

**OHIO SCHOOL BOARDS ASSOCIATION  
2016 CAPITAL CONFERENCE**

**OCSBA SCHOOL LAW WORKSHOP**

Columbus, Ohio  
November 15, 2016

*“Legal Issues for Today’s Hottest Tech Toys”*

Presented by

Gary T. Stedronsky



---

Cincinnati • Cleveland • Columbus

## I. Introduction

## II. Trends in Technology Use

### A. Trends in Technology Use for Educators

Many students (and staff) no longer use traditional PCs to connect to the Internet at home. The vast majority of students have access to mobile devices. Students use mobile devices during the school day to support classroom learning. Students use technology at home to complete homework assignments.

Students in grades 9–12 who use smartphones	86%
Students in grades 6–8 who use smartphones	72%
Students in grades 3–5 who use smartphones	46%
Students who think every student should have access to a mobile device during the school day to support learning	76%
Students who use mobile devices in class to look up information	50%
Students who say they have received better grades by using technology within learning	53%
Students in grades 6–8 who watch online videos for schoolwork	74%
Students who communicate with their teachers by email	48%
<i>Source: Speak Up Survey 2015 from Project Tomorrow</i>	

How does technology rank in terms of importance to students? The top tools depend on the task:

- Laptops – for writing reports, taking online tests, and working on group projects
- Smartphones – for connecting with classmates and accessing social media

### B. A Glimpse into the Future . . .

Artificial intelligence (AI) can be used to grade multiple choice and even essay assignments. Individualized learning software is available that adapts to student needs. AI tutors can help students with homework.

- Interconnected apps
- Wearable devices that contain sensors to gather user data
- Machines that can “learn”
- Autonomous agents
- Adaptive security technology

## III. Gadgets in Today’s World

### A. Unmanned Aircraft Systems (UAS) – aka Drones

Drones have increasingly made their way onto school property in recent years and are used for everything from class projects to coaching tools for athletics. But use of drones on school property may have big implications for districts.

#### 1. Regulation of Drones

All navigable airspace is in the public domain. It is unclear how much states and local governments can regulate drones. The federal government has exclusive sovereignty of U.S. airspace, and the Federal Aviation Administration (FAA) regulates use of this airspace. However, FAA has been slow to pass useful regulations, and drones have presented a danger in several circumstances.

The first UAS regulations were issued by FAA in 1981 for model aircraft. A 2007 regulation made it illegal for any person to operate a UAS in U.S. airspace without specific authority. In 2012 Congress mandated that the FAA create comprehensive UAS regulations. The FAA released “Part 107” in June 2016, effective in August 2016. It is likely that the FAA will need to revise the rules in the near future as people find new ways to use the machines.

It is important to note that exclusive federal sovereignty over airspace does not exclude state regulation over other areas. If the focus of the law is not an aspect of aviation that the FAA actively controls, states may pass laws and regulations. For instance, a plane operator with a license to fly advertising banners sued to challenge a state prohibition on air advertisements. The state law was upheld because it had authority to control advertising. Other examples include criminal prohibitions against stalking, voyeurism, harassment, and the like.

## **2. FAA Regulations – General**

FAA regulations apply to nonrecreational use of drones, not to hobby or recreational use, and are designed to minimize risks to aircraft, people, and property. Drones may fly in Class G (uncontrolled) airspace without air traffic control authorization but need air traffic approval for flight in any other airspace.

Remote UAS pilots must conduct a preflight check of aircraft; make available the aircraft for FAA inspection; and report to the FAA any flight that results in serious injury, loss of consciousness, or property damage of \$500 or more.

## **3. FAA Regulations – Operational**

- Maximum weight = 55 lbs. including cargo
- Maximum speed = 100 mph
- Maximum altitude = 400 feet
- Must be operated in visual line-of-sight (VLOS) of remote pilot or visual observer
- Pilot/observer must be able to see the aircraft with unaided vision, excluding corrective lenses
- May not operate over anyone not directly participating in the operation, under any covered structure, or inside a covered stationary vehicle
- Daylight only, or 30 minutes before sunrise/after sunset
- Must yield right of way to other aircraft

However: “Most of the restrictions discussed above are waivable if the applicant demonstrates that his or her operation can safely be conducted under the terms of a certificate of waiver.”

## **4. Drone Uses and FAA Enforcement**

### **a) Business Use**

FAA can regulate any use that is connected with business/commerce. Businesses must obtain registration and certification, which takes approximately one year. Remote pilots must obtain certification.

### **b) Recreational Use**

FAA is prohibited from regulating recreational use of drones. However, the 400-foot de facto altitude restriction still applies, and FAA may regulate anything that

is a danger to flight safety. Recreational users are subject to mandatory registration (\$5 online).

#### **5. State Regulation of Drones**

State and local regulations may define what a UAS is. States may regulate how drones may be used in law enforcement, how they may be used by the general public, and how they can be used in recreation and sports such as hunting and fishing. In 2013, Idaho became the first state to regulate drones. As of August 2016, laws are in effect in 26 states; however, Ohio has not yet adopted any drone regulations.

#### **6. Recreational (Personal) Use of Drones**

FAA regulations do not apply to recreational users; however, recreational users must keep drones within eyesight, fly aircraft below 400 feet, and not fly aircraft within 5 miles of an airport without permission from the control tower. The FAA developed a smartphone app, B4UFly, to help UAS operators with flight restrictions and requirements.

Section 336 of Public Law 112-95 does, however, apply to recreational use of drones:

#### **SEC. 336. SPECIAL RULE FOR MODEL AIRCRAFT.**

(a) *In General.*--Notwithstanding any other provision of law relating to the incorporation of unmanned aircraft systems into Federal Aviation Administration plans and policies, including this subtitle, the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if--

- (1) the aircraft is flown strictly for hobby or recreational use;
- (2) the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
- (3) the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
- (4) the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and
- (5) when flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport)).

(b) *Statutory Construction.*--Nothing in this section shall be construed to limit the authority of the Administrator to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system.

(c) *Model Aircraft Defined.*--In this section, the term "model aircraft" means an unmanned aircraft that is--

- (1) capable of sustained flight in the atmosphere;

- (2) flown within visual line of sight of the person operating the aircraft;  
and
- (3) flown for hobby or recreational purposes.

## **7. Real Challenges for Schools**

Drones are very popular with students and staff, and it is likely that many careers will rely on drones in the future, which creates a present need to educate students on drones. However, schools must carefully weigh these considerations against others, such as the safety of students, staff, spectators, and property; violations of laws and regulations – FAA rules, FERPA, OHSAA regulations, state laws, and local restrictions; misuse of technology and discipline on the part of both staff and students.

### **a) Policy Considerations**

Likewise, schools are faced with policy considerations about if and how drones may be used on school grounds. As boards of education consider policy options, it is important to consult with legal counsel about FAA regulations, as well as other state and federal laws and regulations. The law is in state of flux, so policies may need to be reviewed and changed frequently. Also consider whether policies and resolutions are enforceable, and if so, by whom:

- By the board of education? The board has the right to control the premises, but remember, airspace is not “premises.” Operators do not need to be present on property to control the drone remotely.
- By local law enforcement? Traditionally, local law enforcement do not have authority to enforce federal FAA rules?
- By the FAA? The FAA has limited control over drones used for recreational purposes.

The legal considerations are more significant than one might imagine. For instance, it is unlikely that staff members will know that they are flying an unmanned vehicle in restricted airspace. Airspace may be restricted temporarily (for instance, cannot fly drones during presidential visit or inaugural parade) or permanently (cannot fly within so many yards of protected buildings, runways, etc.).

### **b) Other Considerations**

Schools will also face other considerations. Classes for drones focus on technical development and regulations, and not on flight. Protection of property and people is a must. Schools should consider whether they should adopt rules restricting use of drones. If schools regulate the use of drones, they would need to have rules in place for both staff and students, as well as avenues for discipline if misused.

OHSAA has urged schools to adopt a resolution prohibiting use of drones on campus. Many schools are banning them at practices and games. Drones are not permitted at OHSAA tournaments in any sport, and it is up to individual schools to decide whether to allow use of them during the regular season.

## **B. Smart Pens and Other Audio-Recording Devices**

### **1. Advanced Audio-Recording Devices**

Many audio-recording devices may be an asset in schools. They may assist with assessments of student and staff performance, provide effective and low-cost

accommodations for students with disabilities, assist with recall about important conversations with parents or other parties, and create a more dynamic learning environment that caters to students with different learning styles.

## 2. “Hot” Tech Toys on the Market

- Smart Pens – Allow user to write notes and record audio at the same time, syncs the two, and wirelessly transfers to mobile device or PC.
- “Spy” recorders – Designed to look like something else, they record audio and sometimes video files that can be uploaded and stored.
- TSAs (Top-Secret Recording Apps) – Downloadable apps for mobile devices that enable a variety of recording and storing features; can even sync with other recordable data.
- R.C. 2933.52 – It is legal to record as long as *one* person involved in the conversation is aware and gives consent (this includes the individual who is doing the recording).

## C. Smart Watches

### 1. Features

Smart watches can be linked to cell phones through Bluetooth up to 12 feet away and can be used to access phone content (cheat sheets). Apps include problem-solving apps. These are in the category of “wearables,” like Google Glass but less obtrusive. Some record video and audio. New features allow users to scroll through documents just by a turn of the wrist.

### 2. School Considerations

Academic dishonesty and student privacy, although not new problems, are a consideration for schools in allowing smart watches. Consider banning smart watches during testing, treating them the same as cell phones. Smart watches may also be used inappropriately by employees.

### 3. How Smart Watch Cheating Can Work



This example is from a paper presented at the International Conference on Financial Cryptography and Data Security in 2014.

The watch has an app paired to a cell phone. During the exam, the smartphone relays data from the cloud-based app to the smart watch. The phone is out of sight in the student's backpack, but it is communicating and relaying the info to the smart watch. The smart watch shows the correct date and time on the face. The app allows students to provide

and view collaboratively decided answers. Students vote for an answer by double-clicking watch buttons. The answers students voted for actually appear on the watch face as pixels on the date and time. Kids easily learn to use this code on the app to get answers. The point is that they are communicating on answers in a way that might not be easily detected.

## **D. Surveillance**

Surveillance technology changes almost daily, and the law has been slow to follow its progression. We will likely see court decisions continue to evolve with the change in technology as systems capabilities change. Even where there is a definitive answer, the law may change over time as implementation and understanding of technology changes, and integration of technology into our lives continues.

### **1. Student and Staff Surveillance Issues**

Within these two groups are different legal issues with surveillance video. Among students, video surveillance implicates student privacy laws, which keep student information confidential. How privacy laws affect who may view surveillance video and when, or what steps need to be taken for the school to disclose or share the video, is the source of much confusion – and rightly so, as the current guidance is not especially clear.

The **Family Policy Compliance Office (FPCO)** is a federal agency that issues guidance in response to **FERPA** issues. They have issued some official guidance, but their advice has changed over the years. Despite repeated requests for further official guidance, FPCO has not clarified their position on how to interpret FERPA as it relates to the issue of videos in school.

**Law enforcement unit records** are another exception to FERPA as it relates to surveillance videos of students. The common questions about surveillance videos are *who* can see the video and *when* they can see it.

For staff, however, the use of surveillance video brings up different legal issues. Using surveillance video of staff members generally boils down to whether there is a **reasonable expectation of privacy** – for example, in the bathroom, in the break room, or at their desks.

Has the district provided **notice** that staff may be taped? Do any provisions of a **collective bargaining agreement** affect the issue, or should it? Does an employer have a management right to tape its premises? Employee discipline from evidence caught on surveillance cameras is, of course, where much of the litigation arises.

Another issue is what the staff make available on **social media**. How far does the employer's right to keep tabs on its employees and their speech extend? This is an evolving issue, but case law is developing. The **First Amendment** right to free speech and the **Fourth Amendment** rights of privacy and freedom from unreasonable search and seizure are **constitutional** issues.

### **2. Students and FERPA**

#### **a) FPCO Guidance**

Under the FPCO's *official* guidance, which was issued in 2004 – (think how much technology has changed since then) – general surveillance is not an “education record.” A focus on one student is an education record of that student; only the parents of the student may view it but may give consent to show to others. A focus on two students (such as in a fight) is an education record of both

students; both sets of parents may view, but other students must be redacted; other parents must give written consent to view. The district may inform parents what their child is doing in the video. This official guidance is more restrictive than the unofficial guidance.

Under the FPCO's *unofficial* guidance, a focus on two students (see above) is an "education record" of both. Parents may view, but not get a copy unless the other parents give consent or the other student's image is redacted. The unofficial guidance has been provided informally to school attorneys via email and letters since 2006. The unofficial guidance has been documented enough by school attorneys that it does appear to represent the FPCO's current position, even if it has not been stated officially. It is expected that when FPCO does update their official guidance, they will adopt the unofficial guidance. Until they do, choices regarding this issue should be made consistently and in consultation with your school attorney.

#### **b) FERPA, Law Enforcement, and Student Records**

One exception to FERPA is the "law enforcement unit" exception (34 CFR 99.8). The district designates the law enforcement unit. Video and other records are maintained by the law enforcement unit for school safety purposes. In this case, video is exempt from FERPA and may be shared with outsiders without parental consent. If shared with school officials, it becomes an "education record" subject to FERPA.

This is another facet of FERPA and video surveillance compliance. Videos that are maintained by the law enforcement unit are now out of the realm of FERPA-covered videos – unless certain uses are made of them, as outlined above. Many districts have implemented this approach – creating and designating the law enforcement unit and having the records maintained there. Discuss with counsel in specific situations.

### **3. Real Challenges for Schools**

Parents send students with concealed devices to record what teachers and staff say during school and meetings, to catch bullies in action, and other similar purposes. Employees use devices to record meetings with other staff members, administrators, even students. Journalists may use devices to get the scoop on what is going on inside schools.

One device called AngelSense is marketed to parents of special-needs children. It is a wearable GPS tracker that sends updates to the parent's app. The "Listen In" feature enables the microphone on the GPS device for live one-way audio. So far, the device does not record. "School Guardian" feature allows school to turn off Listen In feature. It is marketed as a spying app for parents to spy on care providers, teachers, and others.

#### **E. Body Cameras**

Body cameras are becoming a reality for many police departments and should be discussed with **school resource officers** and **security**. Questions to ask include when the body cameras will be used, what policies and procedures are in place when using body cameras, who can view or review the footage, how long it is stored, what it is used for, and whether it is securely downloaded and how often. These terms can be addressed in a **memorandum of understanding (MOU)** for services.

**Law enforcement unit records** and **FERPA** must be addressed, as well as **students' reasonable expectation of privacy**.



Law enforcement has many uses for body camera footage, including **collecting evidence** for prosecution, ensuring adherence to **policies and procedures**, and **training**. If a law enforcement unit is maintaining the video, it is not a school education record subject to FERPA. It could be a **public record**, subject to public records requests and the Sunshine Law.

### 1. **Body Camera Legislation**

Ohio has proposed legislation, but no enacted laws. **House Bill 407** was introduced on December 7, 2015, and reported to the Local Government Committee on May 24, 2016. This bill would require that law enforcement agencies intending to use body cameras must create policy within 6 months of the effective date of the legislation. The policy would include when the cameras will be worn; activities during which use is mandatory, optional, or prohibited; procedures for obtaining consent when entering private residences and exceptions; who may access footage; procedures for investigations and complaints; standard procedures for public records requests; and sanctions for officers who do not comply with the policy. Upon adoption, the policy must be made available to the public.

This bill is very short and does not address the issue of confidentiality of student data obtained in a school by a law enforcement officer. This bill could be a way to obtain an exception to the public records law.

Ohio **House Bill 585** was introduced on July 11, 2016. This proposed bill states that body camera footage is generally a public record with some exceptions:

- Records retention for minimum of 1 year.
- Records created in a residence are not public records.
- Records created in an area of “nonresidential private property” are not public records.
- Record created at a residence must be given to owner upon request.
- Record with audio/video of minor or victim of violent sex offense, menacing, human trafficking, domestic violence.
- These may become public records after conviction/guilty plea.

### 2. **Body Camera Lawsuits**

The Ohio Supreme Court heard arguments in June 2016 in two cases involving access to police officer camera footage.

- *State ex rel. Cincinnati Enquirer v. Ohio Dept. of Pub. Safety*, No. 2015-0390: Involves dash cam video from an Ohio State Highway Patrol vehicle during a high-speed chase on I-71.
- *State ex rel. Cincinnati Enquirer v. Deters*, No. 2015-1222: Involves a University of Cincinnati police officer’s body cam video during a fatal shooting.

The main issue in each case was whether footage from police officer body cams or dash cams are public records or are exempted from public records law as investigative material. Oral arguments were held, but a decision has not yet been issued.

### 3. **Body Camera Law, Recording, Wiretapping**

Body camera use and law will be developing across the country over the next few years.

R.C. 2933.52 – It is legal to record as long as *one* person involved in the conversation is aware and gives consent (this includes the individual who is doing the recording).

Likewise, federal law permits intercepting and publishing cell phone conversations between other people as long as one individual has knowledge and gives consent.

#### **4. School Policy Considerations**

Schools should have updated policies in place that prohibit recordings of IEP and other meetings. If prohibited, state at the beginning of a meeting that audio and video recordings are not permitted. Consider how the audio records created by the district should be retained and stored. It's all about content, not format. Remember, if you record audio, you may be creating an education record or public record. Train building administrators how to collect and use audio evidence, as well as how to address parents and students who try to capture audio.

#### **5. Other Considerations**

Public records – An Ohio attorney general opinion declared that an audio recording of a board of township trustees meeting, which was used in lieu of taking notes for preparation of meeting minutes, is a public record and must be maintained and made available for inspection.

FERPA – Are voices considered personally identifiable information covered by FERPA?

Staff concerns – Although not surprising, staff may not welcome audio or video recording.

## **IV. Final Thoughts on Managing the Latest Tech Toys**

### **A. Planning for Technology**

Technology strategies necessarily must involve frequent review of current technology policies. Update the following policies frequently, or consider adopting policy if current district policies are not already in place:

- Acceptable Use
- Social Media
- Texting
- Bring Your Own Device

Make sure you have staff knowledgeable about the latest and greatest technology, and have a plan to address changes in technology. Set up mechanisms for enforcement.

### **B. Don't take things too far...**

Faraday cages – May not use devices that block the flow of data completely.

Discrimination – May not block some messages at the expense of others (content neutral, no viewpoint discrimination).

First Amendment rights – Consider constitutional freedoms of students and staff.

Call legal counsel – to avoid legal complications when you have questions about records, policy interpretations, and privacy.