



Inappropriate Use of Technology in Schools

David Sallay, Data Privacy
Auditor

What is
“appropriate”?



LEGAL
COMPLIANCE



AVOIDING
HARM



COST/BENEFIT



PARENT



INTENDED USE



PEDAGOGICAL
VALUE

Appropriate
use of funds

LEARNING & TECH

The LA School iPad Scandal: What You Need To Know

August 27, 2014 · 3:32 AM ET
Heard on [Morning Edition](#)

ANNIE GILBERTSON

FROM **KPCC**

A massive expansion of classroom technology has come to a grinding halt in Los Angeles.

The LA Unified School District had planned to buy some 700,000 iPads for its students and teachers. The Apple tablets would include learning software built by publishing giant Pearson. But Superintendent John Deasy announced earlier this week he is canceling the contract and restarting the bidding process.

The decision comes on the heels of an investigation by NPR member station KPCC, which obtained emails



Los Angeles Unified School District Superintendent John Deasy exchanged multiple emails with executives at Pearson PLC about the potential for working together.

Damian Dovarganes/AP

What would parents think?

In general, develop technology policies with parent input



An illustration on a dark blue background. On the left, a large, stylized figure of a person wearing a black hoodie and a black balaclava is shown in profile, looking towards the right. They are holding a large magnifying glass. The magnifying glass is positioned over a smaller, stylized figure of a person sitting at a desk and working on a computer. The person at the desk is also wearing a black hoodie. The magnifying glass is held in a way that it appears to be inspecting the person at the computer. The overall scene suggests surveillance or monitoring.

Is it appropriate...

To monitor a student's online activities?

CIPA

Children's Internet Privacy Act

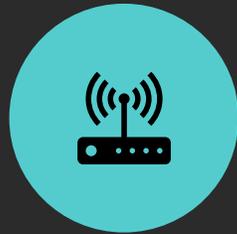
Applies to students younger than 17

Requires schools to have an Internet safety policy

CIPA Internet Safety Policies



RESTRICT ACCESS TO
INAPPROPRIATE AND
HARMFUL MATERIALS



ENSURE SAFETY AND
SECURITY OF MINORS
ONLINE



PREVENT UNAUTHORIZED
ACCESS, INCLUDING
HACKING



PROHIBIT UNAUTHORIZED
DISCLOSURE AND USE OF
PERSONAL INFORMATION



INCLUDE MONITORING OF
THE ONLINE ACTIVITIES OF
MINORS

“Webcamgate”

- Lower Merion School District (PA) remotely activated student webcams at home on 1:1 devices
- Accused of violating the Electronic Communications Privacy Act
- Settled outside of court for \$610,000

Posted on Sun, Feb. 28, 2010

Monica Yant Kinney: Another pin in the privacy balloon

• By Monica Yant Kinney
Inquirer Columnist

In the week since the Lower Merion School District “Webcamgate” saga went viral, many have focused on unanswered questions, angry denials, and salacious details about the accusing family. But let’s not lose sight of the unassailable facts:

Lower Merion officials admitted using remote-access Web cam software 42 times this academic year, ostensibly to hunt missing laptops.

They admitted they had not sought parental permission to peer into minors’ personal lives and homes.

And the district did not put a halt to the clandestine activity until it was sued by the family of Harriton High student Blake Robbins.

As Lillie Coney of the Electronic Privacy Information Center put it: “If they thought it was right, they wouldn’t have stopped.”

“But they weren’t thinking. And they weren’t planning to get caught. So they didn’t tell anybody.”

A fourth fact about this educational eye-opener? That it’s yet another example of a troubling post-9/11 erosion of personal privacy.



STEVEN M. FALK / Staff Photographer

Blake Robbins, who accuses Lower Merion School District officials of spying, reads a statement outside his home.

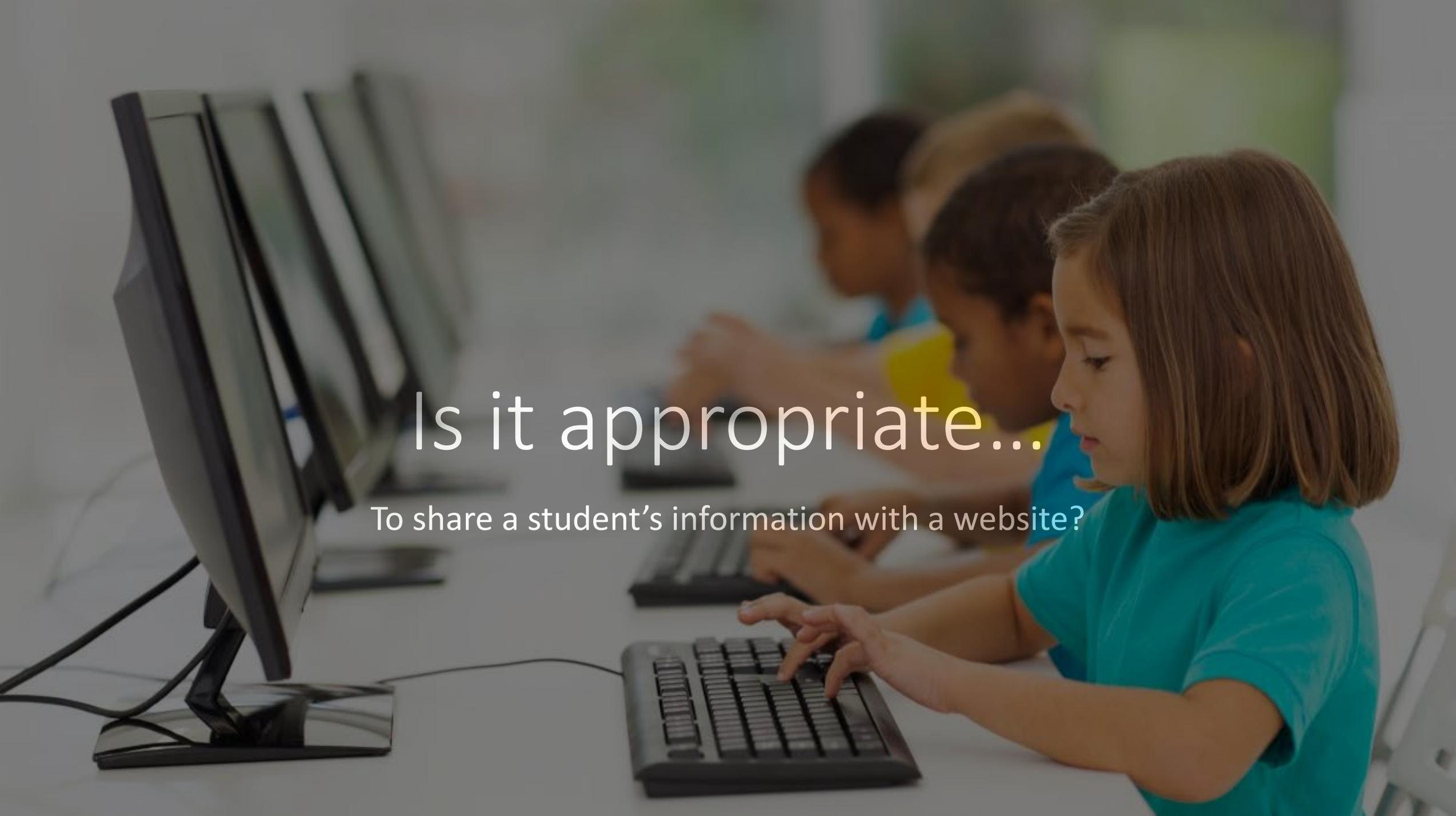
Effects on motivation

Journal of Personality and Social Psychology
1975, Vol. 31, No. 3, 479-486

Turning Play into Work: Effects of Adult Surveillance and Extrinsic Rewards on Children's Intrinsic Motivation

Mark R. Lepper and David Greene
Stanford University

Preschool children engaged in a novel activity in individual sessions. In the expected reward conditions, subjects expected to win a chance to play with highly attractive toys by engaging in the activity; in the unexpected reward conditions, subjects had no prior knowledge of this reward. Orthogonally, subjects in the surveillance conditions were told that their performance would be monitored via a television camera; while subjects in the nonsurveillance conditions were not monitored. Two weeks later, unobtrusive measures of the subjects' intrinsic interest in the activity were obtained in their classrooms. Two significant main effects were obtained reproducing and expanding findings from earlier studies. Subjects who had undertaken the activity expecting an extrinsic reward showed less subsequent interest in the activity than those who had not expected a reward, and subjects who had been placed under surveillance showed less subsequent interest than those not previously monitored.

A young girl with brown hair, wearing a teal t-shirt, is sitting at a desk in a classroom, focused on typing on a black keyboard. In the background, other students are also working at their desks with computer monitors. The scene is brightly lit, suggesting a modern educational environment.

Is it appropriate...

To share a student's information with a website?

YES,

But...

But what does the law say?

There is nothing in federal or state law that prohibits a teacher from sharing **any** student information with a website provided that

- It is for a legitimate educational purpose
 - This includes behavioral data, medical data, or even information from IEPs
- A few reasonable requirements are met

FERPA

(B) A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party -

- (1)** Performs an institutional service or function for which the agency or institution would otherwise use employees;
- (2)** Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
- (3)** Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

(ii) An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests.

Direct control has to follow
“reasonable methods”

So what is reasonable?

What is reasonable?

- Teachers share with admin/parents what they're using in the classroom
- Schools request that data be destroyed once no longer used
- Parents aren't denied FERPA rights (e.g., access to records)
- Could be based on input from teachers, parents, stakeholders

COPPA

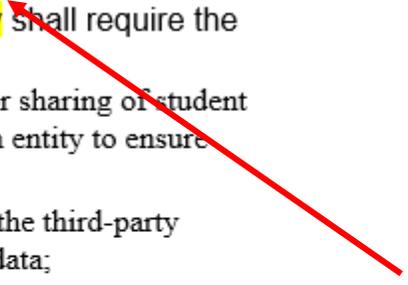
- Only applies to students younger than 13
- School can consent to share data in place of parent **ONLY** if the website uses the data for an educational purpose
 - No targeted advertising

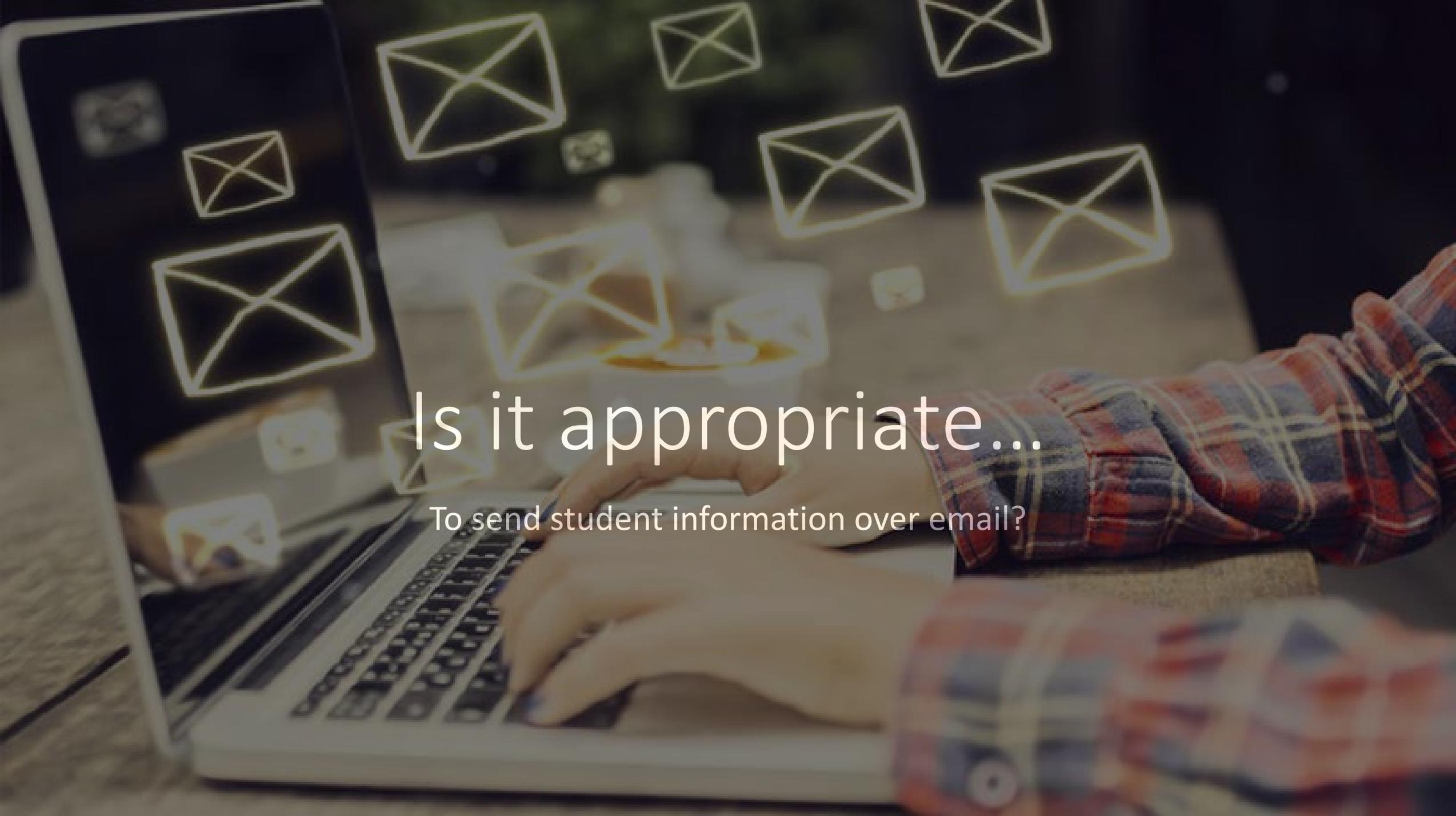
Student Data Protection Act

- Specific terms related to direct control must be spelled out when the **district or charter school** are procuring a service
- Unclear if it applies to teachers procuring services

- (2) When contracting with a third-party contractor, an **education entity** shall require the following provisions in the contract:
- (a) requirements and restrictions related to the collection, use, storage, or sharing of student data by the third-party contractor that are necessary for the education entity to ensure compliance with the provisions of this part and board rule;
 - (b) a description of a person, or type of person, including an affiliate of the third-party contractor, with whom the third-party contractor may share student data;
 - (c) provisions that, at the request of the education entity, govern the deletion of the student data received by the third-party contractor;
 - (d) except as provided in Subsection (4) and if required by the education entity, provisions that prohibit the secondary use of personally identifiable student data by the third-party contractor; and
 - (e) an agreement by the third-party contractor that, at the request of the education entity that is a party to the contract, the education entity or the education entity's designee may audit the third-party contractor to verify compliance with the contract.

Defined as school district or charter



A person wearing a red and blue plaid shirt is typing on a laptop. The laptop screen and the surrounding area are filled with glowing white envelope icons, suggesting email communication. The scene is dimly lit, with the primary light source being the laptop screen and the floating icons.

Is it appropriate...

To send student information over email?

Sending email without encryption is like sending a postcard



Previous guidance

Any information about a student is potentially sensitive and should not be shared over unencrypted email

Solution	Cons
Paid encryption	Expensive
Password-protected documents	Clunky, opened up different security risks
MOVEit	Not everyone has access; overkill when just needing to share small amount of information

OVERKILL

General guidance

- Federal standard for being safe from reidentifying a student is if you can narrow it down to **three students**
- A combination of student information where a reasonable member of the community could not narrow the identity down to three students is a safe harbor



Are they bald? It only narrows it down to 4...

Safe harbor

When emailing USBE, so long as you only send a minimum amount of information, in most cases it is acceptable over unencrypted email to send a combination of

- SSID
- Test name
- Class/teacher name

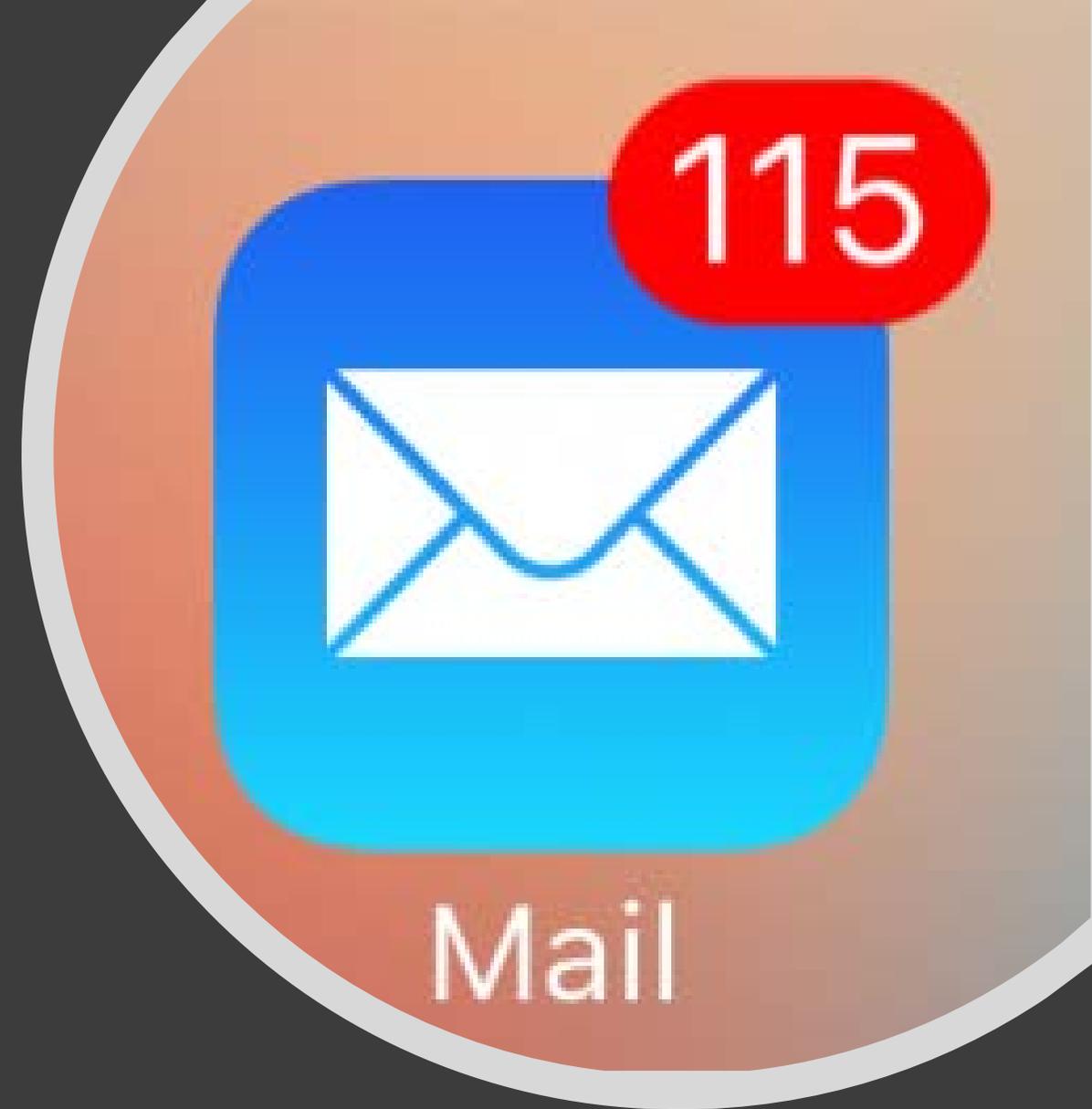
Just remember:

- Be careful of gender pronouns (he/she)!
- Be careful with more sensitive assessments (UAA/DLM)
- Don't send student names



What about emailing parents?

- Parents have a right to access their child's student records
- True, student names are PII
 - So are parent names and email addresses!
 - It is impossible to email a parent without disclosing PII
- Weigh risk and benefits when emailing



A young boy in a school uniform is using a VR headset. He has a surprised expression. Other students are looking at him. The scene is in a classroom.

Is it appropriate...

To use emerging technologies in the classroom?



IoT integration

- RFID chips used in student IDs to automatically track attendance (and probably other things...)
- At Saint Louis University, Echo Dots are in all student living spaces to provide answers to questions about university events
- And frankly, teachers are probably bringing in all sorts of other things...



Personal assistants

- COPPA explicitly treats “voice” as personally identifiable
- However, the FTC says when voice is used as a replacement for written words (e.g., perform a search), they will not take enforcement action
- Unclear whether student’s voice would always qualify as part of education record under FERPA
- These devices work outside your firewall (so it’s likely that they are violating CIPA)

Amazon's
opinion...



Bill Fitzgerald

@funnymonkey



At a conversation I was part of yesterday, an Amazon rep was asked by a tech integrator whether or not Alexa should be used in a classroom.

The rep's unequivocal answer: No.

He said that Alexa and Dot are not intended for the classroom.

The response was unambiguous.

7:54 AM - Jun 25, 2018



111



61 people are talking about this



Potential misfires



From edsurge.com [article](#) 2018-07-11:

Privacy aside, [Jason Hong, Carnegie Mellon University] doesn't think voice assistant devices are really ready for educational environments. **They are intended for home use, he says, and teachers should consider the potential for misfires (Alexa could be accidentally activated) and disruptions (a Kindergartner who keeps yelling out for Alexa to turn off the lights).** Voice assistants could be useful in specific instances in a college setting, such as a lab where students need hands-free interaction, but even then, there are risks.

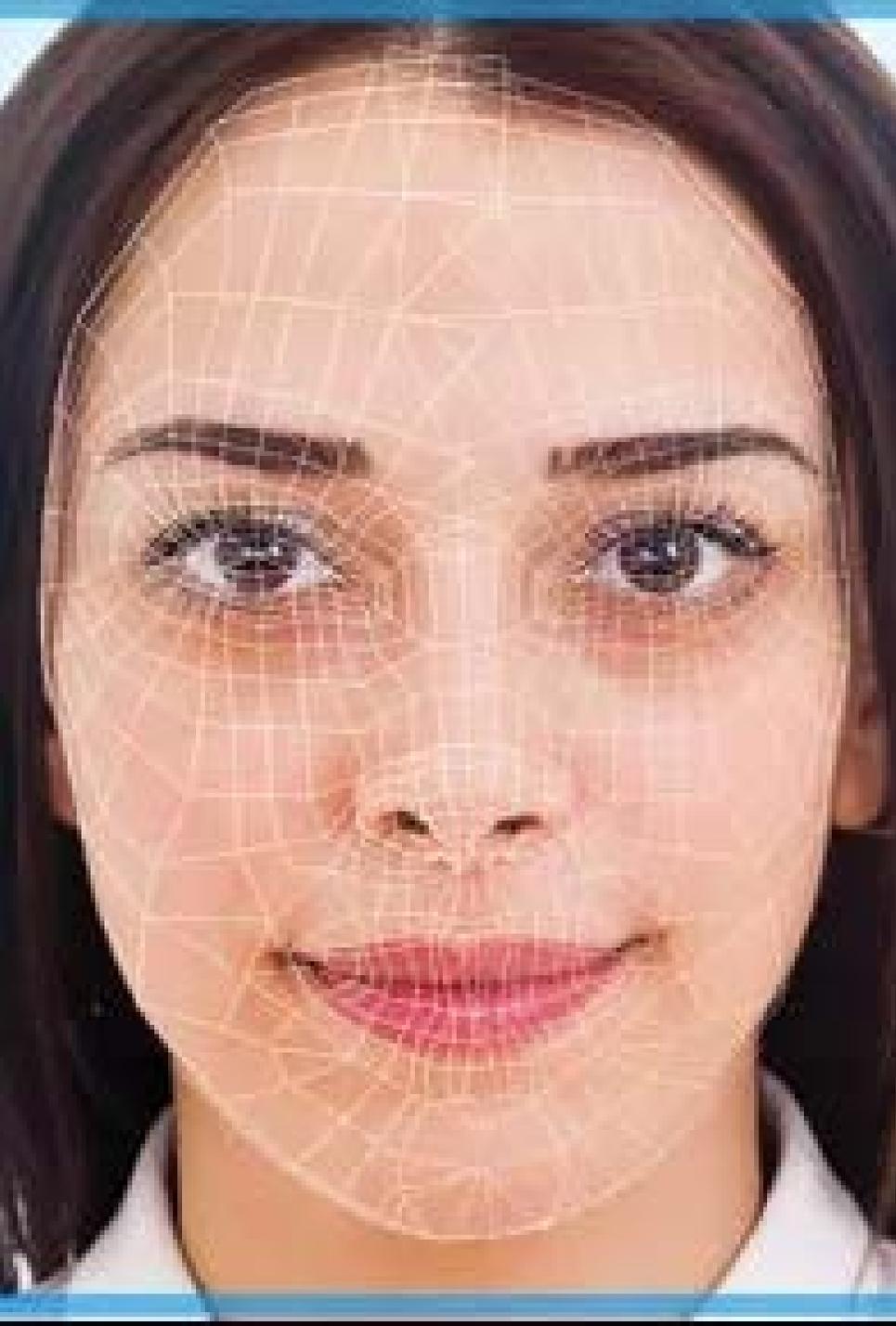
Social media monitoring

- Company “geofences” posts from social media that appear threatening
- Company shares flagged posts with LEA
- Concerns:
 - Adequate notice to parents?
 - Effectiveness?
 - Extra liability?

Could Monitoring Students on Social Media Stop the Next School Shooting?



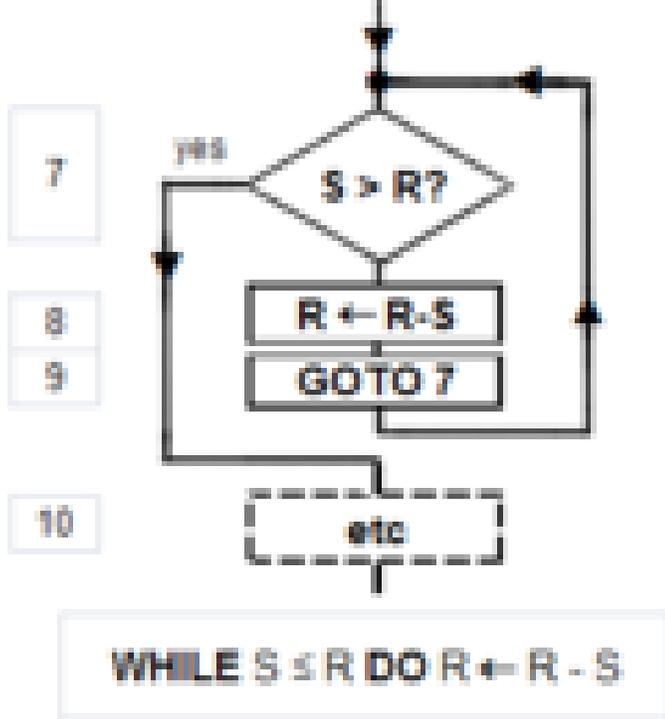
Employees at Social Sentinel in Burlington, Vt. “If a student is posting about shooting their teacher, we would hope we’d be able to find something like that,” said Gary Margolis, the company’s chief executive. Hilary Swift for The New York Times



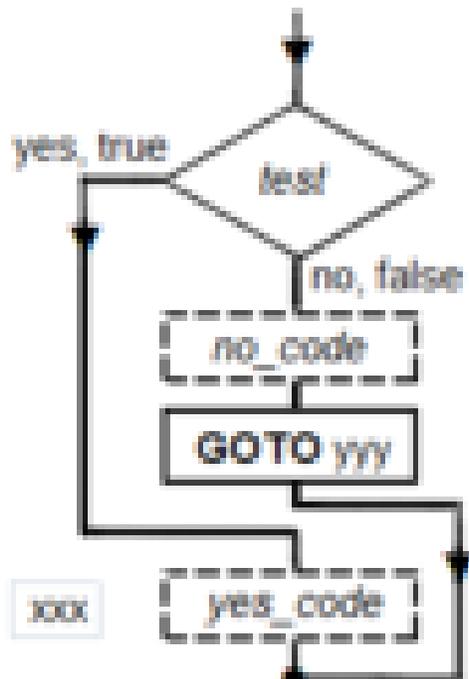
Facial-Recognition for school safety

- July 18 Education Week [article](#) discusses how more districts are purchasing surveillance/facial-recognition technology to increase school safety
- Unclear how effective they are at stopping threats

Algorithms



- Adequate transparency?
- How high stakes are the results? What is the worst thing that will happen if there is a false negative?
- Ability to contest decisions (particularly when high stakes)?
- Monitoring fairness/Feedback mechanism





 **Anup Kaphle** 
@AnupKaphle



Above: #Ferguson, on Twitter

Below: Rest of America, on Facebook

9:54 PM - Aug 17, 2014

 692  1,626 people are talking about this

Is algorithmically-
filtered content
best for students?

What does YouTube say about public education?

Study by Burhanettin Keskin, “What Do YouTube Videos Say About Public Education?”

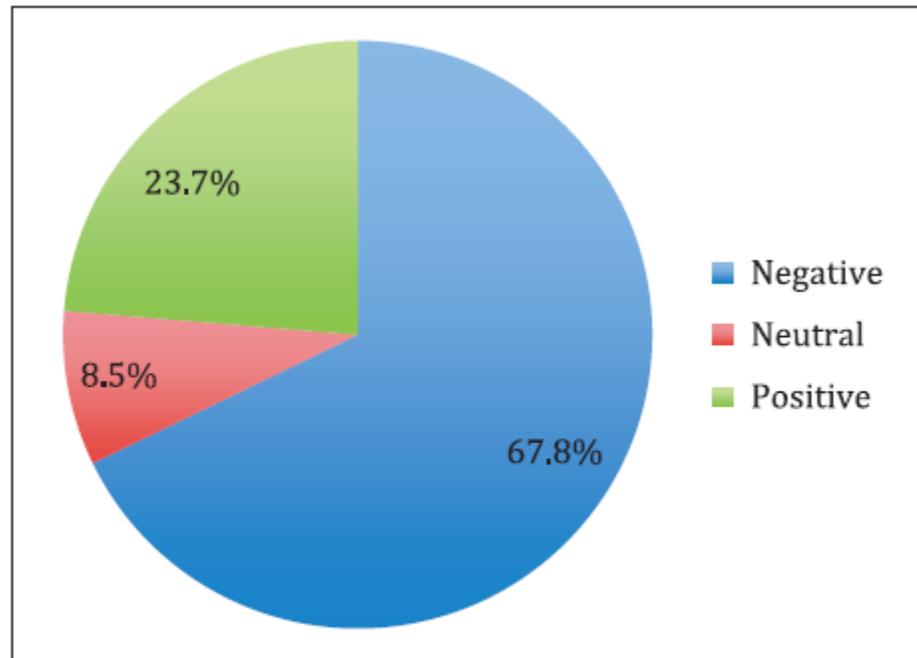


Figure 1. The content coding of the YouTube videos on public education.

Discussion

The results show that a majority of the selected videos examined in this study presented public education negatively. A substantial amount of these videos contained blunt attacks on public education. The following video titles provide clues about the nature of these attacks: “Planned Failure: Why No Amount of Money Can Fix Public Education,” “Abolish Public Education: Privatize All Schools,” “How Public Education Controls Your Perception—Mind Control,” “The Truth About Public Education! (A Systemic Destruction of Human Ingenuity),” “Public ‘Education’ Has Become Indoctrination and Distraction,” “Against Public Education,” “Common Core: UN Agenda 21, Communitarianism & The Public Education Plan to Destroy America.” Many of these videos claim that public education is a tool created by the government and is used to indoctrinate people. Such vid-

Takeaways



BE
TRANSPARENT



BE SPECIFIC



BE
REASONABLE



ASK FOR HELP