Executive Summary

Public and private actors are turning to artificial intelligence (AI) and other big data technologies 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.”

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. The New Jim Code carries unique threats to youth and young adults of color, especially in the context of K-12 public schools.

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. 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.
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. This is especially true for young people from historically marginalized communities, including Black, brown, LGBTQIA+, immigrant, low-income, and disabled populations. 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.

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.

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.

**Introduction**

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. However, schools function as a critical nexus in the broader expansion of police and carceral surveillance. 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.

School districts nationwide are adopting controversial police surveillance technologies that systematically abuse the civil rights and liberties of marginalized youth. These technologies are the latest chapter in the longstanding school pushout crisis, also referred to as the “school-to-prison pipeline.” 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.

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.

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. The number of schools using anonymous threat reporting systems increased from 43.9 percent to 65.7 percent over the same period.

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.

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, even though nearly 93 percent of schools were using either all-virtual or hybrid instruction.
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

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

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

#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. 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. 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. 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. In addition, surveillance technologies like facial recognition and predictive policing have consistently demonstrated bias against Black and brown communities.

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. 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+. 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. For example, an Iowa school district recently “asked” ChatGPT which books to ban, including Toni Morrison’s Beloved.

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. 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. 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. Young people themselves have expressed serious concerns about the use of these technologies and their impact on wellness and safety.

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.

ERODING STUDENT PRIVACY AND TRUST AND SCHOOL SAFETY
Federal law protects the unauthorized disclosure of student records to third parties, including law enforcement. 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. Students and families voice strong opposition to this encroachment, especially families who are Black and/or have students with disabilities. 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.
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. 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. 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.

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. 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. In cities like Washington D.C., New York City, and Chicago, these databases are largely composed of Black and Hispanic youth and young adults. 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.

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. Nevertheless, vape detection technologies are in over 1,500 school districts nationwide. 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.

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.
School Surveillance to Data Criminalization Nexus

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.”

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).

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.

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.

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. Every AI policy framework should center principles of racial justice and data justice.

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. 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.

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

<table>
<thead>
<tr>
<th>TERMS</th>
<th>DEFINITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aerial Surveillance Systems (aka drones)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Algorithmic Bias</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Automated Gunshot Detection</strong></td>
<td>Automated gunshot detection is a police surveillance technology largely used in low-income communities of color that uses acoustic sensors to detect the sound of gunshots and automatically alert law enforcement. 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. Many researchers and advocates challenge these claims and argue that these technologies are incompatible with privacy and human rights.</td>
</tr>
<tr>
<td><strong>Behavioral Threat Assessments</strong></td>
<td>Behavioral threat assessments are methods used by schools to proactively identify students who might pose a future risk of harm to themselves or others. The team that conducts these assessments is typically comprised of educators, mental health providers, and law enforcement. They make their predictions by relying on surveillance methods, including student device monitoring, student social media monitoring, and anonymous threat reporting systems. 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. At least nine states have laws mandating the use of behavioral threat assessments.</td>
</tr>
<tr>
<td><strong>Facial Recognition</strong></td>
<td>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. Federal, state, and local law enforcement agencies routinely use facial recognition technologies to support criminal investigations, arrests, and convictions. Facial recognition systems have been used by schools to regulate building access and support various law enforcement activities in schools.</td>
</tr>
<tr>
<td>TERMS</td>
<td>DEFINITIONS</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Predictive Policing</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Student Device Monitoring</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Technosolutionism</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Vaping Detection</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.


6 Tanksley, Mehrotra, Coyle, and McCormack supra, note 4.


11 Okoh, “AI is supercharging child surveillance.


Endnotes


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 2022, 10.2196/22053.

Endnotes

24 Johnson and Jabbari, “Infrastructure of social control.”
25 Benjamin, Race After Technology.
30 Okoh, “AI is supercharging child surveillance.”
37 Gee, “Unalarmed”.
39 Ibid.
ns-personal-information-advertising.
42 Anyangwe and Okoh, “The Bipartisan Safer Communities Act”.
44 Johnson and Jabbari, “Infrastructure of social control”.
45 McGrory and Bedi, “Targeted.”
47 McGrory and Bedi, supra note 14.
48 McGrory and Bedi, supra note 14.
Endnotes

49 McGrory and Bedi, supra note 14.


52 Benjamin, Race After Technology.


54 Laird, Grant-Chapman, Venzke, et. al., “Hidden Harms.”

55 Laird, Grant-Chapman, Venzke, et. al., “Hidden Harms.”


65 Jamie Gorosh, “New Report Highlights LGBTQ+ Student Views on School Technology and Privacy,” Future of Privacy Forum,
Endnotes


66 20 U.S.C. § 1232g.
67 Marlow, Greytak, Duarte, et. al, “Digital Dystopia.”
69 Marlow, Greytak, Duarte, et. al, “Digital Dystopia.”
70 Yurkanin and Tyrens-Fernandes, “Alabama Launches Vape Courts.”
71 Ibid.
81 Gelardi, “Hacked Emails.”
83 Pinto, “NYPD Added Nearly 2,500.”
88 Office of Science and Technology Policy, “Blueprint for an AI Bill of Rights,” The White House, .
89 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

90 Coyle and McCormack, “A NY School.”
93 “ShotSpotter is deployed overwhelmingly,” MacArthur Justice Center; Feathers, “Gunshot-Detecting Tech.”
94 “ShotSpotter is deployed overwhelmingly,” MacArthur Justice Center; Feathers, “Gunshot-Detecting Tech.”
98 Ibid.