

Facial Recognition Technology

What School System Tech Leaders Need to Know

ISSUE RECAP

Facial recognition technology is being used in school systems to improve efficiency of campus entry, enhance safety practices, and research student engagement. With it, meaningful questions are being raised about privacy as well as the appropriateness and efficacy of the technology. This CoSN Member Exclusive Brief provides an overview of the issues, as well as CoSN's perspective and guidance on how to evaluate the technology for your district.

What are Some Potential Uses for Facial Recognition Technology in School System?

Facial recognition technologies work by mapping facial features from a photograph or video, comparing that information with a database of known faces and identifying a match. School systems are using it in a variety of circumstances, including:

Use Case	Perceived Benefits
Expediting student entry into the school campus	Using facial recognition technology may expedite student entry into the school system as compared with swipe cards or entry that is not facilitated by technology.
Expediting employee entry into the school campus	Using facial recognition technology may expedite employee entry into the school system and eliminate the need for a reception area or other human gatekeeper.
Improving safety	Student and employee safety may be improved by: - preventing unauthorized individuals from entering campus - identifying individuals on registered sex offender lists in attendance at public school events
Assessing student attention	When used to assess student engagement in online learning, facial recognition can support improvement of online courses and help educators provide

	targeted intervention
--	-----------------------

However, the debut of facial recognition technologies in school systems has not been without controversy.

Questions about efficacy and racial bias emerged in the public eye after Amazon’s facial recognition technology falsely identified 28 members of the US Congress as individuals who had been arrested on criminal charges.¹ Amazon moved swiftly to improve its product,² however such early stumbles had a profound impact on public perception, prompting meaningful and important questions from school systems and parents.

Additional questions related to efficacy and security led to controversy in Lockport, NY where facial recognition technology was implemented to improve student safety in the wake of school shootings. Implementation proceeded despite the lack of evidence that such technology can be effective in preventing such tragedies. According to documentation obtained by the New York Civil Liberties Union (NYCLU), the district did not have policies in place to protect the privacy of the data being collected by the cameras. As stated in an editor’s note on the NYCLU statement, “The serious lack of familiarity with cybersecurity displayed in the email correspondence we received and complete absence of common sense redactions of sensitive private information speaks volumes about the district’s lack of preparation to safely store and collect biometric data on the students, parents and teachers who pass through its schools every day.”³

What are the Privacy Implications?

In addition to questions regarding bias and efficacy, facial recognition technology raises important privacy questions when used in school systems. If you plan to use the technology with students, your first consideration should be to ensure that collection of student biometric information is permitted under your state student data privacy law. Facial Recognition is currently prohibited in certain states. Consider this to be a fundamental requirement that must be addressed before moving forward.

In addition, when student data is involved, FERPA privacy requirements must be considered, as the data collected will likely be part of the education record. For more information, see the U.S. Department of Education’s [FAQ’s on Photos and Videos Under FERPA](#) and [When is a Photo or a Video of a Student and Education Record Under FERPA](#). If you were to qualify the technology provider as a school official, what contractual considerations should be in place to maintain the requisite direct control over the student personal information and ensure that it is used only to support your legitimate educational interest? Are there other data protection laws applicable to your intended use case that must be considered?

¹ Snow, Jacob. 2018. Amazon’s Face Recognition Falsely Matched 28 Members of Congress with Mugshots. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>

² Das, Ranju and Bagaria, Venkatesh. 2018. Amazon Rekognition announces updates to its face detection, analysis, and recognition capabilities. <https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-updates-to-its-face-detection-analysis-and-recognition-capabilities/>

³ Editor’s Note. Coyle, Stefanie and Dann, Naomi. 2018. New York Civil Liberties Union. We Asked for Answers on Facial Recognition in Schools, Our Questions Remain. <https://www.nyclu.org/en/news/we-asked-answers-facial-recognition-schools-our-questions-remain>

Whether or not the technology will be used with students, employees or visitors, the data being collected is personally identifiable, subject to special privacy protections and security considerations. Plan to define and document the following:

- Who will have access to the data inputs and results and for what purpose
- What access controls will be in place
- How will the data be secured
- How long will the data be stored

Also, clearly document escalation policies for addressing potential security threats if they indicate that an unauthorized individual is attempting to enter the premises.

What Questions Should You Consider Before Bringing Facial Recognition Technology to Your School System?

Before bringing any technology into your school system, it's important to assess not only how it will benefit your school system, but also the privacy and security practices. Here are 10 questions to consider:

1. Do your state student data privacy laws permit collection of biometric student data in the manner intended by your use of facial recognition technology?
2. What is the benefit you hope to gain by using the technology? Does the technology provider have evidence demonstrating that it can meet those needs? Are there other technologies that don't collect sensitive data that would serve the same purpose?
3. Is there evidence that the technology provides accurate results?
4. Is the use case envisioned by your school system consistent with the age of the students with which it will be used? For example, if you plan to use the technology for security purposes, will you use it with very young students as well as older students?
5. Have you assessed the privacy and security practices of the technology provider?
6. Do you have a data protection agreement in place with the technology provider to maintain control over any student data that might be shared with them?
7. What work will you need to complete in order to implement the technology? Who will be responsible for uploading student and employee photos? If you are using the technology to prevent access by individuals with a criminal record, who will be responsible for obtaining and uploading those photos? How will you ensure that the photo database remains up-to-date so that the results remain accurate and the technology effective?
8. Will the data be hosted locally or remotely by the technology provider? How will you prevent unauthorized access to surveillance systems storing or accessing biometric data? What physical and software security measures are in place?
9. Will the data be used by the technology provider to inform improvement of their product or for other purposes? If so, are those purpose in alignment with your requirements under FERPA, your state student data privacy laws and your district policies?
10. How will you introduce the use of the technology to parents in your community? What objections might you anticipate? Are you prepared to answer questions they may have about how the technology will be used as well as the data protection practices that will be in place?

CoSN's PERSPECTIVE

Sensible and balanced use of technology in school systems is at the core of CoSN's mission. School systems should not rush to implement technology without an advance plan that includes the following :

-
1. Well-defined goals for the use of facial recognition technology
 2. An implementation strategy that considers requirements and available resources, including finances, manpower and knowledge
 3. Maintenance plans to ensure the effectiveness and accuracy of the technology
 4. An efficacy measurement plan
 5. Appropriate and reasonable data privacy and security protections
-

When considering use of facial recognition technology in your school system, we encourage you to partner with technology companies to determine whether and how they will support your efforts in all five of the above requirements. Their responses may be used as part of your diligence review prior to engaging with any company.

CoSN RESOURCES

To ensure that you understand the fundamental requirements of federal student data privacy protections, refer to the [Protecting Privacy in Connected Learning Toolkit](#).

ADDITIONAL READING

[Ensuring School Safety While Also Protecting Privacy](#) - FERPA/SHERPA

[Privacy Principles for Facial Recognition Technology in Commercial Applications](#) - Future of Privacy Forum

This material is being provided as a benefit of CoSN membership. We hope you find it useful. Feel free to cut & paste snippets for your team members, but please refrain from posting it, in its entirety, in a public platform. For more privacy resources, visit CoSN.org/Privacy.

©2018 Consortium for School Networking. All rights reserved.