Should facial recognition cameras be used in schools?

What they said...

'Data can perhaps be used to discover learning strengths and areas of concern, enabling more tailored learning experiences that can lead each student to better outcomes'
An education technology company explaining how in-class facial recognition monitoring of students can assist their learning

'This takes away a huge sense of freedom for these children'
Dr Niels Wouters, of the Microsoft Research Centre for Social Natural User Interfaces at the University of Melbourne

The issue at a glance

On October 5, 2018, it was reported that Victoria's Education Minister, James Merlino, had directed the Education Department to assess immediately the facial recognition software currently being trialled in some Victorian private schools. He also asked the Department to contact every Victorian state school to remind them that they must undertake a privacy impact assessment before considering the software.

The software was due to be trialled in some Victorian state schools; however, the Minister's statement appears to have delayed this process.

https://www.theage.com.au/national/victoria/minority-report-crackdown-on-facial-recognition-technology-in-schools-20181005-p5080p.html

In August, 2018, it was reported that facial recognition technology, used for roll marking, was being trialled by a small number of Victorian private schools.

https://www.heraldsun.com.au/kids-news/australian-schools-begin-spying-trials-using-facial-recognition-technology/news-story/2d38f743af6309dd2f68f696c3ffedc1

On February 14, 2018, seventeen students were killed in a school shooting at Marjory Stoneman Douglas High School, Parkland, Florida.

https://en.wikipedia.org/wiki/List_of_school_shootings_in_the_United_States#2015_to_present These deaths appear to have provided a significant impetus for the trial or uptake of facial recognition systems by schools in the United States that are intended to increase the safety of students. https://www.independent.co.uk/news/world/americas/facial-recognition-us-schools-lockport-real-networks-marjory-stoneman-nikolas-cruz-a8459486.html

Reports have also been published of schools in China, and one business college in France, using facial recognition technology to monitor student engagement.

All these uses of the technology have convinced advocates and critics anxious about their privacy and other implications.

Background

A facial recognition system

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods by which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analysing patterns based on the person's facial textures and shape.

https://en.wikipedia.org/wiki/Facial_recognition_system

It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Although the accuracy of facial recognition system as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless and non-invasive process. https://en.wikipedia.org/wiki/Facial_recognition_system Recently, it has also become increasingly popular in schools and other educational intuitions. https://www.edweek.org/ew/articles/2018/07/18/facial-recognition-systems-pitched-as-school-safety-solutions-ra.html

Use of facial recognition technology in United States schools
In the United States, especially as a response to concerns regarding school shootings, there is a growing use of facial recognition technology. https://www.independent.co.uk/news/world/americas/facial-recognition-us-schools-lockport-real-networks-marjory-stoneman-nikolas-cruz-a8459486.html
Some schools and technology companies are using facial recognition to enhance security systems for tracking school visitors. A Seattle-based company RealNetworks has developed and recently released a facial recognition system called Secure, Accurate Facial Recognition (SAFR). According to the website, the technology is intended for installation at K-12 schools or at event venues, and RealNetworks offers the technology free for all schools in the United States and Canada. It is currently being tested at University Child Development School in Seattle, and the state of Wyoming is developing a plan to implement the system. Lockport City School District in New York is already installing facial recognition technology-based security, although they are using a system from a Canadian company, SN Technologies. Other schools, districts, and states across the nation are also considering bringing this sort of technology to their schools to enhance security and prevent tragedies. https://www.fosi.org/good-digital-parenting/3-ways-facial-recognition-technology-childrens-lives/
The various systems of facial recognition security work differently. The SAFR system currently installed in Seattle monitors access onto school property, scanning faces and comparing them to a list of approved students, parents, and faculty. The system chosen for Lockport schools uses a database of faces of expelled students, disgruntled employees, and sex offenders to compare with the faces of people entering the buildings. Given the technology's early stage in schools, consensus regarding the best use and form of this technology will require more time. https://www.fosi.org/good-digital-parenting/3-ways-facial-recognition-technology-childrens-lives/

Facial recognition technology in schools in China
In China, some schools are now testing systems to monitor student performance and to check whether they are paying attention in class. Algorithms are used to interpret facial expressions. Another family of technologies, emotional surveillance, is already in use in the Chinese army and in several private companies. This involves placing wireless sensors in caps or hats that can read brain waves and then decide when someone needs a break or to be assigned a new task, all in the name of greater efficiency. https://www.forbes.com/sites/enriquedans/2018/06/25/facial-recognition-and-future-scenarios/#4fd138811ac9

Internet information

On October 31, 2018, The Daily Mail published a report titled 'New York school district switches on controversial $4m facial recognition technology to identify potential shooters'

which outlines the use of facial recognition cameras by a high school in Lockport City School District.
The full text can be accessed at https://www.dailymail.co.uk/sciencetech/article-6334861/New-York-school-district-uses-facial-recognition-technology-identify-potential-shooters.html

On October 30, 2018, Motherboard published a comment and analysis by Rose Eveleth titled ' Facing Tomorrow's High-Tech School Surveillance' which considers the implications of facial recognition cameras being used in United States schools and in other countries around the world.
The full text can be accessed at https://motherboard.vice.com/en_us/article/j53ba3/facial-recognition-school-surveillance-v25n3

On October 17, 2018, the Foundation for Economic Education published a report on the potential use of facial recognition cameras in United States schools to protect children against school shooters and others posing a threat to their safety.
The full text can be accessed at https://fee.org/articles/facial-recognition-scanning-in-schools-has-arrived-fueling-privacy-concerns/

On October 5, 2018, The Age published a report titled 'Minority report: crackdown on facial recognition technology in schools' which details the concerns of the Victorian Minister for Education, James Merlino, and Information Commissioner, Sven Bluemmel, regarding the use of facial recognition cameras in schools.
The full text can be accessed at https://www.theage.com.au/national/victoria/minority-report-crackdown-on-facial-recognition-technology-in-schools-20181005-p5080p.html

On September 12, 2018, ABC News published an analysis titled 'Chinese video surveillance network used by the Australian Government' which suggests the potential for espionage via the use of Chinese surveillance cameras in Australia.
The full text can be accessed at https://www.abc.net.au/news/2018-09-12/chinese-video-surveillance-network-used-by-australian-government/10212600

On August 29, 2018, The New Daily published a report titled 'Smile kids! Schoolyard sins could ruin lives' which reports on some schools in Australia using facial recognition cameras to replace roll marking. The report suggests this restricts children's freedom.
The full text can be accessed at https://thenewdaily.com.au/life/tech/2018/08/29/facial-recognition-schools-trial/?utm_source=Adestra&utm_medium=email&utm_campaign=Morning%20News%2020180830

On August 29, 2018, The Herald Sun's young people's supplement Kid Wise published a news report and background piece by Mandy Squires titled 'Australian schools begin spying trials using facial recognition technology' which reports on private trials being undertaken in some Australian schools to gauge the effectiveness of facial recognition cameras as a device for taking rolls and locating students.
The full text can be accessed at https://www.heraldsun.com.au/kids-news/australian-schools-begin-spying-trials-using-facial-recognition-technology/news-story/2d38f743af6309dd2f68f696c3ffedc1

On August 15, 2018, the New York Civil Liberties Union (NYCLU) published a comment by Toni Smith Thompson titled 'Here's What Happens When We Allow Facial Recognition Technology in Our Schools' which outlines some of the risks that attach to this use of technology in schools.
The full text can be accessed at https://www.nyclu.org/en/news/heres-what-happens-when-we-allow-facial-recognition-technology-our-schools

On August 3, 2018, Tech Ed published an article titled 'Company Offers Free Facial Recognition Software to Boost School Security' which details RealNetworks' offer to make facial recognition software SAFR available for free trials in over 100,000 school districts.
The full text can be accessed at https://edtechmagazine.com/k12/article/2018/08/company-offers-free-facial-recognition-software-boost-school-security

On July 25, 2018, gov.tech.com published a report titled 'Facial Recognition Might Be Ready for Schools, but Are They Ready for It?' which considers the increasing number of trials of facial recognition cameras in United States schools.
The full text can be accessed at http://www.govtech.com/em/preparedness/Facial-Recognition-Might-Be-Ready-for-Schools-but-Are-They-Ready-for-It.html

On July 23, 2018, The New York Post published a report titled 'Schools using facial recognition tech to boost safety' which outlines the use of facial recognition cameras by a high school in Lockport City School District.
The full text can be accessed at https://nypost.com/2018/07/23/schools-using-facial-recognition-tech-to-boost-safety/

On July 19, 2018, Fast Company published an article titled 'Schools can now get free facial recognition software to track students' which raises some of the issues surrounding the use of facial recognition cameras in schools.
The full text can be access at https://www.fastcompany.com/90205116/schools-can-now-get-free-facial-recognition-software-to-track-students

On July 13, 2018, Brad Smith, the president and chief legal officer of Microsoft, posted a public statement on the Microsoft official blog calling on the United States government to develop regulations around facial recognition technology.
The full text can be accessed at https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

On June 18, 2018, the New York Civil Liberties Union published a comment by Stefanie Coyle and John A. Curr III titled 'Facial Recognition Cameras Do Not Belong in Schools' which argues against the use of this technology in schools.
The full text can be accessed at https://www.nyclu.org/en/news/facial-recognition-cameras-do-not-belong-schools

On June 7, 2018, SFGate published an article by Drew Harwell of The Washington Post titled 'Unproven facial-recognition companies target schools, promising an end to shootings' outlining the increasing use of facial recognition cameras in some United Schools, including pre-schools, and suggesting the limitations of the technology.
The full text can be accessed at https://www.sfgate.com/business/article/Unproven-facial-recognition-companies-target-12977216.php

On May 31, 2018, The Intercept published a comment by Ava Kofman titled 'Face Recognition Is Now Being Used in Schools, but It Won’t Stop Mass Shootings' which considers the inadequacies of this technology as a means of protecting students.
The full text can be accessed at https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/

On May 21, 2018, Business Insider published an article titled 'A school in China is monitoring students with facial recognition technology that scans the classroom every 30 seconds' which gives an overview of how surveillance technology is being used in China.
The full text can be accessed at https://www.businessinsider.com.au/china-school-facial-recognition-technology-2018-5?r=UK&IR=T

On May 18, 2018, The South China Morning Post published a news report titled 'Pay attention at the back: Chinese school installs facial recognition cameras to keep an eye on pupils' which outlines the use of facial recognition cameras by a school in eastern China to monitor the attentiveness of students in class.
The full text can be accessed at
https://www.scmp.com/news/china/society/article/2146387/pay-attention-back-chinese-school-installs-facial-recognition

On May 26, 2017, The Verge published a report titled 'This French school is using facial recognition to find out when students aren’t paying attention'. The report refers to a business school in Paris will soon begin using artificial intelligence and facial analysis to determine whether students are paying attention in class.
The full text can be accessed at https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france

On January 22, 2018, Business Insider published an article titled 'India will install cameras in classrooms amid a rise of surveillance measures in Asia' which details the plan to have surveillance cameras installed in all classrooms in India’s capital territory Delhi, after a spate of violent incidents.
The full text can be accessed at https://www.businessinsider.com.au/india-to-install-cameras-in-classrooms-surveillance-trend-asia-2018-1

On January 12, 2013, The Economist published an article titled 'Chips off the old block' which detailed the use of technology in a range of countries to allow parents to check their children's whereabouts and safety.
The full text can be accessed at https://www.economist.com/international/2013/01/12/chips-off-the-old-block

On September 4, 2010, Scottish Educational Review published an article titled 'Biometric surveillance in schools : cause for concern or case for curriculum?' by Tom Bryce et al or the University of Strathclyde, Glasgow. (The article was updated on October 21, 2018.)
The full text can be accessed at https://pureportal.strath.ac.uk/files-asset/3317520/SER42_1_Bryce_1_.pdf

Arguments in favour of using facial recognition cameras in schools

1. Facial recognition technology can efficiently and ongoingly monitor student attendance

All Australian schools are required by law to mark rolls through the day, to monitor attendance and to seek and record reasons for student absence from parents. There are similar requirements of schools in other jurisdictions around the world. One of the purposes for which facial recognition cameras are currently being used in schools is to monitor student attendance. Advocates of this system claim it is accurate, time-saving and gives an ongoing record of which students are on campus and in class. It can also be used to check student attendance during off-campus activities.

One of the manufacturers of these facial recognition programs, LoopLearn, has stated, 'Small, unobtrusive LoopLearn Devices are easily installed in all spaces and observe which students are present – displaying this information in an easy to use web dashboard and mobile app...Made for the classroom, these devices scan your learning spaces in real time providing detailed attendance data down to the minute.' https://www.heraldsun.com.au/kids-news/australian-schools-begin-spying-trials-using-facial-recognition-technology/news-story/2d38f743af6309dd2f68f696c3ffedc1

Another manufacturer of this technology, Ayra Analytics, has described the utility of its product in this way: 'Our team is currently solving one of the big challenges of student management – tracking attendance. Manually checking off names on a register is time-consuming for teachers and is prone to errors. After putting our collective heads together, we hit upon the perfect solution – facial recognition!

We initiated this technology using Python OpenCV, which is an image processing library that can be processed with pictures and video. The student pictures are saved in the library. School cameras are then able to sync with this image library to match student faces to the pre-loaded pictures, which happens via advanced machine learning algorithms.

This sophisticated technology can also be applied to identify students on school buses, to cut down on truancy.' https://www.ayraanalytics.com.au/facial-recognition-to-track-student-attendance/

One of the Victorian schools trialling facial recognition for roll marking is Ballarat Clarendon College. The College's acting principal, Shaune Moloney, has claimed that this technology allowed staff a chance to respond quicker to class absences in what was a duty of care, allowed them to know students were safe through the school day and to monitor more easily those who needed to leave early.

Mr Moloney said teachers no longer needing to take the roll helped to free up valuable teaching time in the classroom for carefully planned lessons. He also noted the technology would help eliminate the need for teachers to update the roll for late students.
https://www.thecourier.com.au/story/5658846/college-to-use-face-scan-technology-for-class-roll-call/

In July, 2014, the International Journal of Advances in Engineering & Technology, published a favourable evaluation of the use of facial recognition software in Indian schools and universities for monitoring student attendance. The article stated, 'When it comes to schools and universities, the attendance monitoring system is a great help for parents and teachers both. Parents are never uninformed of the dependability of their children in the class if the university is using an attendance monitoring system...With the monitoring system in place, the information can easily be printed or a soft copy can be sent directly to parents in their personal email accounts.' http://www.e-ijaet.org/media/38I21-IJAET0721360_v7_iss3_974-979.pdf

2. Facial recognition technology can increase student safety

One of the main arguments used to justify the use of facial recognition cameras in schools is that they help to create a safe school environment. According to this argument, facial recognition cameras can inhibit anti-social behaviour among students and can help identify and thus protect against dangerous intruders.

On May 19, 2016, School Governance published a comment by Craig D’Cruz, the National Education Consultant at CompliSpace, an Australian provider of Governance, Risk and Compliance (GRC) programs and services. D'Cruz stated, 'One of the prime objectives for Australian schools is to ensure that they provide a stable, safe and secure teaching and learning environment for their students and teachers. The development and maintenance of this environment often results in the promotion of a safety culture that is often identified in orderly and disciplined schools.'

D'Cruz went on to argue that surveillance technology can be an important part of promoting a safe environment within schools. He stated, 'The use of this technology can enhance the perception of safety amongst students and staff, can protect school property against acts of vandalism and can aid in the identification of perpetrators of crimes and anti-social behaviour. Security experts in schools that use surveillance technologies comment that students and teachers seem to appreciate the increased sense of security and peace of mind. Research also suggests that although cameras are generally passive, information about their presence quickly becomes apparent throughout the school and the wider community. Schools advise that the school community feels safer knowing that potential perpetrators will be scared off by the presence of cameras before committing an offence.' http://www.schoolgovernance.net.au/2016/05/19/the-use-of-closed-circuit-cameras-in-schools/

It has further been noted that facial recognition cameras can help protect students against dangerous intruders. The trend toward the use of facial recognition cameras for this purpose has been particularly pronounced in the United States as a means of helping to prevent school shootings.

On June 8, 2018, Ed Scoop published an analysis by Emily Tate of the use of technology in United States schools for security purposes. Tate noted the more frequent employment of 'high-tech systems to increase security, such as mobile apps that allow real-time head counts during emergency situations, facial recognition technology that identifies individuals who have been placed on a school’s “blacklist” and tools that recognize and alert officials to exposed guns.' https://edscoop.com/school-safety-security-role-of-technology-in-school-shootings/

Referring to the facial recognition cameras being used in New York's Lockport High School, its manufacturers, SN Tech notes, '[It] alerts school staff to any unwanted individuals on school property when those individuals’ faces come into view of one of the 300 high-resolution digital cameras on Lockport’s premises. The list includes registered sex offenders and anyone with a violent criminal conviction, but it may also extend to students who have been suspended or expelled, employees who have been fired, parents who have lost custody or anyone else who may pose a threat and whose photo has been programmed into the system.' https://edscoop.com/school-safety-security-role-of-technology-in-school-shootings/

3. Facial recognition technology can help teachers monitor student engagement

Another area where facial recognition technology has been claimed to be of benefit to schools is in the monitoring of student engagement.

Ellucian, an education technology company which operates in nearly 50 countries around the world, actively promotes the use of facial recognition cameras to 'enhance the student experience.' The Ellucian Internet site states, 'Facial recognition technology can be programmed to recognise a wide range of nonverbal expressions and emotions. Through this, a professor can assess the emotion levels of the class to determine the parts of his lecture that are the most exciting and engaging, or where students’ attention appears to diminish. In this way, every unique face can function like a uniquely identifiable thumbprint that also speaks, through verbal and nonverbal data.' https://www.ellucian.com/emea-ap/insights/facial-recognition-can-give-students-better-service-and-security

The site further explains, 'As class-engagement data of this sort comes in, week to week and semester to semester, faculty and administrators can partner to build new data models that unlock powerful insights into how students learn, what methods are most effective, and what differentiates great classes (and great teachers) from less-effective learning experiences. Furthermore, as a student matriculates toward graduation one semester at a time, aggregate data can perhaps be used to discover learning strengths and areas of concern, enabling more tailored learning experiences that can lead each student to better outcomes.' https://www.ellucian.com/emea-ap/insights/facial-recognition-can-give-students-better-service-and-security

This technology has begun to be used in some Chinese schools. It has been reported that the technology scans classrooms at Hangzhou No. 11 High School every 30 seconds and records students' facial expressions, categorising them into happy, angry, fearful, confused or upset. The system also records student actions such as writing, reading, raising a hand, and sleeping at a desk. https://www.businessinsider.com.au/china-school-facial-recognition-technology-2018-5?r=UK&IR=T

The information collected by this system is analysed and reported to teachers so they can better supervise the performance of their students. Zhang Guanchao, the school's vice principal, that the system can help teachers rethink their teaching method using statistical data. http://en.people.cn/n3/2018/0519/c90000-9461918.html

An unnamed student was quoted as saying, 'Beforehand in some classes that I didn't like much, sometimes I would be lazy and do things like take naps on the desk or flick through other textbooks. Since the school has introduced these cameras, it is like there are a pair of mystery eyes constantly watching me, and I don't dare let my mind wander.' The unnamed student added he felt everyone's concentration had improved. https://www.scmp.com/news/china/society/article/2146387/pay-attention-back-chinese-school-installs-facial-recognition

4. Facial recognition technology is favoured by many parents

Supporters of the introduction of facial recognition cameras into schools for security purposes argue that this technology is generally valued by parents as an important means of keeping children safe, especially from attacks from intruders at their schools.

The parent-supported use of facial recognition technology in a number of United States schools has been used to demonstrate parents' acceptance of such programs. Since March, 2017, Seattle's private elementary University Child Development School (UCDS), has used a facial recognition system, Secure, Accurate Facial Recognition (SAFR), to control the entry and exit of parents who come to pick up or drop off their children.

The system acts as an automatic doorman for parents and staff members - if a parent's face is recognized by the camera mounted above the front gate, the door opens, largely removing the need for someone inside the school to answer a buzzer. The school sent out information about the system to parents and gave them the option of adding their face to the machine's database, which about 300 parents and caregivers have done. https://www.seattletimes.com/business/technology/as-facial-recognition-technology-grows-so-does-wariness-about-privacy/?utm_content=buffer4bcc1&utm_medium=social&utm_source=twitter&utm_campaign=owned_buffer_tw_m

Parent Ana Hedrick, whose daughter attends the school, has stated that the use the SAFR technology to recognize a great number of individuals makes her feel more secure about her child’s attendance at University Child Development School. Hedick stated, 'It's very convenient. It feels safe.' https://fee.org/articles/facial-recognition-scanning-in-schools-has-arrived-fueling-privacy-concerns/

This opinion was reiterated by another mother whose children attended the University Child Development School, who stated, 'Feeling like my kids are safe here is huge.' https://www.seattletimes.com/business/technology/as-facial-recognition-technology-grows-so-does-wariness-about-privacy/?utm_content=buffer4bcc1&utm_medium=social&utm_source=twitter&utm_campaign=owned_buffer_tw_m

A similar reaction has been recorded from David Weil, the director of an after-school recreation centre in Bloomington, Indiana. The centre has installed a system that logs thousands of visitors’ faces - alongside their names, phone numbers and other personal details - and checks them against a regularly updated blacklist of sex offenders and unwanted guests. Weil, whose granddaughter attends the centre he directs, has stated, 'Some parents still think it’s kind of "1984". A lot of people are afraid we’re getting too much information. . . . But the biggest thing for us is that we protect our kids.' https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html?utm_term=.ddbf714d52e3

In 2014, St. Mary’s High School in St. Louis because one of the first schools in the United States to install facial recognition cameras to help guarantee its students' safety. The school’s president, Mike England, has stated, 'When Parkland [an area which suffered a student mass shooting on February 14, 2018] happened, I was watching it on the TV going, "Boy, I’m glad we have what we have." Some people were saying we would be violating privacy laws, and my answer to all of them is: That’s really not my biggest concern right now. . . . I’m going to do whatever I need to do to keep my kids safe.' https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html?utm_term=.78df0b75acf4

The support of other parents for the security program operating at St. Mary’s High School was indicated in an article published in the St Louis Post-Dispatch on March 9, 2015. One of the parents, Mary Pat Banach, whose 16-year-old son, Michael, attended St. Mary’s, was quoted as saying that the cameras offered 'comfort', not a sense of confinement. She stated she had watched the company install the equipment from inside the school gift shop, where she volunteers, and concluded, 'I’ve always felt safe on campus, but it is just something that makes you feel comfortable because with any school, you just never know what could happen.' https://www.stltoday.com/news/local/crime-and-courts/st-mary-s-high-school-adds-facial-recognition-locks/article_db488bb5-44f2-5301-b131-8a7ebe04bba9.html

5. Facial recognition technology need not infringe student privacy

Many supporters of the use of facial recognition technology in schools, including those who manufacture the systems, argue that it can be used in a way that does impinge upon student privacy.

RealNetworks, the developers of the SAFR facial recognition systems recommend a set of steps to ensure that clients' (including students') privacy and autonomy is respected. They stress, 'The first element of proper facial recognition implementation is clear and transparent communication with stakeholders—including parents, staff and students—at the early stages of consideration. Soliciting thoughts and concerns from the community before any systems are installed improves the chances of a smooth and successful deployment.

Once the decision to implement a facial recognition system has been discussed and approved, all stakeholders should be notified, preferably in writing or via email, of the upcoming installation and told precisely what data will be collected and how it will be used.

Schools should take a thoughtful approach regarding camera placement. This includes avoiding putting cameras in areas likely to be considered sensitive, such as restrooms, locker rooms, classrooms, nurses' offices, or guidance counsellor offices. Once systems are installed, notice should be clearly posted wherever cameras are present.'
https://safr.com/general/privacy-by-design-best-practices-for-using-facial-recognition-to-support-safer-k-12-campuses/
RealNetworks then recommends, 'To meet Privacy by Design principles and legal requirements, schools should obtain explicit consent prior to collecting biometric data. A sign stating, "By entering these premises, you agree to being photographed" is not sufficient. Explicit consent means that a person needs to "opt in" or "say yes" before agreeing. If there are parties who are underage, an appropriate guardian can opt in on their behalf.
Explicit consent also requires that the school be clear about what they are doing, why they are doing it and what is being done with the data. Again, signage assuming consent fails to meet this standard. An example of explicit consent could be a signed document reading, "I agree to be recorded so that my face can be matched to a database of people allowed to enter this campus. I understand that my data will not be shared with any third parties and will not be retained for more than one year." Consent can be revoked when a user deletes his or her account, or sends in a form stating consent has been withdrawn. Upon withdrawal, all data of that individual should be immediately removed from the system and destroyed.'
https://safr.com/general/privacy-by-design-best-practices-for-using-facial-recognition-to-support-safer-k-12-campuses/
A further element of privacy protection that RealNetworks emphasise is data security. RealNetworks states, 'When a new security system has been implemented, staff, students, and visitors may expect that the school is taking care to protect their data and privacy. To meet this expectation, schools need to have modern security protections in place.
RealNetworks provides several options to support secure data storage, with options for storage at the school or managed in the cloud. Having multiple options for data security ensures flexibility for the school, and protection for the user. The data is also password-protected, encrypted, and can only be accessed by a select group of authorized users.'
https://safr.com/general/privacy-by-design-best-practices-for-using-facial-recognition-to-support-safer-k-12-campuses/

Arguments against using facial recognition cameras in schools

1. Facial recognition technology is not sufficiently accurate
Opponents of the use of facial recognition technology in schools argue that they are not sufficiently accurate to be relied upon. Inaccuracies make these devices unsuitable both as a means of alerting a school that a potentially dangerous intruder is on campus or as a means of monitoring student attendance.
The American Civil Liberties Union of Northern California tested Amazon's Rekognition facial recognition system by loading it with photos of members of Congress and letting it run comparisons to arrest photos. The test resulted in 28 false matches, of which nearly 40 percent were of people of color, even though they make up only 20 percent of Congress.
https://www.aclu.org/blog/privacy-technology/surveillance-technologies/heres-what-happens-when-we-allow-facial

Joy Buolamwini, a researcher, at Massachusetts Institute of Technology, has demonstrated that for some commercial facial recognition software the accuracy rate in 99 percent when the subject is a white male; this rate drops dramatically for other racial groups and for women. For darker skinned women the error rate rose to nearly 35 percent.
https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

This error rate reflects the data bias of the information bank used to establish the system. The more instances of a particular race or gender the databank holds the more accurate the system will be. This means that for minority groups or groups otherwise underrepresented in the databank there is a far greater risk of misidentification.
https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

This misidentification should be less likely to occur in a roll marking system where the databank is composed of all the children in a particular school; however, where a system is alerting a school to the presence on its campus of someone on its 'blacklist', the biases in that databank could well led to misidentification.

It has been noted that the accuracy of the technology is reduced when the subject to be identified has been photographed in a different light or in motion. It has also been noted that children pose particular problems for facial recognition technology. This is significant whether the technology is being used to monitor student attendance or to indicate the presence of intruders. Demonstrating the potential recognition problems children pose, Apple has recently warned that its new facial recognition tool, Face ID, should not be used by children under the age of 13. The firm claims that their faces 'may not have fully developed' and are too similar, increasing the chance that their iPhone could be unlocked by someone else. https://www.dailymail.co.uk/sciencetech/article-4926328/Q-A-How-Apples-Face-ID-facial-recognition-works.html

For children, whose appearances change rapidly as they grow, the accuracy of this technology is questionable. A spokesperson for the American Civil Liberties Union of Northern California has stated, 'False positives for a student entering school or going about their day can result in traumatic interactions with law enforcement, loss of class time, disciplinary action, and potentially a criminal record.' https://www.aclu.org/blog/privacy-technology/surveillance-technologies/heres-what-happens-when-we-allow-facial

2. Facial recognition technology does not guarantee student safety

Critics of facial recognition technology as a means of ensuring student safety argue that such systems are unlikely to be effective.

In an opinion piece published on The Intercept on May 31, 2018, Ana Kofman criticised the probable ineffectiveness of the facial recognition-based surveillance system being employed within the Lockport School District, New York. Kofman stated, 'Given the nature of gun violence at schools, Lockport’s purchase of surveillance technology appears inefficient and expensive. All of the major school shootings in the last five years in the U.S. have been carried out by current students or alumnae of the school in question. “These are students for whom the school wouldn’t have a reason to have their face entered into the face recognition system’s blacklist,” explained Rachel Levinson-Waldman, a security and policing expert at the Brennan Center for Justice.' https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/

Similar claimed were made by Toni Smith-Thompson in an opinion piece published by the American Civil Liberties Union on August 15, 2018. Smith-Thompson states, 'While the current call for increased safety against school shooters has fuelled a wave of increased surveillance, this technology does not mitigate the risk. The vast majority of school shooters are first-time offenders and would not be included in any database to prevent them from entering a school. Indeed, perpetrators who are themselves students would easily gain access to school facilities.' https://www.aclu.org/blog/privacy-technology/surveillance-technologies/heres-what-happens-when-we-allow-facial

Smith-Thompson further noted that facial recognition technology can be easily subverted. She wrote, 'Facial recognition technology is especially prone to sabotage: for 22 cents, you can purchase a pair of cardboard glasses to fool it.' https://www.aclu.org/blog/privacy-technology/surveillance-technologies/heres-what-happens-when-we-allow-facial

Researchers from Carnegie Mellon University have shown that specially designed spectacle frames can mislead state-of-the-art facial recognition software. The glasses can make the wearer disappear to such automated systems. It can also cause these systems to misidentify the wearer as someone else. https://www.theverge.com/2016/11/3/13507542/facial-recognition-glasses-trick-impersonate-fool

Andrew Ferguson, a law professor at the University of the District of Columbia, has claimed that surveillance companies are preying on the dread of schools and parents by selling experimental 'security theatre' systems that offer only the appearance of safer schools. Professor Ferguson has stated, 'These companies are taking advantage of the genuine fear and almost impotence of parents who want to protect their kids and they're selling them surveillance technology at a cost that will do very little to protect them.' https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html?utm_term=.2af0642f492f

3. Use of facial recognition technology can be overly restrictive

Opponents of the constant use of facial recognition technology in schools argue that this undermines students' privacy in a way that damagingly restricts their freedom, limiting their capacity to explore different sorts of behaviour because they fear being judged or punished.

Martin Chorzempa, a fellow at the Peterson Institute for International Economics, has considered the way in which surveillance can be used to shape behaviour and force compliance. Chorzempa stated, 'The whole point is that people don't know if they're being monitored, and that uncertainty makes people more obedient.' He described the approach as a panopticon (an institutional arrangement through which people are potentially watched at all times), the idea that people will follow the rules precisely because they believe they may be under observation. https://www.seattletimes.com/business/inside-chinas-dystopian-dreams-ai-shame-and-lots-of-cameras/

It has been claimed that one of the values of privacy is that it is an opportunity to act without fear of judgement. Dr Niels Wouters, of the Microsoft Research Centre for Social Natural User Interfaces at the University of Melbourne, has stated, 'A child trying out who they are under the constant gaze of an intelligent camera could mean they become forever judged for pulling weirdo faces.' Dr Wouters is equally concerned that fear of this potential judgement means that children do not explore different types of behaviour. He has stated, 'This takes away a huge sense of freedom for these children...It's an important thing in childhood to explore boundaries.' https://thenewdaily.com.au/life/tech/2018/08/29/facial-recognition-schools-trial/?utm_source=Adestra&utm_medium=email&utm_campaign=Morning%20News%2020180830

The New York Civil Liberties Union (NYCLU) has similarly warned of the damagingly restrictive quality of facial recognition technology used within schools. Responding to its use within the Lockport City School District, Toni Smith-Thompson of NYCLU stated, 'Schools should be safe environments for students to learn and play. They should be places where

students can test out and practice ideas, interactions, and activities and be supported to make their own (safe) choices. Pervasive monitoring and collection of children’s most sensitive information — including their biometric data — can turn students into perpetual suspects. It exposes every aspect of a child’s life to unfair scrutiny.'
https://www.nyclu.org/en/news/heres-what-happens-when-we-allow-facial-recognition-technology-our-schools
A similar point was made by two other members of the NYCLU in an article published on June 18, 2018. Stefanie Coyle and John A. Curr III warn, 'In the system Lockport purchased, once a person’s facial image is captured by the technology and uploaded, the system can go back and track that person’s movements around the school over the previous 60 days.
It’s easy to imagine that students will feel like they are constantly under suspicion. Lockport is sending the message that it views students as unpredictable, potential criminals who must have their faces scanned wherever they go.' https://www.nyclu.org/en/news/facial-recognition-cameras-do-not-belong-schools
Privacy advocates are concerned about the atmosphere of suspicion that ongoing facial recognition surveillance could create within schools. In a letter of protest written by the NYCLU on June 18, 2018, its authors noted, 'Lockport plans to utilize this technology in each school in the District, including elementary schools, resulting in facial imaging of four-and five-year-old children. That fact should shock the conscience of any person who cares about education. We are concerned that no one at the District...questioned the wisdom of this purchase from the perspective of school climate, or the message it sends to our young people about their futures, their relationships with adults, or their sense of belonging in their school.
Rather than protecting them, the District is treating every child as a threat; rather than human relationships, the District is relying on machines to do its job.'
https://www.nyclu.org/sites/default/files/field_documents/june18_2018_nyclu_letter_re_lockport_city_school_district.pdf

4. Facial recognition technology is often installed without adequate community consultation
Critics of the use of facial recognition cameras within schools are concerned that these devices are being introduced without the consent of the whole school community and without the nature of their operation being properly explained.
The New York Civil Liberties Union (NYCLU) has investigated the manner in which facial recognition cameras were introduced into schools in the Lockport School District, New York, and has discovered a lack of consultation with parents and students before the devices were introduced. The NYCLU states, 'The Smart Schools Bond Act, which provides funding for technology in schools, includes specific requirements for engaging community stakeholders, including children, teachers and parents... [The] documents the Lockport School District provided show they held only one public meeting to introduce the community to the idea of using state money for technology in the classroom to purchase surveillance technology. After the meeting, the school moved forward with an application to acquire the facial recognition software. That meeting was in the middle of a weekday afternoon in August, when many parents are at work or out of town. There were no emails or flyers showing engagement of students and parents in the process of deciding to adopt this technology. In fact, the head of the Lockport Education Association told a reporter they were not consulted.'
https://www.nyclu.org/en/news/we-asked-answers-facial-recognition-schools-our-questions-remain
Lockport resident, Jim Shultz, has created a petition asking the Lockport City School District to postpone the implementation of the facial recognition system within the district's schools until proper community consultation has taken place. Mr Shultz has complained that concerns

about the cost and the relative effectiveness of the system have not been addressed and that there has been no adequate opportunity for school communities to give their view. https://www.lockportjournal.com/news/local_news/citizens-petition-lcsd-to-postpone-security-project/article_e8d547e1-0e3a-5a2e-81c3-5879422548c2.html

In a comment published in Times Union on November 6, 2018, Mr Shultz stated, ' State education officials need to halt the state funding for the Lockport plan until it is audited for its financial irregularities and its lack of community consultation, and until serious privacy protections are guaranteed.' https://www.timesunion.com/opinion/article/School-cameras-give-illusion-of-safety-at-13368490.php

5. There need to be stronger laws and regulations to ensure that facial recognition technology is not misused

Critics of the use of facial recognition technology within schools argue that for systems that are intended to increase control of school environments, their operation is often not properly regulated. There are serious questions often left unanswered about the use and misuse of the data and critics are concerned that transparent protocols for its application and storage have not been set up. Underlying this is the concern that in many jurisdictions there are inadequate legal guarantees to protect citizens' privacy.

The New York Civil Liberties Union (NYCLU) has expressed concern about the lack of regulation to control the use of facial recognition data collected in the Lockport School District. The NYCLU has stated, 'There are...no regulations in place to account for the serious inaccuracy of this technology, which is most likely to misidentify people of color. And there is no policy in place to limit who will have access to the data collected from the cameras that scan the faces of thousands of parents, teachers and children every day.' https://www.nyclu.org/en/news/we-asked-answers-facial-recognition-schools-our-questions-remain

A similar complaint was made by a parent, Jim Shultz, whose daughter attends Lockport High School. Mr Shultz's comment was published in Times Union, on November 6, 2018. Mr Shultz stated, 'No rules or policies exist regarding who can put a student's facial image in the system, how long the images can be held, or who has the authority to use the system to track a student's movements. Can the local police demand access to the system? Federal agencies? None of this is spelled out. State education officials approved the funds for this new surveillance system without any consideration as to how it can be used.' https://www.timesunion.com/opinion/article/School-cameras-give-illusion-of-safety-at-13368490.php

On July 13, 2018, Microsoft President, Brad Smith, made a public appeal for governments to establish some regulation of facial recognition systems. In a public post on the company's blog site, Smith stated, 'It seems especially important to pursue thoughtful government regulation of facial recognition technology, given its broad societal ramifications and potential for abuse.' https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

In Australia, concern regarding inadequate regulation of the use of facial recognition technology in schools is underpinned by concerns regarding a more general lack of safeguards surrounding citizens' privacy. In an opinion piece published in The Conversation on October 6, 2017, Bruce Baer Arnold, Assistant Professor, School of Law, University of Canberra, stated, '[Australia is] a nation where Commonwealth, state and territory privacy law is inconsistent. That law is weakly enforced, in part because watchdogs such as the Office of the Australian Information Commissioner (OAIC) are under-resourced, threatened with closure or have clashed with senior politicians.

Australia does not have a coherent enforceable right to privacy. Instead we have a threadbare patchwork of law (including an absence of a discrete privacy statute in several jurisdictions).' https://theconversation.com/lets-face-it-well-be-no-safer-with-a-national-facial-recognition-database-85179

There have been similar concerns expressed about a lack of effective overarching privacy legislation in the United States. In an analysis written by Drew Harwell of the Washington Post and published on June 7, 2018, it was noted, 'No federal law restricts the use of facial-recognition technology, and only Illinois and Texas have passed laws requiring companies to get people's consent before collecting what the industry calls "faceprints." That allows local police forces, cities, employers and school boards to largely set their own policies.' https://www.sfgate.com/business/article/Unproven-facial-recognition-companies-target-12977216.php

Those who are concerned about the lack of adequate laws to protect privacy argue that China's leading role in developing and using facial recognition technology is concerning. China has a more problematic attitude to the protection of individual liberties than do Western democracies. Tiffany Lee, writing for The World Post, in an opinion piece published on August 7, 2018, warned that China's relative indifference to privacy issues is likely to influence international attitudes. Lee states, 'China's rapidly advancing technology industries and massive consumer market are already influencing norms around the world. China will likely impact the way privacy is understood and protected.' Lee argues that China's increasing influence has created an even greater need for strengthened national and international digital privacy laws. https://www.washingtonpost.com/news/theworldpost/wp/2018/08/07/china-privacy/?utm_term=.efc6c5a30613

Further implications

One of the major concerns about the use of facial recognition technology in schools is that it may habituate young people to accept the use of these systems and desensitise them to the potential risks involved. It is argued that this will encourage schoolchildren to accept subsequent, more extensive applications of such systems which could have harmful implications for their personal freedoms.

Adam Schwartz, a lawyer with United States digital privacy group Electronic Frontier Foundation, has stated, 'There’s a general habituation of people to be tolerant of this kind of tracking of their face. This is especially troubling when it comes to schoolchildren. It’s getting them used to it.' https://www.seattletimes.com/business/technology/as-facial-recognition-technology-grows-so-does-wariness-about-privacy/

Victoria's Information Commissioner, Sven Bluemmel, has raised the same concern. Mr Bluemmel has queried, 'Do we want our children to feel like it’s normal to be constantly under surveillance?' https://www.theage.com.au/national/victoria/minority-report-crackdown-on-facial-recognition-technology-in-schools-20181005-p5080p.html

The material which follows is an abbreviation of an opinion piece written by Cynthia Wong, published in the Australian edition of The Guardian on August 17, 2018, which aims to warn readers of some of the dangers associated with the Australian government's Identity Matching Services Bill. https://www.theguardian.com/commentisfree/2018/aug/17/we-underestimate-the-threat-of-facial-recognition-technology-at-our-peril

' Should the government be able to track your every move when you walk down the street, join a protest, or enter your psychiatrist’s building? Facial recognition technology may make that a reality for Australians. Parliament should refuse to expand its use until the government can demonstrate it won’t be used to violate human rights or turn us all into criminal suspects.

The bill would create a nationwide database of people's physical characteristics and identities, linking facial images and data from states and territories and integrating them with a facial recognition system.

The system would initially enable centralised access to passport, visa, citizenship, and driver license images, though states and territories may also link other information, for example, marine licenses or proof-of-age cards. Government agencies and some private companies would then be allowed to submit images to verify someone's identity. Government agencies will also use it to identify an unknown person. The Department of Home Affairs would manage the system.

Prime minister Malcolm Turnbull describes the proposal as a "modernisation" and "automation" of existing data-sharing practices between law enforcement agencies, making facial recognition "available in as near as possible real time." But the proposal is too broad, enables using facial recognition for purposes far beyond fighting serious crime, and leaves significant details to departmental discretion or future interpretation. The lack of safeguards combined with the centralisation of a massive amount of information raises the potential for abuse and ever-expanding mission creep (the expansion of the use of the technology beyond the scope originally intended)...

The bill raises immediate alarms about privacy and other rights. With scant limits on future data collection and use, the amount of data is likely to grow over time. It also obliterates notions of consent since information people disclose for one purpose—obtaining a fishing license—could be easily used for entirely different ones like targeting "jaywalkers or litterers."

Proponents contend that the system will not involve "surveillance" or direct integration with CCTV cameras. Nonetheless, the bill has the potential to facilitate broad tracking and profiling, especially when images are combined with other data. Imagine the chilling effect if officials ran photos taken from surveillance cameras at a demonstration or outside a union hall. Or the assumptions that could be made if you're caught on cameras outside of a drug treatment centre, abortion clinic, or marriage counsellor's office.

Notably, the proposal doesn't require law enforcement agencies to get a warrant before using the system to identify someone, which is critical to preventing abuse. And what would prevent the government from integrating it with CCTV once the technologies are in place?

Facial recognition technology is far from perfect. Independent studies have found these systems often have a racial or ethnic bias. Yet the government has not disclosed enough information about the accuracy of the system it intends to use. What are its error rates and are they higher for racial and ethnic minorities? This is not a trivial issue. False positives mean people are wrongly accused or placed under unwarranted suspicion. False negatives mean criminals may continue to walk free...

Lack of explicit safeguards in the bill means that information could be abused by government officials, police officers, or even private companies against people in unpredictable and unexpected ways. Australia's patchwork of data protection laws provides insufficient safeguards against these risks...'