducting the search, if not to justify the search in the first place.

**Conclusion**

Advances in technology have brought significant changes to the ways in which schools conduct business. Technology has eased the burden for school districts that are tasked with managing databases of information on students and employees. Mobile technology has created wonderful learning opportunities for students and teachers. Technology can even create greater opportunities for parents to engage with what their children are learning in school. But, with these advantages come some great challenges, particularly when it comes to protecting student privacy. A lot of questions remain unanswered, but as more statutory and case law develops, certainly some of the issues presented by use of technology in schools will become clearer.

One of the biggest concerns for student privacy comes from the way data can be collected during ordinary online activity. Data miners have become so sophisticated that school districts often do not recognize when and where third parties are collecting student data. Likewise, attempting to keep up with the way in which technology is being used to collect data can be futile because technology, and data collection along with it, continues to evolve.
Criminals are also becoming more adept at infiltrating databases, leaving less sophisticated district technology at risk of being hacked and student information susceptible to exposure or theft. Finally, as more devices are being used in the classroom, teachers and administrators are faced with the delicate balance between needing to monitor student online activity and not infringing on students’ right to privacy when using digital devices or the Internet.

Further complicating all of these issues is the fact that the law addressing these issues is often vague and sometimes even nonexistent. Technology is advancing at a rapid rate and where relevant law exists it has evolved piecemeal, making it difficult to identify and understand how the law applies. Additionally, both federal and state law apply to student privacy issues, as well as local regulations, so more layers must be considered when attempting to decipher the legal puzzle.

Because of the responsibility placed on districts to protect student privacy and the sensitivity of the personal student information that is at risk, districts—particularly those that have or are considering implementing one-to-one technology initiatives—would be wise to consider student privacy issues prior to beginning a technology program. Addressing these concerns in district policy manuals, handbooks, and responsible use policies as well as seeking advice from legal counsel is also recommended.