WRITTEN STATEMENT OF CLARENCE OKOH  
SENIOR POLICY COUNSEL & JUST TECH FELLOW  
CENTER FOR LAW AND SOCIAL POLICY (CLASP)  

U.S. COMMISSION ON CIVIL RIGHTS PENNSYLVANIA ADVISORY COMMITTEE  

PUBLIC BRIEFINGS ON CIVIL RIGHTS AND THE RISING USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION  

March 25, 2024

Introduction  
Thank you for the opportunity to provide testimony. My name is Clarence Okoh, and I am a civil rights attorney serving as Senior Policy Counsel at the Center for Law and Social Policy (CLASP) and an inaugural member of the Just Tech Fellowship with the Social Science Research Council (SSRC). I was previously a legal fellow at the NAACP Legal Defense Fund and worked in the New York Attorney General’s Civil Rights Bureau focused on issues of race, technology and civil rights. In my work, I collaborate with organizers, researchers, advocates, educators, and youth activists to investigate and challenge the use of emerging technologies to undermine the civil and human rights of youth and young adults of color and their communities.

I am an original member of the PASCO Coalition: People Against the Surveillance of Children and Overpolicing—a coalition of over 30 local, state, and national organizations working together to end the Pasco County Sheriff’s predictive policing program in local schools. Our collective advocacy has resulted in the district suspending its bulk data-sharing of confidential student records of nearly 18,000 schoolchildren with local law enforcement to target, surveil, and harass vulnerable students and their families. We also have successfully prompted federal policymakers to terminate a federal grant that funded local predictive policing activities that had a disparate impact on Black and Hispanic residents. We successfully challenged the Sheriff in court to gain access to open records that were critical to understanding the implications of their activities on local residents. We also successfully pushed the U.S. Department of Justice (DOJ) to investigate the school’s data-sharing practices. This resulted in a settlement agreement announced earlier this month where the DOJ found that the district’s data-sharing practices violated the Americans with Disabilities Act.

I am also a co-founder of the NOTICE Coalition: No Tech Criminalization in Education—a national network of advocates, researchers, and organizers building a movement to end the use of data and technology to surveil, police, or criminalize young people and their communities. Earlier this year, we shared an open letter to the U.S. Department of Education demanding that they ban and divest federal aid to schools that support police surveillance technologies and data criminalization.
Throughout my work, I aim to translate the radical imaginations of youth of color into legal and policy solutions that build just futures for us all.

Today, I will focus my remarks on the growing use of AI-enabled police surveillance technologies deployed in public schools to drastically expand the school-to-prison pipeline and the broader criminalization of Black and brown youth and other marginalized young people. I will describe the urgent need for policymakers to impose a ban on the use of police surveillance technologies in schools and the broader need for comprehensive data privacy legal protections in the United States centered on the needs of youth of color.

**Digital Pushout: AI-Enabled School Surveillance Technologies are Fueling a Civil Rights Crisis in Public Education**

Public and private actors are turning to artificial intelligence (AI) and other big data technologies to engineer futures for structural racism and social inequality in the United States, a phenomenon that the sociologist Ruha Benjamin has termed the “New Jim Code.” Schools routinely procure controversial surveillance technologies from private, third-party vendors without adequately scrutinizing these systems’ technical, legal, or ethical implications. Both the design and use of these technologies often contravene decades of civil and human rights legal standards that protect students of color, students with disabilities, and students who are LGBTQIA+. Police surveillance tech dramatically expands the presence of law enforcement in the lives of marginalized student populations and their families by transforming physical and digital learning environments into sites of censorship, surveillance, and punishment. As advocates like Marika Pfefferkorn have noted, these systems have transformed the school-to-prison pipeline into “the cradle-to-prison algorithm.”

**The Scope of Police Surveillance Tech in Public Schools**

Driven by concerns about school safety, schools have embraced a suite of problematic technologies and data-driven practices, including facial recognition, automated weapons detection, bathroom vape sensors, social media surveillance, automated license plate readers, behavioral threat assessments, police-networked smart cameras, predictive policing, and aerial drone surveillance, among others. A 2023 national survey of educators conducted by the Center on Democracy and Technology found that—

---

38 percent of teachers reported that their school shares sensitive student data with law enforcement,
36 percent reported their school uses predictive analytics to identify children who might commit future criminal behavior,
36 percent reported their school tracks students’ physical location through their phones and other digital devices,
37 percent reported their school monitors students’ personal social media accounts and
33 percent reported their school uses facial recognition to regulate access to schools.4

The survey also found that teachers at Title I schools and special education teachers reported a higher prevalence of many of these controversial technologies in their schools.5

Data from the National Center on Education Statistics (NCES) supports the survey’s findings. NCES data demonstrates a dramatic expansion in various surveillance and school hardening technologies, including a 34 percent increase in schools using anonymous threat reporting and a 70 percent increase in schools’ use of surveillance cameras in recent years.6

Examples of Police Surveillance Tech and Data Criminalization in Public Schools
The drastic expansion of school surveillance and youth data criminalization has led to dystopian outcomes in schools nationwide. For example:


5 Id. at 15.

• In Philadelphia, local leaders are considering deploying a suite of aerial surveillance drones to monitor “high-crime areas” near public schools in addition to expanding automated weapons detection systems and police networked cameras in schools.7

• In Alabama, a local school district is piloting an AI “vaping detection” technology that is placed in middle and high-school bathrooms to identify students who are vaping or using related substances.8 Children detected by the AI system are subject to school-based discipline in addition to an appearance before a local adult misdemeanor court, which imposes probation, fines, fees, and possibly jail time.9 126 students appeared before the vape court in its first year.10

• In Florida, the Pasco County school district shared confidential student records—including histories of childhood abuse, grades, and attendance records—with law enforcement to build a secret predictive policing system to surveil and punish students believed to be “destined for a life of crime.”11 Local law enforcement built a database that included up to 18,000 students and instructed school-based police to surveil schoolchildren and develop actionable criminal intelligence used to push those children and their families out of the community. The Department of Justice recently entered into a settlement agreement with the school district after finding that the district’s data-sharing practices with law enforcement violated the Americans with Disabilities Act.12

• In Minnesota, local policymakers attempted to develop a predictive analytics system to identify students who were allegedly at risk of future contact with the juvenile legal system.13 A proposed data-sharing agreement between local schools and police agencies would have enabled local agencies to collect, share, and use cross-linked identifiable data about children and their families.14

---

9 Id.
10 Id.
14 Id.
In Boston, local school-based police officers shared an estimated 135 student incident reports with the Boston Regional Intelligence Center—an intelligence-sharing hub for local, state, and federal law enforcement agencies, including the Department of Homeland Security. At least one student was detained and subsequently deported due to the school’s data-sharing practices with local law enforcement.

Police Surveillance Tech and Data Criminalization Undermine Student Success and Enable Digital Authoritarianism

School surveillance and youth data criminalization harm youth and young adults from historically marginalized communities by:

- **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. Student device monitoring and social media surveillance expand schools’ capacity to enforce state censorship laws by limiting students’ access to digital content that affirms their identities.

- **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 a more extensive research literature, which finds that young people’s exposure to law enforcement leads to heightened emotional distress, trauma, and post-traumatic stress.20

- **Negatively Impacting Academic Success.** 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 were more likely to face exclusionary discipline—outcomes that had a disproportionate impact on Black students.21

- **Eroding Student Privacy, Trust and School Safety.** Federal law protects the unauthorized disclosure of student records to third parties, including law enforcement.22 School surveillance technologies grant law enforcement extensive access to students' lives, including their social media, devices, geolocation, and even biometric data, exposing the most intimate details of students' lives to state officials and third-party commercial vendors in legally suspect ways.23 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.24

---

Police Surveillance Tech is Legally Suspect & Scientifically Flawed

Many of the technologies embraced by school districts today have historically raised serious concerns about equity, ethics, and scientific validity. For example, school-based policing and “threat assessment” programs make schools less safe for children with disabilities, Black and brown students, and other students from historically marginalized communities.25 The Department of Justice recently entered into a settlement agreement with the Pasco County School District after finding that local threat assessment

---


22 20 U.S.C. § 1232g.


24 Id.

data-sharing practices with law enforcement violated the Americans with Disabilities Act. Beyond threat assessments and data-sharing, researchers have found consistent, significant racial disparities related to predictive policing, risk assessments, and firearm detection technologies—each disadvantage Black and Hispanic communities.

**Disparate Impact Analysis Across the AI Lifecycle**

The disproportionate burden of police surveillance technologies against youth of color, queer and trans youth, and youth with disabilities may constitute unlawful forms of discrimination, including disparate impact and disparate treatment. Demographic disparate impacts in algorithmic technologies are driven by several factors across the algorithmic lifecycle. At the pre-design stage, developers may introduce bias in framing the problems that their AI models are designed to address. At the design stage, developers can build and train AI models by using datasets and selection criteria tainted with “dirty data” sources that contain and reflect historic patterns of racial and social inequality and civil rights abuses. At the deployment stage, bad actors can implement algorithmic systems in a manner that introduces or exacerbates structural social and economic disadvantages for protected classes.

Beyond disparate impact, AI technologies may cause intentional discrimination—especially those that are rooted in explicit historical theories of scientific racism and eugenics. For example, some EdTech vendors market “aggression” detection and “affect” recognition technologies that claim to use artificial intelligence to predict a child’s emotional state based on their facial expressions or “tone” of voice. These methods are rooted in theories of phrenology and physiognomy, which have long been condemned.

---


and discredited by the scientific community because they lack scientific validation and are inseparable from 19th and 20th-century white supremacist ideologies.32

**Barriers to Legal Accountability for AI-Enabled Rights Abuses**

The use of AI and algorithmic technologies for school safety and student discipline directly implicate a range of federal antidiscrimination and privacy protections, including Titles VI and IV of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act, the Americans with Disabilities Act, the Individuals with Disabilities Education Act, Title IX of the Education Amendments of 1972, the Family Educational Rights and Privacy Act, and the Children’s Online Privacy Protection Act. Police surveillance technologies and data criminalization also implicate the First, Fourth, and Fourteenth Amendments of the U.S. Constitution in schools.

Despite these protections, legal researchers and practitioners have observed unique barriers to bringing legal challenges under existing civil and human legal standards. Those challenges include:

- **Causation and the Black Box Dilemma.** The technical inscrutability of AI technologies, often described as the “black box dilemma,” creates an effective bar to private litigants seeking to bring algorithmic discrimination claims.33 Frequently, AI developers are incapable of explaining how their models reach specific recommendations, scores, or outcomes due to the opacity of their systems—even when the outcomes of an AI system result in disparate effects for protected classes. Moreover, AI developers also struggle to determine when the interaction between variables may produce the explicit use of protected characteristics like race, gender, disability status, or close proxies of those protected classes. The black box dilemma is especially concerning when schools turn to algorithmic predictive analytics, risk assessments, threat assessments, and early warning systems that may discriminate against vulnerable students in technically unknowable ways to students, teachers, or parents.

- **Lack of Transparency.** Police surveillance technologies used in schools are often procured and used in schools without notice to parents, students, or the public. For example, in Pasco County, the local Sheriff secured a data-sharing agreement with the local school district granting the agency access to students’ grades, attendance histories, discipline records, and other confidential, FERPA-protected records for almost a decade before public disclosure through local reporting from the Tampa Bay Times.34 Two years before the story broke, the school district and Sheriff’s

---

32 Id.
office successfully applied to the U.S. Department of Justice to hire an intelligence officer who played an integral role in creating the Sheriff’s predictive policing program. There were no public notice, hearings, comment opportunities, or stakeholder engagement related to these practices, even as officers dramatically escalated their enforcement tactics like targeted civil citations, home visitations, involuntary psychiatric detention, and other methods designed to coerce targeted families to either “move or sue.” Pasco County demonstrates how the absence of public notice creates significant barriers to identifying how systems impact individuals and communities—including how AI technologies violate civil and human rights.

- **Inadequate Remedies for the Scale of Algorithmic Harms.** AI and big data systems operate at a large scale, possibly harming students and families in previously impossible ways. Under federal civil rights statutes, existing remedies were not designed to redress discrimination at the scale of AI, creating a rights-remedy gap. Policymakers must urgently close this gap by crafting new legal remedies that enable the courts, school leaders, and others to adequately redress algorithmic discrimination and structural disadvantages that match the scale and scope of harm. Policymakers can embrace approaches rooted in transformative justice and reparations as a starting point for approaching digital justice remedies. Policymakers can also look to tools like algorithmic disgorgement and data purges as new forms of equitable relief for algorithmic discrimination that generate large-scale harms.

**Conclusion**

The expansion of police surveillance technologies and data criminalization comes at an especially perilous moment in our history. State lawmakers, with the support of federal courts, have systematically dismantled a range of fundamental rights protecting the freedoms of people of color, immigrants, women, and queer and trans folks. States have enacted measures to silence and censure discourse on social inequality while gutting guarantees under the Fourteenth Amendment, including reproductive autonomy and affirmative action. As states continue to roll back these freedoms, emerging technologies offer the precise tools needed to effectuate their oppressive aims. Against this backdrop, public education has become an essential terrain to impose these new, terrifying realities.

Policymakers cannot allow public schools to become the testing grounds for authoritarian technologies. While initial federal policy frameworks like the White House AI Bill of Rights were promising, implementation has raised a host of challenges—especially the consistent demand and appropriation of

---

greater investments in policing technologies and the integration of AI into law enforcement practices. Federal, state, and local lawmakers must take immediate steps to enact comprehensive policy solutions that ban and divest from police surveillance technologies in schools, remove legal barriers to challenging algorithmic rights violations, and embrace transformative justice approaches towards AI governance.

Thank you for your time, and I look forward to hearing your questions.