

Dangerous Data

What Communities Should Know about Artificial Intelligence, the School-to-Prison Pipeline, and School Surveillance

By: Clarence Okoh

May 2024

Executive Summary

Public and private actors are turning to artificial intelligence (AI) and other big data technologies¹ to engineer new futures for structural racism and social inequality in the United States, a phenomenon that the sociologist Ruha Benjamin has termed the “New Jim Code.”²

These technologies are upending decades of civil and human rights legal standards, expanding mass criminalization, restricting access to social services, and enabling systemic discrimination in housing, employment, and health care, among other areas.³ The New Jim Code carries unique threats to youth and young adults of color, especially in the context of K-12 public schools.⁴

In recent years, federal policymakers have taken steps to address the societal implications of AI and big data technologies, including the White House Blueprint for an AI Bill of Rights, President Biden’s Executive Order on Artificial Intelligence, and the U.S. Department of Education’s guidance on AI in schools.⁵ However, these efforts have largely failed to address the specific harms that these technologies raise for youth and young adults of color and youth from other historically marginalized communities.

As the infrastructure of police surveillance grows in public schools, communities must be prepared to safeguard the rights and freedoms of students and families. This report is designed to help youth justice advocates, youth leaders, educators, caregivers, and policymakers understand and challenge the impact of school surveillance, data criminalization, and police surveillance technologies in schools.

This report includes:

- An analysis of six key facts about the impacts of data criminalization and school surveillance technologies on education equity.
- A case study of an AI school surveillance technology that can land children in adult misdemeanor court.
- Key recommendations for education policymakers and school district leaders for advancing youth data justice.

Introduction

Emerging technologies such as AI and machine learning have rapidly transformed the educational landscape. While much of the discourse on AI in education has focused on its role in learning and instruction, less attention has been devoted to the impact of these systems on educational equity and students' civil and human rights, especially in the context of school discipline and policing.

Young people must navigate a complex and growing web of school surveillance technologies that leverage student data to monitor, punish, and control their lives not just at school but at home and online.⁶ This is especially true for young people from historically marginalized communities, including Black, brown, LGBTQIA+, immigrant, low-income, and disabled populations.⁷ The popularity of school surveillance technologies has grown in recent years, fueled by increased COVID-era education funding and heightened fears surrounding school shootings and youth violence.⁸

School surveillance blurs the boundary between the schoolhouse and the jailhouse by providing a digital infrastructure that deepens the role of law enforcement, including immigration enforcement and family policing, in the lives of marginalized youth and their families.⁹

This report offers an overview of the growth, impact, and harm of school surveillance and youth data criminalization. Its purpose is to demystify the role of these technologies and help communities better understand how these systems work to resist their harms more effectively.

This report includes a discussion of two related but distinct concepts, school surveillance and youth data criminalization.



School surveillance:

Refers to surveillance techniques, systems, and technologies that extract, analyze, and/or compile sensitive details about students' lives for the purposes of monitoring, censoring, punishing, criminalizing, or controlling them, their families, and others connected to schools. This term includes technologies such as student device monitoring, social media surveillance, facial recognition, vape detection, weapons detection, geolocation tracking, surveillance cameras, and license plate readers.



Youth data criminalization:

Occurs when public or private actors use sensitive data (e.g. education records, biometric data, mental health records) related to individual youth and their communities to advance the prerogatives of law enforcement and carceral systems. Tactics include predictive policing, data-sharing between schools and law enforcement, gang databases, youth risk assessments, and behavioral threat assessments. Youth data criminalization is a larger phenomenon that includes both school surveillance and data-driven criminalization that happens outside the education context.¹⁰ However, schools function as a critical nexus in the broader expansion of police and carceral surveillance.¹¹ Both issues are powerful examples of the New Jim Code and the role of technology in perpetuating structural racism and social inequality.



The Impact of Data Criminalization and School Surveillance Technologies

The following overview of six critical insights on the impact of data criminalization and school surveillance technologies on education equity provides a deeper examination of some of the harms that these methods cause students, families, and communities.

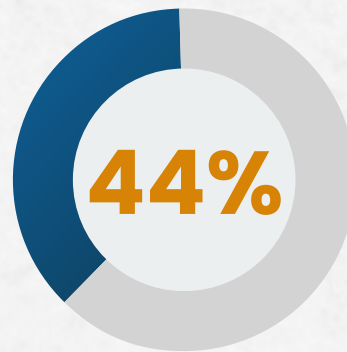
#1 | Law enforcement agencies routinely collaborate with school districts to implement new technologies that are used to surveil, discipline, and criminalize students from historically marginalized communities, effectively reinventing the school-to-prison pipeline.

School districts nationwide are adopting controversial police surveillance technologies that systematically abuse the civil rights and liberties of marginalized youth.¹² These technologies are the latest chapter in the longstanding school pushout crisis, also referred to as the “school-to-prison pipeline.”¹³ School districts use a wide variety of technologies, including facial recognition, social media surveillance, predictive policing weapons detection, automated license plate readers, student device monitoring, automated vape detection, and sharing student data with law enforcement, to monitor a broad range of student activities, behaviors, and speech.¹⁴

A 2023 national survey of educators conducted by the Center on Democracy and Technology found that:

- 88 percent of teachers reported that their school surveils students’ online activity.
- 38 percent of teachers reported that their school shares sensitive student data with law enforcement.
- 36 percent reported that their school uses predictive analytics to identify children who might commit future criminal behavior.
- 36 percent reported that their school tracks students’ physical location through their phones and other digital devices.
- 37 percent reported that their school monitors students’ personal social media accounts.
- 33 percent reported that their school uses facial recognition to regulate access to schools.¹⁵

Separately, researchers found that 44 percent of teachers indicated that they personally knew of students who were contacted by police because of student device monitoring.¹⁶



"44 percent of teachers indicated that they personally knew of students who were contacted by police because of student device monitoring."

These numbers are corroborated by federal data, which shows a rapid growth in the use of surveillance technologies across K-12 campuses. According to the National Center for Education Statistics at the U.S. Department of Education, the number of schools using surveillance cameras increased from 80.6 percent to 91.1 percent between 2015 and 2019.¹⁷ The number of schools using anonymous threat reporting systems increased from 43.9 percent to 65.7 percent over the same period.¹⁸

The growing use of school surveillance technologies could help explain how approximately 61,900 students were referred to law enforcement, and 8,900 were arrested in K-12 schools in the 2020–2021 school year,¹⁹ even though nearly 93 percent of schools were using either all-virtual or hybrid instruction.²⁰

#2 | School surveillance technologies are not race-neutral alternatives to traditional law enforcement.

Proponents of school surveillance technologies argue that these tools enable school leaders to proactively identify and intervene against potential threats to school safety.²¹ However, there is little to no evidence that these technologies improve student wellness or school safety.²² On the contrary, evidence indicates that they are detrimental to learning, health, and safety outcomes for students.²³ A 2022 study in the *Journal of Criminal Justice* found that students attending “high surveillance” schools had lower test scores, were less likely to attend college, and more likely to face exclusionary discipline—outcomes that had a disproportionate impact on Black students.²⁴

Schools and other institutions that serve youth often turn to data-driven technologies as safety solutions under the false assumption that these tools are effective and free from human bias. While data-driven technologies are often portrayed this way, extensive research demonstrates that policing technologies perpetuate demographic bias and structural inequality.²⁵ A coalition of youth justice and civil rights organizations recently submitted a letter to the U.S. Department of Justice outlining the civil rights and data privacy abuses affiliated with the use of a predictive policing program used in a Florida public school system.²⁶

These misconceptions are often rooted in techno-solutionist ideas.²⁷ This term refers to the widely held belief that technologies are politically neutral tools that can, and should, be used to solve complex social problems.²⁸ In reality, technologies reflect the social contexts in which they are deployed and are capable of harm, including civil and human rights abuses.²⁹

#3 | Very little federal or state guidance on AI specifically addresses school surveillance, data criminalization, and education equity.

AI and other data-driven school surveillance technologies are often implemented without public notice, student consent, or independent testing to determine if the technology is scientifically valid or evidence-informed.³⁰ As of November 2023, only Oregon and California have issued comprehensive guidance on the role of AI in public education, while only eleven more states plan to develop guidance in the next year.³¹ Neither Oregon nor California mention student discipline, school surveillance, or data-sharing with law enforcement in their guidance.

While the federal government has issued non-binding guidance to schools on the use of AI in the classroom, it fails to address the growing use of AI-driven surveillance technologies in student discipline and school policing.³²

#4 | School surveillance technologies are often inaccurate, deceptive, and scientifically flawed.

In the absence of comprehensive state and federal guidance, technologies that have the potential to harm students have spread across public schools.

Tech vendors have made misleading claims about the capabilities of their technologies. For example, some claim that their technologies can accurately measure a student’s mood or emotional state.³³ Others boast the ability to accurately identify students at risk of dropping out.³⁴ Many claim to be able to prevent or respond to school shootings, including through the use of armed classroom drones.³⁵ While the technical limitations of existing AI models prevent



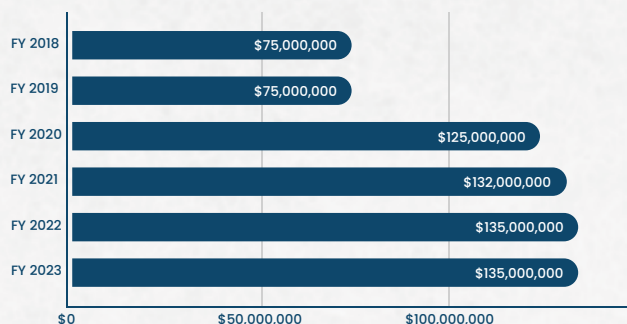
them from achieving many of these safety-related outcomes,³⁶ many schools only learn about those limitations after they purchase them.³⁷ As a result, a growing number of school districts are abandoning costly technologies after discovering the systems were ineffective or scientifically invalid.³⁸ Utica City Schools District in upstate New York is just one district that has abandoned the use of automated weapons detection technology after experiencing how poorly it performed in real-world settings.³⁹

Other schools have been forced to abandon surveillance technologies because they lack legal compliance. Federal agencies have taken enforcement action against EdTech vendors for allegedly engaging in unfair and deceptive business practices related to their handling of student data in violation of the Children Online Privacy Protection Act.⁴⁰

#5 | The federal government plays a central role in funding school policing and surveillance technologies.

The proliferation of policing technologies in schools is a direct consequence of federal funding strategies that conflate surveillance with safety.⁴¹ Federal legislation, including the American Rescue Plan Act and the Bipartisan Safer Communities Act, offered increased resources to schools and police departments to acquire, develop, and advance school surveillance and youth data criminalization.⁴² Research shows that 2023 and 2024 were the highest levels of funding for the STOP School Violence Act Program, which is a Department of Justice grant program used by school districts and law enforcement to procure and implement controversial school surveillance technologies and youth data criminalization practices, including predictive policing.⁴³

STOP School Violence Act Grant Program Enacted Budget (2018–2023)



Source: United States Department of Justice
“Budget and Performance”

#6 | School Surveillance and Data Criminalization Harms Young People.

School surveillance and youth data criminalization introduce a range of harms to youth and young adults from historically marginalized communities, including:



EXPANDING SCHOOL PUSHOUT AND CRIMINALIZATION

School surveillance technologies offer schools and law enforcement new tools for student discipline and punishment and places students at greater risk of suspensions, expulsions, and school-based arrests.⁴⁴ In some instances, students have been coerced into acting as “criminal intelligence” sources by school-based law enforcement.⁴⁵ In other cases, students’ digital footprints, including their social media activity, have been used to criminally prosecute them.⁴⁶ Law enforcement has also used students’ health and academic data to enforce involuntary psychiatric detention or initiate court-ordered substance use treatment.⁴⁷ Students’ families have been targeted as a consequence of these practices,⁴⁸ with parents, siblings, and other relatives harassed by law enforcement using tactics like ordinance violations, home visitations, and arrests.⁴⁹



STRENGTHENING THE SCHOOL-TO-DEPORTATION PIPELINE AND FAMILY POLICING SYSTEMS

Immigration authorities and family policing systems also use school surveillance technologies for family separation.⁵⁰ A student in Boston was subject to deportation after school officials shared the student’s social media records with a regional intelligence center connected with Immigration and Customs Enforcement.⁵¹



INTRODUCING NEW FORMS OF BIAS, DISCRIMINATION, AND INJUSTICE

Research shows that AI and other data-driven technologies can introduce and amplify bias and discrimination across a range of contexts,

including public education.⁵² School surveillance technologies are concentrated in low-income schools and used in ways that uniquely disadvantage students of color, students with disabilities, LGBTQIA+ students, and immigrant students.⁵³ School surveillance practices often disrupt or deny access to supportive services for students with disabilities, especially those that have had previous contact with the criminal legal system.⁵⁴ These tools can also be used to police queer and trans youth, outing their identities to parents, schools, or law enforcement entities that are homophobic or otherwise harmful.⁵⁵ In addition, surveillance technologies like facial recognition and predictive policing have consistently demonstrated bias against Black and brown communities.⁵⁶



EXPANDING STATE CENSORSHIP

The expansion of school surveillance is especially alarming as state lawmakers continue to pursue efforts to silence, erase, and censure Black history and LGBTQIA+ identities.⁵⁷ According to Pen America, in the 2022–2023 school year there were 3,362 instances of book bans in public libraries—disproportionately affecting authors who are women of color and/or LGBTQIA+.⁵⁸ Student device monitoring and social media surveillance expands schools' capacity to enforce state censorship laws by limiting students' access to digital content that affirms their identities.⁵⁹ For example, an Iowa school district recently "asked" ChatGPT which books to ban, including Toni Morrison's *Beloved*.⁶⁰



UNDERMINING STUDENT WELLNESS AND SAFETY

Researchers have found that the presence of metal detectors and cameras can heighten students' fear for their safety at school while evoking perceptions that they are potential perpetrators who deserve to be surveilled.⁶¹ The National Association of School Psychologists cautions schools against the use of extreme school security measures, citing the impact of surveillance on student wellness and safety.⁶² These insights fit within the larger research

literature, which finds that young people's exposure to law enforcement leads to heightened emotional distress, trauma, and post-traumatic stress.⁶³ Young people themselves have expressed serious concerns about the use of these technologies and their impact on wellness and safety.⁶⁴



NEGATIVELY IMPACTING ACADEMIC SUCCESS

A 2022 study on school surveillance found that "high surveillance schools" had higher rates of suspension, lower math scores, and lower rates of college attendance, even after controlling for variations in school demographic characteristics.⁶⁵



ERODING STUDENT PRIVACY AND TRUST AND SCHOOL SAFETY

Federal law protects the unauthorized disclosure of student records to third parties, including law enforcement.⁶⁶ Unfortunately, school surveillance technologies grant law enforcement extensive access to students' lives, including their social media, devices, geolocation, and even biometric data. This exposes the most intimate details of students' lives to the state and third-party commercial vendors in ways that are likely inconsistent with federal law and constitutional rights.⁶⁷ Students and families voice strong opposition to this encroachment, especially families who are Black and/or have students with disabilities.⁶⁸ Students note that the presence of these technologies makes them less willing to seek help from their schools when experiencing mental wellness challenges, an outcome that ultimately makes schools less safe for everyone.⁶⁹

Real-Life Harms: Alabama AI Vape Sensors in Student Bathrooms

According to an investigative report by AL.com, at least three Alabama school districts have installed controversial high-tech vape sensors in school bathrooms and locker rooms.⁷⁰ Two of the school districts spent a combined \$360,826 to install at least 216 HALO sensors across dozens of middle and high schools.⁷¹ These sensors rely on a “dynamic vape detection algorithm” to “automatically learn the environment” to detect both vaping and the “masking” of vape smoke with perfumes and cologne.⁷² If a sensor detects vaping, it automatically generates an alert for school officials who can access cameras placed near student bathrooms to identify suspected students. IPVideo, which created the HALO sensor, claims that their technology can also detect gunshots, marijuana use, “aggressive behavior and bullying,” and even chemical spills.⁷³

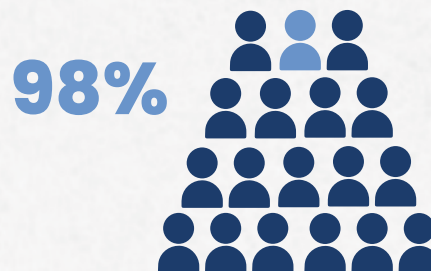
Students who are flagged can be suspended and/or referred to a specialized adult misdemeanor court where they are forced to complete a six-hour online substance use course and up to 24 hours of community service. Students can be fined up to \$50 for each offense. In one county, over 120 children ages 12-17 have been referred to youth vape courts.

This represents one of the starkest examples of how school surveillance technologies bring youth into greater contact with law enforcement and the criminal legal system. These approaches depart from evidence-informed public health strategies that support students while addressing the root causes of substance dependence.⁷⁴ Nevertheless, vape detection technologies are in over 1,500 school districts nationwide.⁷⁵ Such approaches raise serious ethical and legal concerns, especially related to the warrantless, non-consensual search and disclosure of student health records to law enforcement and prosecutors.

Youth Data Criminalization Beyond Schools

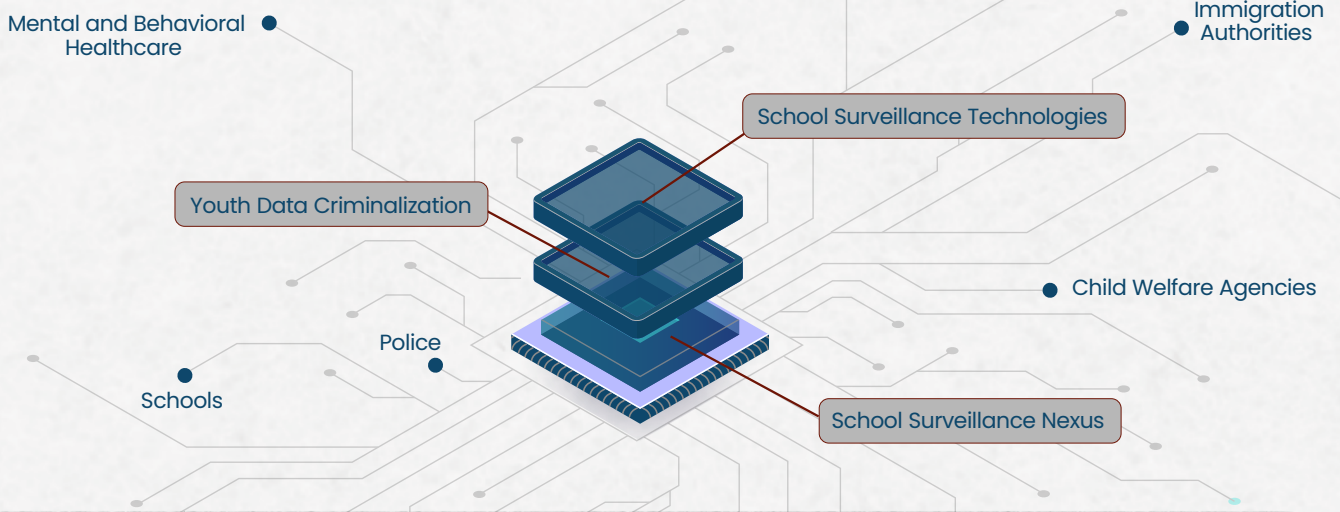
Police surveillance and data criminalization in schools reflect a larger transformation in policing, one that has opened a new chapter in mass incarceration and criminalization.⁷⁶ Data-driven law enforcement strategies saturate communities of color and low-income communities with such intense levels of surveillance that, rather than bringing people to prison, these systems bring prison to people.⁷⁷ Police departments use advanced technologies to surveil and control the most intimate aspects of people’s lives, including physical locations, familial and social networks, spending habits, religious affiliations, reproductive health decisions, political affiliations, and sexual and gender identities.⁷⁸

While these developments impact the public at large, the highest costs of surveillance and data criminalization are imposed on Black, brown, and Indigenous youth. Several major police departments have used a variety of surveillance technologies to build large-scale gang databases largely composed of Black and brown youth and young adults.⁷⁹ These databases are lists of individuals who are suspected to be members of or affiliated with gangs. Law enforcement uses social media monitoring and other surveillance tools to make specious allegations about an individual’s gang affiliation. For example, wearing certain color clothing, being in photos with others who are gang affiliated, or even using particular emojis can get young people placed on a gang database.⁸⁰ In cities like Washington D.C., New York City, and Chicago, these databases are largely composed of Black and Hispanic youth and young adults.⁸¹ An investigative report by the Intercept found that 99 percent of people in Washington, D.C.’s Metropolitan Gang Database were Black or Hispanic and included children as young as newborns.⁸² In 2019, New York City’s gang database was over 98 percent non-white and included the names of over 1,400 individuals under age 18.⁸³



"In 2019, New York City's gang database was over 98% non-white and included the names of over 1,400 individuals under age 18."

School Surveillance to Data Criminalization Nexus



Know Your Youth Digital Rights

New technologies like AI require more expansive thinking about civil and human rights for youth and young adults. There are many existing laws that protect people against the harms of digital technologies, including:

CIVIL RIGHTS AND EQUAL PROTECTION

These rights prohibit the use of data-driven technologies, such as AI, to discriminate against individuals or treat them unfairly based on race, disability status, gender, sexuality, and nationality, among other identities. There are no distinctions between human bias and algorithmic bias recognized under federal law.⁸⁴

- Relevant law includes Title VI, Title VII, the Americans with Disabilities Act, Section 504, the Fair Housing Act, and Section 1557 of the Affordable Care Act.

DATA PRIVACY RIGHTS

Laws that give young people and their parents the right to determine how their personal data is accessed, collected, and/or shared with others, especially in sensitive contexts like education and health care.

- Relevant law includes the Family Education Rights and Privacy Act (FERPA), the Privacy Act of 1974, and the Health Insurance Portability and Accountability Act (HIPAA).

RIGHT TO DUE PROCESS

Due process prevents the government from taking

someone's personal property or depriving them of a legal right without first providing notice and the opportunity to challenge the government's decision. For example, the right to due process would prevent a state from using AI to automatically terminate someone's access to public benefits without providing notice or an opportunity to challenge that decision.

- Relevant law includes the 14th Amendment and *K.W. v. Armstrong* (9th Cir. 2015).

CONSUMER PROTECTION RIGHTS

Consumer rights protect people from unfair, deceptive, or abusive business practices, including from AI and EdTech companies. Private businesses cannot intentionally misrepresent the accuracy, effectiveness, or impact of the technologies that they sell, especially when the product or service is designed for youth and young adults.

- Relevant law includes the Federal Trade Commission Act and the Children's Online Privacy Act.

FOURTH AMENDMENT RIGHTS

The Fourth Amendment is a constitutional right that generally prevents law enforcement from searching, collecting, or sharing an individual's personal data,

devices, and digital accounts without first obtaining a warrant from a judge, unless there is an exigent circumstance.

- *Relevant cases include Carpenter v. United States and Leaders of a Beautiful Struggle v. City of Baltimore.*

FIRST AMENDMENT RIGHTS.

The First Amendment is a constitutional right that largely protects the freedom of speech, protest, and content creation in physical and digital settings. It also protects the “freedom of association,” or the ability to be in a community with people of one’s choosing without interference from the government.

STATE AND LOCAL LAWS AND REGULATIONS

Many of the rights mentioned above exist at the state and local levels. It is possible that those laws may

protect more people or have stronger enforcement provisions than federal laws. In some instances, cities and states have affirmatively banned the use of harmful technologies like facial recognition in schools and/or community settings.

- *Examples Include: Biometric Information Privacy Act (Illinois, 2008), New York State Department of Education Facial Recognition Ban (2023), and Surveillance Technology Ordinance (Santa Cruz, California, 2020).*

Algorithmic technologies, including artificial intelligence, can facilitate unlawful discrimination at every stage of the “AI lifecycle—from pre-design to implementation of the system.”⁸⁵ School districts are legally obligated to ensure that the use of AI in the classroom comports with these laws.

Policy Strategies and Solutions

Federal and state education policymakers must divest from school surveillance systems and technologies and ban their use given the threat to civil rights, privacy rights, and youth wellness, among other ethical considerations. In particular, the Department of Education and the Department of Justice should use their existing legal authority to prohibit the use of federal funding to procure police surveillance technologies in schools. In addition, state lawmakers and education agencies should follow the lead of New York state and ban biometric surveillance, among other detrimental, rights-impacting technologies from use in public schools including facial recognition, predictive policing, drone surveillance, and automated vape detection.⁸⁶

Policymakers and school district leaders should embrace the principles of the White House AI Bill of Rights and incorporate its standards in developing legally binding and enforceable standards for the use of AI technologies in schools.⁸⁷ Every AI policy framework should center principles of racial justice and data justice.⁸⁸

Federal and state policymakers should provide algorithmic auditing and impact assessment services and resources to local school districts to ensure that the procurement of

high-risk technologies and systems are ethical, lawful, scientifically valid, and affirmatively advance education equity. And policymakers at all levels of government should develop strategies that center youth and community voices in the development and implementation of AI guidance and standards in public schools.

Finally, cities and states should ban law enforcement’s use of police surveillance technologies beyond schools, with a particular focus on outlawing those that impact youth and young adults from historically marginalized communities.

Conclusion

Nationwide, communities are actively challenging the proliferation of police surveillance technologies used against marginalized youth.⁸⁹ Many communities have developed innovative, interdisciplinary grassroots campaigns to push their communities to divest from these technologies and invest in youth-led visions of community safety.⁹⁰

Policymakers and local leaders should follow the lead of these communities by divesting from these harmful systems and developing comprehensive legal protections to vindicate the rights of young people in the digital era.

Glossary

TERMS

DEFINITIONS

Aerial Surveillance Systems (aka drones)

Aerial surveillance systems refers to the use of small, unmanned aircraft, otherwise known as drones, equipped with high-resolution video cameras, infrared sensors, license plate readers, or other surveillance capabilities. Drones enable law enforcement to monitor and track the location of targeted individuals, groups, and activities over time. After the tragedy in Uvalde, Texas, a technology firm proposed installing taser-enabled drones in school classrooms as a safety measure.

Algorithmic Bias

Algorithmic bias refers to the use of data-driven systems to disadvantage historically marginalized groups in ways that reinforce white supremacy and other systems of oppression. Algorithmic bias has been observed in a variety of data-driven interventions including pretrial risk assessments and predictive policing. When algorithmic bias infringes upon a legally protected right, it becomes a form of algorithmic discrimination that can be addressed through legal action.

Automated Gunshot Detection

Automated gunshot detection is a police surveillance technology largely used in low-income communities of color⁹¹ that uses acoustic sensors to detect the sound of gunshots and automatically alert law enforcement.⁹² Companies that design these systems argue that the algorithmic models underlying the technology enable their detectors to accurately differentiate between the sound of gunshots and other loud noises.⁹³ Many researchers and advocates challenge these claims and argue that these technologies are incompatible with privacy and human rights.⁹⁴

Behavioral Threat Assessments

Behavioral threat assessments are methods used by schools to proactively identify students who might pose a future risk of harm to themselves or others.⁹⁵ The team that conducts these assessments is typically comprised of educators, mental health providers, and law enforcement.⁹⁶ They make their predictions by relying on surveillance methods, including student device monitoring, student social media monitoring, and anonymous threat reporting systems.⁹⁷ Disability justice and racial justice advocates have highlighted how behavioral threat assessments perpetuate ableist stigmas and racial profiling that increase student contact with law enforcement.⁹⁸ At least nine states have laws mandating the use of behavioral threat assessments.⁹⁹

Facial Recognition

Facial recognition is an AI technology trained on large amounts of biometric data and used to detect and identify individuals based on images of their face.¹⁰⁰ Federal, state, and local law enforcement agencies routinely use facial recognition technologies to support criminal investigations, arrests, and convictions.¹⁰¹ Facial recognition systems have been used by schools to regulate building access and support various law enforcement activities in schools.¹⁰²

Glossary

TERMS

DEFINITIONS

Predictive Policing

Predictive policing refers to the use of data analytics to proactively identify individuals or geographic areas that law enforcement suspects will engage in future unlawful activity. Predictive policing systems are designed to analyze historical criminal legal data and related datasets to identify individuals and/or neighborhoods to target for increased police presence. Researchers have found that predictive policing concentrates police presence in Black and brown neighborhoods, amounting to a digital version of racial profiling.

Student Device Monitoring

Student device monitoring refers to technologies that enable school officials and law enforcement to monitor what students do on devices used at school and home settings. Often framed as supportive services, researchers have found that these systems are used as another point of contact between law enforcement and marginalized youth.

Technosolutionism

Technosolutionism refers to the belief that technologies can solve social problems. In the school safety context, technosolutionism occurs when school leaders turn to surveillance technologies as a response to fears of school violence rather than addressing the underlying social conditions that enable school violence.

Vaping Detection

Vaping detection technologies use sensors to detect particulates associated with vaping. The detectors rely on AI technologies to differentiate between vape particulates and other particles in the air. The detectors are often designed to automatically generate alerts to school officials, who in turn rely on the alerts to support student discipline, including referrals to law enforcement.

Endnotes

- ¹“Big data technologies” refers to technical systems that are capable of processing vast amounts of data in ways that were not previously possible with conventional tools. In the law enforcement context, these technologies include predictive policing and interagency data-sharing that drastically expand the capacity of law enforcement to surveil individuals and communities.
- ²Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity, 2019), pp. 5–6.
- ³Clarence Okoh, “The Dilemma of Black Coding: Assessing Algorithmic Discrimination Legislation in the United States,” *Court Review*, 2023, <https://heinonline.org/HOL/LandingPage?handle=hein.journals/ctrev59&div=8&id=&page=>.
- ⁴Tiera Tanksley “AI Technology Threatens Educational Equity for Marginalized Students,” *The Progressive*, 2024, <https://www.tieratanksley.com/publications>; Neil Bedi and Kathleen McGrory, “Targeted,” *Tampa Bay Times*, 2020, <https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/>; “The Cradle to Prison Algorithm,” Twin Cities Innovation Alliance, <https://www.tciamn.org/cpa-journey>; Dhruv Mehrotra, “ICE Is Grabbing Data From Schools and Abortion Clinics,” *Wired*, April 2023, <https://www.wired.com/story/ice-1509-custom-summons/?redirectURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fice-1509-custom-summons%2F>; “School Surveillance Factsheet,” *The Advancement Project*, June 2023, <https://policefreeschools.org/resources/school-surveillance-fact-sheet/>; Stefanie Coyle and Simon McCormack, “A NY School is Using Face Surveillance on Its Students,” *NYCLU*, January 2020, <https://www.nyclu.org/en/news/ny-school-using-face-surveillance-its-students>.
- ⁵“Blueprint for an AI Bill of Rights,” Office of Science and Technology Policy, The White House, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>; Exec. Order No. 14110, 88 FR 75191 (2023), <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>; “Artificial Intelligence and the Future of Teaching and Learning,” Office of Education Technology, United States Department of Education, May 2023, <https://tech.ed.gov/ai-future-of-teaching-and-learning/>.
- ⁶Tanksley, Mehrotra, Coyle, and McCormack *supra*, note 4.
- ⁷“Hidden Harms: How Student Activity Monitoring Increases Risk of Discipline and Police Contact,” *Center for Democracy and Technology*, November 2022, <https://cdt.org/event/hidden-harms-how-student-activity-monitoring-increases-risk-of-discipline-and-police-contact/>; Clarence Okoh, “AI is supercharging child surveillance and the school-to-prison pipeline,” *The Hill*, November 2023, <https://thehill.com/opinion/technology/4319035-ai-is-supercharging-child-surveillance-and-the-school-to-prison-pipeline/>.
- ⁸“School Surveillance Factsheet,” *The Advancement Project*, June 2023, <https://policefreeschools.org/resources/school-surveillance-fact-sheet/>.
- ⁹“The Cradle to Prison Algorithm,” Twin Cities Innovation Alliance, <https://www.tciamn.org/cpa-journey>; Shannon Dooling, “Citing New Documents, Advocates Call On Boston Public Schools To Stop Sharing Info With ICE,” *WBUR*, January 2020, <https://www.wbur.org/news/2020/01/06/bps-ice-information-sharing-new-documents>; Bedi and McGrory, “Targeted”.
- ¹⁰“From Data Criminalization to Prison Abolition,” *Community Justice Exchange*, 2022, <https://abolishdatacrim.org/en>.
- ¹¹Okoh, “AI is supercharging child surveillance.”
- ¹²Lois Beckett, “Under digital surveillance: how American schools spy on millions of kids,” *The Guardian*, October 2019, <https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle>.
- ¹³“School pushout” refers to the use of punitive school discipline practices to remove students from the classroom and push them into greater contact with the juvenile and criminal legal systems. Such practices include suspensions, expulsions, and school-based arrests. Research indicates that youth subject to exclusionary discipline face an array of other barriers to academic success and economic security that persist into adulthood. “What is School Pushout,” *Dignity in Schools*, <https://dignityinschools.org/resources/dsc-created-fact-sheets/>; Denise C. Gottfredson, Scott Crosse, Zhiqun Tang et. al., “Effects of school resource officers on school crime and responses to school crime,” *Criminology & Public Policy*, https://neighborsvt.org/wp-content/uploads/2020/09/Gottfredson-et-al_2020.pdf; Janet Rosenbaum, “Educational and Criminal Justice Outcomes 12 Years After School Suspension,” *Youth and Society*, vol. 52 (no. 4), January 2018, <https://journals.sagepub.com/doi/full/10.1177/0044118X17752208>.
- ¹⁴“Department of Education Announces the Florida Student Safety Portal,” *Florida Department of Education*, August 2019, <https://www.fldoe.org/newsroom/latest-news/departments-of-education-announces-the-florida-schools-safety-portal.shtml>;

Endnotes

- Mila Koumpilova, "Chicago Public Schools is monitoring students' social media for 'worrisome behavior'," Chalkbeat Chicago, November 2022, <https://chicago.chalkbeat.org/2022/11/17/23465255/chicago-public-schools-social-media-monitoring-safer-schools-together/>; "Schools: Social Media Surveillance," Brennan Center, <https://www.brennancenter.org/issues/protect-liberty-security/social-media/schools-social-media-surveillance>; Kristal Dixon, "Fulton schools to get license plate readers," Axios, September 2022, <https://www.axios.com/local/atlanta/2022/09/26/fulton-schools-to-get-license-plate-readers>; "Which States Require In-School Threat Assessment Teams," Everytown, January 2024, <https://everytownresearch.org/rankings/law/school-threat-assessment-teams/>; "What are Threat Assessment Teams and How Prevalent Are They in Public Schools," National Center for Education Statistics, July 2018, <https://nces.ed.gov/blogs/nces/post/what-are-threat-assessment-teams-and-how-prevalent-are-they-in-public-schools>; "Table 233.50. Percentage of public schools with various safety and security measures: Selected years, 1999–2000 through 2019–20," Digest of Education Statistics, https://nces.ed.gov/programs/digest/d21/tables/dt21_233.50.asp?current=yes; Bedi and McGrory, "Targeted"; "The Cradle to Prison Algorithm," Twin Cities Innovation Alliance, <https://www.tciamn.org/cpa-journey>; Mehrotra, "ICE Is Grabbing Data"; "School Surveillance Factsheet," Advancement Project, January 2023, <https://policefreeschools.org/resources/school-surveillance-fact-sheet/>; Coyle and McCormack, "A NY School; Davey Alba, "Facial Recognition Moves Into a New Front: Schools," The New York Times, February 2020, <https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html>; Elyse Chengery, "Board approves weapon detection systems for all Lee County schools next year," Fox4 Southwest Florida, April 2023, <https://www.fox4now.com/news/local-news/lee-county/board-approves-metal-detectors-for-all-lee-county-schools-next-year>; Georgia Gee, "Un-Alarmed: AI Tries (and Fails) to Detect Weapons in Schools," The Intercept, May 2023, <https://theintercept.com/2023/05/07/ai-gun-weapons-detection-schools-evolv/>.
- ¹⁵ "EdTech Threats to Student Privacy and Equity in the Age of AI," Center for Democracy and Technology, September 2023, pp. 14–15, <https://cdt.org/wp-content/uploads/2023/09/FINAL-Off-Task-Report-Slides.pdf>.
- ¹⁶ Elizabeth Laird and Aaron Spitter, "Hidden Harms: Increased Law Enforcement Interactions," Center for Democracy and Technology, November 2022, <https://cdt.org/insights/brief-hidden-harms-increased-law-enforcement-interactions/>.
- ¹⁷ "Safety and Security Practices at Public Schools," National Center for Education Statistics, May 2022, <https://nces.ed.gov/programs/coe/indicator/a19/school-reported-safety-practices?tid=200>.
- ¹⁸ "Safety and Security Practices," National Center for Education Statistics.
- ¹⁹ "Referrals to Law Enforcement and School-Related Arrests in U.S. Public Schools During the 2020–21 School Year," United States Department of Education Office for Civil Rights, November 2023, https://www2.ed.gov/about/offices/list/ocr/docs/crdc-law-enforcement-school-arrests-snapshot.pdf?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=
- ²⁰ "Student Discipline and School Climate in U.S. Public Schools," United States Department of Education Office for Civil Rights, November 2023, https://www2.ed.gov/about/offices/list/ocr/docs/crdc-discipline-school-climate-report.pdf?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=
- ²¹ "Department of Education Announces the Florida Student Safety Portal," Florida Department of Education, August 2019, <https://www.fldoe.org/newsroom/latest-news/departement-of-education-announces-the-florida-schools-safety-portal.stml>.
- ²² Colin Burke and Cinnamon Bloss, "Social Media Surveillance in Schools: Rethinking Public Health Interventions in the Digital Age," Journal of Medical Internet Research, Vol. 11 (no. 11), November 2020, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7691090/>; John Hopkins University Applied Physics Laboratory, "A Comprehensive Report on School Safety Technology," United States Department of Justice, Office of Justice Programs, October 2016, <https://www.ojp.gov/pdffiles1/nij/grants/250274.pdf>.
- ²³ Odis Johnson and Jason Jabbari, "Infrastructure of social control: A multi-level counterfactual analysis of surveillance and Black education," Journal of Criminal Justice, September 2022, <https://hub.jhu.edu/2022/09/21/school-surveillance-security/>

Endnotes

- ²⁴ Johnson and Jabbari, "Infrastructure of social control."
- ²⁵ Benjamin, *Race After Technology*.
- ²⁶ PASCO Coalition, "Letter to the U.S. Department of Justice," October 2023, <https://www.clasp.org/publications/testimony/comments/letter-pasco-county-sheriff-predictive-policing/>.
- ²⁷ Greta Byrum and Ruha Benjamin, "Disrupting the Gospel of Tech Solutionism to Build Tech Justice," *Stanford Social Innovation Review*, June 2022, https://ssir.org/articles/entry/disrupting_the_gospel_of_tech_solutionism_to_build_tech_justice.
- ²⁸ Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World* (MIT Press, 2019).
- ²⁹ Safiya Noble, *Algorithms of Oppression* (NYU Press, 2018).
- ³⁰ Okoh, "AI is supercharging child surveillance."
- ³¹ Greg Toppo, "AI is Here, but Only California and Oregon Guide Schools on its Use," *The 74 Million*, November 2023, <https://www.the74million.org/article/survey-ai-is-here-but-only-california-and-oregon-guide-schools-on-its-use/>.
- ³² Office of Educational Technology, "Artificial Intelligence and the Future of Teaching and Learning," United States Department of Education, May 2023, <https://tech.ed.gov/ai-future-of-teaching-and-learning/>.
- ³³ Jay Stanley, "Experts Say 'Emotion Recognition' Lacks Scientific Foundation," ACLU, July 2019, <https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific>; Lena Podeletz, "We Have to Talk about Emotional AI and Crime," *AI & Society*; John Cusick and Clarence Okoh, "Why Schools Should Abandon Facial Recognition, not Double Down on It," *Fast Company*, July 2021, <https://www.fastcompany.com/90657769/schools-facial-recognition>.
- ³⁴ Todd Feathers, "Takeaways from Our Investigation into Wisconsin's Racially Inequitable Dropout Algorithm," *The Markup*, April 2023, <https://themarkup.org/the-breakdown/2023/04/27/takeaways-from-our-investigation-into-wisconsins-racially-inequitable-dropout-algorithm>.
- ³⁵ Kari Paul, "After Uvalde shooting, tech companies tout their solutions. But do they work?," *The Guardian*, June 2022, <https://www.theguardian.com/technology/2022/jun/30/us-school-shooting-technology-solution>.
- ³⁶ Georgia Gee, "Unalarmed: AI Tries (and Fails) to Detect Weapons in Schools," *The Intercept*, May 2023, <https://theintercept.com/2023/05/07/ai-gun-weapons-detection-schools-evolv/>.
- ³⁷ Gee, "Unalarmed".
- ³⁸ Ibid. Mark Keierleber, "The Latest School 'Weapons Detection' Tech Can Miss Serious Threats, Experts Say," *The 74 Million*, January 2023, <https://www.the74million.org/article/the-latest-school-weapons-detection-tech-can-miss-serious-threats-experts-say/>.
- ³⁹ Ibid.
- ⁴⁰ "FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts," Federal Trade Commission, May 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising>.
- ⁴¹ Deanie Anyangwe and Clarence Okoh, "The Bipartisan Safer Communities Act: A Dangerous New Chapter in the War on Black Youth," . January 2023, <https://www.clasp.org/publications/report/brief/the-bipartisan-safer-communities-act-a-dangerous-new-chapter-in-the-war-on-black-youth/>.
- ⁴² Anyangwe and Okoh, "The Bipartisan Safer Communities Act".
- ⁴³ "Budget and Performance," United States Department of Justice, <https://www.justice.gov/doj/budget-and-performance>.
- ⁴⁴ Johnson and Jabbari, "Infrastructure of social control".
- ⁴⁵ McGrory and Bedi, "Targeted."
- ⁴⁶ "All Eyes on Us: A Report on Youth Social Media and Surveillance," Center for Court Innovation, July 2020, <https://www.innovatingjustice.org/about/announcements/social-media-surveillance>.
- ⁴⁷ McGrory and Bedi, *supra* note 14.
- ⁴⁸ McGrory and Bedi, *supra* note 14.

Endnotes

- ⁴⁹ McGrory and Bedi, *supra* note 14.
- ⁵⁰ Emma Tynan, "Caught in an Educational Dragnet: How the School-to-Deportation Pipeline Harms Immigrant Youth and Youth of Color," National Immigration Law Center, May 2022 <https://www.nilc.org/2022/05/19/caught-in-an-educational-dragnet-how-the-school-to-deportation-pipeline-harms-immigrant-youth-and-youth-of-color-the-torch/>.
- ⁵¹ Rebecca E.J. Cadenhead, "The State of Surveillance in Boston Schools," The Harvard Crimson, November 2021, <https://www.thecrimson.com/article/2021/11/11/boston-school-surveillance/>.
- ⁵² Benjamin, *Race After Technology*.
- ⁵³ Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, et. al., "Hidden Harms: The Misleading Promise of Student Monitoring Online," Center for Democracy and Technology, August 2022, <https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Report-Final-Accessible.pdf>.
- ⁵⁴ Laird, Grant-Chapman, Venzke, et. al., "Hidden Harms."
- ⁵⁵ Laird, Grant-Chapman, Venzke, et. al., "Hidden Harms."
- ⁵⁶ Aaron Sankin, Dhruv Mehrota, Surya Mattu, et. al., "Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them," The Markup, December 2021, <https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them>.
- ⁵⁷ "Freedom to Learn," African American Policy Forum, <https://www.aapf.org/freedomtolearn/>; "The ACLU is Tracking 508 Anti-LGBT Bills in the United States," ACLU, <https://www.aclu.org/legislative-attacks-on-lgbtq-rights>.
- ⁵⁸ "The Freedom to Write," Pen America, <https://pen.org/report/book-bans-pressure-to-censor/>.
- ⁵⁹ Anne Wen, "How the Rise of School Surveillance Software Affects LGBTQ Students," Youth Today, November 2022, <https://youthtoday.org/2022/11/how-the-rise-of-school-surveillance-software-affects-lgbtq-students/>; James Factora, "Surveillance Programs Are Reportedly Targeting, Outing LGBTQ+ Students," Them, October 2021, <https://www.them.us/story/surveillance-programs-reportedly-targeting-outing-lgbtq-students>; Mark Keierleber, "The risks of student surveillance amid abortion bans and LGBTQ restrictions," The Guardian, September 2022, <https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions>.
- ⁶⁰ Angela Watercutter, "How an Iowa School District Used ChatGPT to Ban Books," Wired, August 2023, <https://www.wired.com/story/chatgpt-ban-books-iowa-schools-sf-496/>.
- ⁶¹ Ronet Bachman, Antonia Randolph, and Bethany Brown, "Predicting Perceptions of Fear at School and Going to and From School for African American and White Students: The Effects of School Security Measures," Youth and Society, May 2010, <https://journals.sagepub.com/doi/10.1177/0044118X10366674>; Sarah Lindstrom Johnson, Jessika Bottiani, Tracy E. Waasdorp, et. al., "Surveillance or Safekeeping? How School Security Officer and Camera Presence Influence Students' Perceptions of Safety, Equity, and Support," Journal of Adolescent Health, December 2018, <https://pubmed.ncbi.nlm.nih.gov/30197197/>.
- ⁶² "Research Summaries: School Security Measures and Their Impact on Students," National Association of School Psychologists, 2018, https://www.nasponline.org/Documents/Research%20and%20Policy/Research%20Center/School_Security_Measures_Impact.pdf.
- ⁶³ Lindsey Webb, Dylan Jackson, Monique Jindal, et. al., "Anticipation of racially motivated police brutality and youth mental health," Journal of Criminal Justice, 2022, <https://www.sciencedirect.com/science/article/abs/pii/S0047235222000873>; Juan Del Toro, Tracey Lloyd, Kim S. Buchanan, et. al., "Criminogenic and Psychological Effects of Police Stops on Adolescent Black and Latino Boys," PNAS, April 2019, <https://www.pnas.org/doi/10.1073/pnas.1808976116>; Juan Del Toro, Dylan B. Jackson, Ming-Te Wang, "The Policing Paradox: Police Stops Predict Youth's School Disengagement Via Elevated Psychological Distress," Developmental Psychology, July 2022, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9465843/>.
- ⁶⁴ Chad Marlow, Emily Greytak, Katie Duarte, et. al., "Digital Dystopia: The Danger of Buying what the Edtech Industry is Selling," ACLU, 2023, https://www.aclu.org/wp-content/uploads/legal-documents/digital_dystopia_report_aclu.pdf.
- ⁶⁵ Jamie Gorosh, "New Report Highlights Lgbtq+ Student Views on School Technology and Privacy," Future of Privacy Forum,

Endnotes

February 2023, <https://fpf.org/blog/new-report-highlights-lgbtq-student-viewson-school-technology-and-privacy/>.

⁶⁶ 20 U.S.C. § 1232g.

⁶⁷ Marlow, Greytak, Duarte, et. al, "Digital Dystopia."

⁶⁸ Elizabeth Laird and Aaron Spitter, "Hidden Harms: Increased Law Enforcement Interactions," Center for Democracy and Technology, November 2022, <https://cdt.org/insights/brief-hidden-harms-increased-law-enforcement-interactions/>.

⁶⁹ Marlow, Greytak, Duarte, et. al, "Digital Dystopia."

⁷⁰ Yurkanin and Tyrens-Fernandes, "Alabama Launches Vape Courts."

⁷¹ Ibid.

⁷² "How Does the HALO Detect Vape?" HALO Smart Sensor, <https://halodetect.com/docs/how-does-the-halo-detect-vape/>.

⁷³ "Halo Vape Sensor Integration with Avigilon Unity Video," Halo Smart Sensor, 2023, <https://assets.avigilon.com/documents/Halo-Sensor-Fact-Sheet-1.pdf>.

⁷⁴ "Vaping and Smoking Detection for Schools and Universities," Halo Smart Sensor, <https://halodetect.com/markets/education/>.

⁷⁵ "What is Halo?" Halo Smart Sensors, <https://halodetect.com/product-info/>.

⁷⁶ Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017); Brian Jefferson, *Digitize and Punish: Racial Criminalization in the Digital Age* (University of Minnesota Press, 2020).

⁷⁷ "#NoDigitalPrisons: Challenging E-Carceration," MediaJustice, <https://mediajustice.org/challengingecarceration/>; Michelle Alexander, "The Newest Jim Crow," The New York Times, November 2018, <https://www.nytimes.com/2018/11/08/opinion/sunday/criminal-justice-reforms-race-technology.html>.

⁷⁸ Ibid. Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017); Brian Jefferson, *Digitize and Punish: Racial Criminalization in the Digital Age* (University of Minnesota Press, 2020).

⁷⁹ K. Babe Howell, "Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing," University of Denver Criminal Law Review, January 2015, <https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1042&context=crimlawrev>; Josmar Trujillo and Alex S. Vitale, "Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing,'" Policing Social Justice Project, 2019, <https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf>.

⁸⁰ Chris Gelardi, "Hacked Emails Give Unfiltered View Into the D.C. Police Gang Database," The Intercept, June 2021, <https://theintercept.com/2021/06/18/dc-police-gang-database-hacked-emails/>.

⁸¹ Gelardi, "Hacked Emails."

⁸² Nick Pinto, "NYPD Added Nearly 2,500 New People to its Gang Database in the Last Year," The Intercept, June 2019, <https://theintercept.com/2019/06/28/nypd-gang-database-additions/#:~:text=The%20database%20is%20growing%2C%20currently,2%2C500%20people%20to%20the%20database>.

⁸³ Pinto, "NYPD Added Nearly 2,500."

⁸⁴ Office of Science and Technology Policy, "Algorithmic Discrimination Protections," The White House, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/>.

⁸⁵ Reva Schwartz, Apostol Vassilev, Kristen Greene, et. al., "NIST Special Publication 1270: Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," National Institute for Standards and Technology, March 2022, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf>.

⁸⁶ "State Education Department Issues Determination on Biometric Identifying Technology in Schools," New York State Department of Education, September 2023, <https://www.nysed.gov/news/2023/state-education-department-issues-determination-biometric-identifying-technology-schools>.

⁸⁷ Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights," The White House, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.

⁸⁸ Clarence Okoh, "From Data Privacy to Data Justice: New technologies including artificial intelligence, raise risks of discrimination and exploitation of students," School Administrator Magazine, February 2024,

Endnotes

<https://www.aasa.org/resources/resource/from-data-privacy-to-data-justice>.

⁸⁹ "P.A.S.C.O. Coalition: People Against the Surveillance of Children and Overpolicing," Southern Poverty Law Center, <https://www.splcenter.org/PASCOcoalition>; "The Cradle to Prison Algorithm," Twin Cities Innovation Alliance, <https://www.tciamn.org/cpa-journey>.

⁹⁰ Coyle and McCormack, "A NY School."

⁹¹ "ShotSpotter is deployed overwhelmingly in Black and Latinx neighborhoods in Chicago," MacArthur Justice Center, <https://endpolicesurveillance.com/burden-on-communities-of-color/>; Todd Feathers, "Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods," Vice, July 2021, <https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-black-neighborhoods>.

⁹² "Gunshot Detection," Electronic Frontier Foundation, <https://sls.eff.org/technologies/gunshot-detection>.

⁹³ "ShotSpotter is deployed overwhelmingly," MacArthur Justice Center; Feathers, "Gunshot-Detecting Tech."

⁹⁴ "ShotSpotter is deployed overwhelmingly," MacArthur Justice Center; Feathers, "Gunshot-Detecting Tech."

⁹⁵ "Behavioral Threat Assessments Harm Students," ACLU-Vermont, April 2023, <https://www.acluvt.org/en/news/behavioral-threat-assessments-harm-students/>; "The Problem with Threat Assessments in Schools," National Disability Rights Network, February 2022, <https://www.ndrn.org/resource/the-problems-with-threat-assessments-in-schools/>.⁹⁵

⁹⁶ "Behavioral Threat Assessments Harm Students," ACLU-Vermont; "The Problem," National Disability Rights Network."

⁹⁷ Ibid. Jazmyne Owens, "Threat Assessments as a School Safety Strategy," New America, December 2021, <https://www.newamerica.org/education-policy/briefs/threat-assessment-systems-as-a-school-discipline-safety-strategy/>.

⁹⁸ Ibid.

⁹⁹ Everytown Research & Policy, "Which states require in-school threat assessment teams?," Everytown, January 2024, <https://everytownresearch.org/rankings/law/school-threat-assessment-teams/>.

¹⁰⁰ Clare Garvie, Alvaro Bedoya and Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition in America," Georgetown Law Center on Privacy & Technology, October 2016, <https://www.perpetuallineup.org>.

¹⁰¹ Ryan Mac, Caroline Haskins, Brianna Sacks, et. al., "Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here," BuzzFeed News, April 2021, <https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table>.

¹⁰² NYCLU, "Letter to the New York State Education Department," NYCLU, January 2020, https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_lockport.pdf.