Comments to the Office of Science and Technology Policy

Introduction

Common Sense Media (Common Sense) is pleased to submit these comments in response to the Office of Science and Technology Policy's request for information on how biometric technology is being used in education. Common Sense is an independent, nonpartisan voice for children that champions policy solutions that puts children first and works to ensure that they can thrive in the 21st century.

Biometric technology, like all invasive technology, raises special privacy questions and concerns for children because of their unique vulnerabilities that stem from their brain development and young age. This is most apparent in the education context, in which some students have needed to agree to using certain technology to fully participate in school.

These comments discuss two ways in which biometric technology is being used in education: ed tech software, namely remote exam proctoring software and student activity monitoring software, and facial recognition in school buildings. Remote exam proctoring software and certain aspects of student activity monitoring software, such as the monitoring of keystrokes and eye movement, surveil students to a degree they find intrusive and disturbing, and can expose them to the risk of privacy breaches. Facial recognition software, which is increasingly used in school buildings to track attendance and admission, can also open students up to the risk of privacy breaches, and is often inaccurate, particularly for students of color. This can lead to wrongful identification and discipline of students, which exacerbates already existing inequities in education in which black children are more likely to be disciplined.

Children and teens are uniquely vulnerable on the internet. Their brains are still developing, which makes it difficult for them to distinguish advertising from content and understand the persuasive intent behind ads.[1] They are also prone to oversharing online without understanding the consequences of their sharing.[2] Young children in particular believe information remains at a device level or within an app, and they do not expect or understand that an app may gather information about them from third party sources or

[1] Ofcom, Children and parents: media use and attitudes report, November 2016.
[2] Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents* 26 Journal of Neuroscience 25 (2006) (teens' brain development can bias them towards risky behaviors).

that the information they delete remains available.[3] Some young children even consider monitoring by others to be positive.[4] Older children – as well as many adults – also cannot comprehend often long and legalistic privacy policies to better understand how their data is being collected and shared.[5] Many teens think that social networking sites do a bad job at explaining how they treat user information.[6] Because of children and teens' vulnerabilities, schools must prioritize their well-being and interests when considering whether to utilize biometric technology in the education context.

I. Students are increasingly using remote exam proctoring software and student monitoring software, making students uncomfortable and opening them up to the risk of privacy breaches

The use of technology in education has become more prominent than ever. In 2020, with most children attending school virtually because of the pandemic, there was a 69 percent increase in the amount of time kids spent using a computer or laptop for education.[7] This increase was driven largely by five- to 10-year olds.[8] Children also spent more time on tablets for education than anything else, a shift from the year before when gaming took the top spot.[9] Even before the pandemic forced students to stay home, educators increasingly saw the value of using technology in the classroom. In a 2019 survey, 89.6 percent of educators responded that they believed technology is a great way to engage students in the classroom, which was a sharp increase from 31.8 percent the previous year.[10]

In particular, schools are increasingly using remote exam proctoring software and student monitoring software. However, both of these types of software open students up to the risk of privacy breaches, and have been shown to make them uncomfortable and exacerbate inequities.

---

[3] "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks. In CHI '21: ACM CHI Conference on Human Factors in Computing Systems, May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA

[4] Gelman, Martinez, Davidson, Noles (2018), Child Development Journal; Sonia Livingstone, Mariya Soilova, Rishita Nadagiri, Children's data and privacy online: Growing up in a digital age, An evidence review, (Dec. 2018).; p. 18.

[5] Children's data and privacy online: Growing up in a digital age, An evidence review, Sonia Livingstone, Mariya Soilova, Rishita Nadagiri, p. 15. (Dec. 2018).

[6] Ofcom, Children and Parents: Media Use and Attitudes Report, (Nov. 2016). Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids, (2018).

[7] Ryan Tuchow, Kid device usage changing as a result of the pandemic, Kidscreen, (Feb. 19, 2021).

[8] *Ibid*

[9] *Id.*

[10] The State of Technology in Education, 2019-2020 Report, Promethean (2019).

A. Remote exam proctoring software

Schools have needed to turn to remote exam proctoring more than ever during the pandemic to conduct online exams and ensure students are not cheating. However, students have expressed privacy concerns about their remote proctoring experiences and reported disturbing incidents.[11] Remote proctoring software Proctorio claims to identify "suspicious behavior" by monitoring a student's webcam, microphone, keyboard, and other computer activity during an exam and then utilizes an algorithm to look for "abnormalities" between a student and their classmates.[12] Everything from abnormal head and eye movements, mouse clicks and scrolls, websites visited, audio levels, the time it takes to finish the test, to the number of faces detected on screen can all result in a student's test session being flagged as suspicious.[13] In addition to invasion of privacy complaints from this intense surveillance, students and faculty have voiced concern on a wide range of other issues Proctorio and similar remote proctoring services pose, such as bias against students of color, students with accessibility needs, and students with learning disabilities, as well as bias against low-income and rural students.[14]

Many schools have also used ProctorU, a software that similarly uses facial biometrics to match students to their photo identification, and then requests access to the camera, microphone, screen, and keystrokes.[15] In April 2020, nearly 4,000 students at Australia's University of Queensland signed a petition asking the university to come up with a better solution for final exams because of their fears the software would threaten their data privacy.[16] Although the company's privacy policy states the data it collects is only used for the exam session and is not sold to other parties, the data is at risk of being sold or transferred if "involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets."[17]

---

[11] Chris Burt, Concerns about biometric online proctoring expressed by students in Australia, U.S., and Canada, Biometric Update (Jul. 3, 2020).
[12] Tyler Sonnemaker, Tech companies promised schools an easy way to detect cheaters during the pandemic. Critics responded by demanding schools stop policing them like criminals in the first place, Business Insider (Nov. 1, 2020).
[13] *Id.*
[14] *Id.*
[15] Luana Pascu, Australian students fear exam platform threatens biometric data privacy, Biometric Update (Apr. 20, 2020).
[16] *Id.*
[17] *Id.*

B. Student activity monitoring software

Additionally, the number of teachers who reported distribution programs of school-issued devices to educate students at home rose from 43 to 86 percent in the first several months of the pandemic, and this number has only risen since.[18] This has created more opportunities for students to be monitored, particularly for students using school-issued devices.[19] Eighty-one percent of teachers report that their school uses some kind of monitoring software, yet only one in four of those teachers report that monitoring is only limited to school hours.[20] Monitoring software is usually installed directly on a device, which grants access to more of the device's information than browser-based software, which only monitors student content and web activity.[21] This puts students who depend on student-issued devices such as low-income students at greater risk.

Student activity monitoring software can interact with different operating systems and device permissions, such as access to biometric information like keystrokes and input devices like cameras and microphones, as well as content on the device screen. In the United States, thousands of school districts have installed surveillance software on school-issued devices to monitor students' online interactions.[22] Several universities have also started using technology to collect data on students' attention, such as a Paris university that tracks students' eye movement and facial expressions through laptop webcams.[23] This surveillance can make students uncomfortable, affecting their ability to freely learn.

The monitoring activity not involving biometrics is worth noting as well. Programs such as Bark, Gnosis IQ, Gaggle, and Lightspeed can be installed to search for language in student emails and chats and online behavior that indicates the possibility of violent tendencies, suicidal ideation, drug use, pornography use, or eating disorders.[24] School districts sometimes monitor students out of concern for their physical safety and mental health, particularly with students' reported increase in self-harm incidents and aggressive

---

[18] Elizabeth Laird, Research Report: Protecting Students' Privacy and Advancing Digital Equity, Center for Democracy & Technology (Oct. 22, 2020).
[19] Teachers reported monitoring software use in 71 percent of school-issued devices, compared to only 16 percent of personal devices. Sustained Surveillance: Unintended Consequences of School-Issued Devices, Center for Democracy & Technology (Sept. 21, 2021).
[20] Laird *supra* note 18.
[21] L. Holden Williams, Student Activity Monitoring Software and the Risks to Privacy, Center for Democracy & Technology (Oct. 6, 2021).
[22] Jessa Crispin, US schools gave kids laptops during the pandemic. Then they spied on them, The Guardian (Oct. 11, 2021).
[23] Erika Gimbel, Biometric tech can track how well students are paying attention, Ed Tech (Feb. 23, 2018).
[24] *Id.*

impulses since the start of the pandemic.[25] However, civil groups, teachers, and parents have warned this surveillance results in harmful, unintended consequences.[26] Most notably, online monitoring could be used to discipline students, "out" LGBTQ+ students who are not ready to come out, and chill student speech.[27] Forty three percent of teachers whose schools or districts use student activity monitoring software report that it is used to identify violations of disciplinary policies.[28] There is also a risk that schools may share this data with law enforcement or other external agencies.[29]

II. Schools are utilizing facial recognition technology that is often inaccurate for children, which can exacerbate inequities by leading to wrongful disciplining of children of color, and chill expression

An increasing number of school districts are utilizing facial recognition technology in schools in the name of reducing paperwork and improving school safety, such as by tracking attendance and entrances into school events. However, facial recognition software is often inaccurate, particularly for people of color and for children who are quickly growing and whose faces are changing. This is problematic because facial recognition software is often linked to criminal databases, and can produce wrongful identifications which can lead to schools disciplining the wrong students and chilling their freedom of expression.

Aside from monitoring of students on school-issued devices, the collection of biometric data is also on the rise in school buildings. School districts are launching biometric initiatives to cut down on paperwork as well as improve school safety.[30] For example, in 2019, a school district in Missouri installed 95 biometric facial recognition cameras that are linked to law enforcement databases.[31] If a camera detects a face from a criminal database, they trigger a school lockdown.[32] Biometrics such as fingerprint scans have also

---

[25] Emily Berger, More children are self-harming since the start of the pandemic. Here's what parents and teachers can do to help, The Conversation (Sept. 7, 2021); Beata Mostafavi, National Poll: Pandemic Negatively Impacted Teens' Mental Health, Michigan Health (Mar. 15, 2021).
[26] *Supra* note 19.
[27] *Id.*
[28] Navigating the New Normal: Ensuring Equitable and Trustworthy EdTech for the Future, Center for Democracy & Technology (Nov. 16, 2021).
[29] *Id.*
[30] Shawna De La Rosa, Biometrics can make schools safer, but privacy concerns persist, K-12 Dive (May 9, 2019).
[31] Chris Burt, Missouri school district deploys Panasonic facial recognition for security and access control, Biometric Update (Apr. 10, 2019).
[32] *Id.*

been used to track student tardiness, library check-out, and entrances to dances and athletic events.[33]

While using biometrics can help make schools safer or cut down on paperwork, like all other types of data, biometric information can be breached and sold. Little is known about how these vendors store and use data.[34] Additionally, most districts do not have full-time employees dedicated to protecting student privacy. Teachers also receive little education on student privacy.[35] However, an increasing number of teachers have received training related to student privacy issues, with the number having risen from 56 to 66 percent of teachers from 2020 to 2021.[36]

The accuracy of facial recognition technology in particular raises concerns. Over time, the appearance of faces change, especially for children who are actively developing and growing. In a 2019 NIST report on facial recognition, researchers found aging increased false negative rates.[37] Factors such as the environment in which a face is scanned, the person's posture, and lighting can also affect the accuracy of a facial scan.[38] Many studies have also shown that facial recognition software is less accurate for people of color and women compared to white men.[39] One study found that such software was inaccurate for up to 35 percent of darker-skinned women.[40]

The consequences are particularly problematic for children of color. Inaccurate facial recognition could lead to misidentification of students suspected of fighting, skipping class, and breaking other school rules, which could lead to the wrong children being investigated or disciplined.[41] This would only further perpetuate the institutional racism seen in school systems and the criminal justice system, which already disproportionately harms black children, because it could encourage them to trust a software's identification over a child's own words.[42]

---

[33] *Id.*
[34] De La Rosa *supra* note 30.
[35] Nadia Tamez-Robledo, What do teachers know about student privacy? Not enough, researchers say, EdSurge (Oct. 8, 2021).
[36] Key Views Toward EdTech, School Data, and Student Privacy, Center for Democracy and Technology (Nov. 2021).
[37] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT), Part 2: Identification, National Institute of Standards and Technology (Sept. 2019).
[38] *Id.*
[39] Facial recognition technology in US schools threatens rights, Human Rights Watch (June 21, 2019).
[40] Steve Lohr, Facial recognition is accurate, if you're a white guy, N.Y. Times (Feb. 9, 2018).
[41] *Supra* note 39.
[42] *Id.*

Even if facial recognition was completely accurate, the risks to children do not stop there. Having facial recognition cameras around could chill children's freedom of expression, such as by discouraging them from being spontaneous or playful or associating with friends or siblings the school regards as troublemakers.[43] This could significantly impact children's emotional and intellectual development.[44]

III. Schools must prioritize students' well-being and interests when deciding whether to utilize new biometric technology

Biometric technology is largely left unregulated, with only a small number of states having passed a biometric-specific law, and even fewer having passed laws restricting the use of facial recognition technology specifically. Due to children's unique developmental vulnerabilities, until more legislation is passed, schools must prioritize students' well-being and interests when utilizing this technology both in an online schooling and an in-person schooling context. Until more legislation is passed, private and public entities must exercise caution in utilizing facial recognition and other biometric technology.

Currently, only five states have a biometric-specific law.[45] Illinois passed the Biometric Information Privacy Act (BIPA) in 2008, becoming the first U.S. state to regulate the collection of biometric data. BIPA requires private entities that obtain biometric information to first inform the subject in writing that their information is being collected and stored, inform the subject of the specific purpose for collection and the term of storage, and obtain a written release from the subject.[46] It prohibits disclosure of biometric information without the subject's consent, unless an exception is satisfied. Since then, Arkansas, California, Texas, and Washington have adopted legislation modeled after BIPA.[47]

Most recently, this summer, Maine passed a law prohibiting the use of facial recognition in all levels of government, making it the toughest facial recognition law yet.[48] However, other states have had very little success in passing laws that ban or heavily restrict facial

---

[43] *Id.*
[44] Lindsey Barrett, Ban facial recognition technologies for children–and for everyone else, 26 B.U. J. Sci. & Tech. L. 225, 252 (2020).
[45] Amy De La Lama, Lauren J. Caisman, and Melissa R. Whigham, United States: U.S. Biometric Laws & Pending Legislation, Mondaq (May 18, 2021).
[46] Dmitry Shifrin and Mary Buckley Tobin, Past, present and future: What's happening with Illinois' and other biometric privacy laws, National Law Review (May 28, 2021).
[47] Christopher G. Ward and Kelsey C. Boehm, Developments in biometric information privacy laws, Foley (June 17, 2021).
[48] Grace Woodruff, Maine now has the toughest facial recognition restrictions in the U.S., Slate (July 2, 2021).

recognition.[49] Such bills failed to advance or were rejected by at least 17 states during the 2020 and 2021 sessions.[50] Washington is the only other state to have a statewide facial recognition law, but it authorizes state police to use facial recognition technology for "mass surveillance of people's public movements, habits, and associations."[51]

In 2019, New York became the first state to enact a moratorium on purchasing or using any biometric identifying technology for school until at least July 2022.[52] The ban also required the New York State Department of Information Technology Services to conduct a study on whether and under what conditions technologies such as facial recognition technology should ever be used in schools.[53]

Children specifically must be given more thought and care. Because of their young age and developing brains, children are already uniquely vulnerable. Using facial recognition and other biometric technology on children can lead to misidentification, particularly for children of color, which can lead to unfair discipline, as well as chill children's freedom of expression. In utilizing this technology, private and government entities must acknowledge the unique vulnerabilities of children before determining whether to put it to use. They must carefully evaluate the negative consequences on students and put their well-being and privacy first. If the benefits do not significantly outweigh the consequences or potential consequences, schools should not utilize the technology.

IV. The Department of Education and the Federal Trade Commission should establish a working group to study the impact of biometric technology on children

Children and teens' unique vulnerabilities make the many concerns biometric technology such as facial recognition poses in the education context so important to address. As a first step, the Department of Education and the Federal Trade Commission should work together to establish a working group that brings key stakeholders together to further study the impact of this technology on children. This working group should include academic researchers, pediatricians, and children's advocates who have specific knowledge of children's development and tendencies. This would offer these agencies

[49] Jake Parker, Most state legislatures have rejected bans and severe restrictions on facial recognition, Security Info Watch (July 12, 2021).
[50] *Id.*
[51] Woodruff *supra* note 41.
[52] Press Release, NYCLU, New York creates first-in-the-nation moratorium on facial recognition in schools (Dec. 22, 2020).
[53] *Id.*

and OSTP with additional information on biometric technology that can be used to inform policy making and proposed regulations.

Conclusion

Common Sense appreciates the opportunity to provide information OSTP with information on how biometric technology is being used in the educational context. OSTP should be aware of the harms that can come from using this technology on children in schools, and encourage entities to use special care when doing so.

Respectfully submitted,
Irene Ly
Policy Counsel, Common Sense Media

Date: January 14, 2022