March 18, 2024

Secretary Miguel Cardona
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

Monique Dixon
Deputy Assistant Secretary for Policy
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

Catherine E. Lhamon
Assistant Secretary for Civil Rights
Office for Civil Rights
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

SENT VIA EMAIL

RE: The Department of Education Must Prohibit Public Schools from Using Artificial Intelligence & Police Surveillance Technologies to Abuse the Civil and Human Rights of Marginalized Youth

Dear Secretary Cardona, Assistant Secretary Lhamon and Deputy Assistant Secretary Dixon,

The No Tech Criminalization in Education Coalition (NOTICE) and the 41 undersigned organizations write to express our concerns about the rapid expansion of artificial intelligence (AI) and big data technologies in K-12 public schools and the potential to violate the civil and human rights of students from historically marginalized communities. We are alarmed by the growing use of surveillance technologies to expand police presence in schools and expose students to greater police contact, exclusionary discipline, and school pushout. We view these developments as a dangerous new chapter in the school-to-prison pipeline and mass criminalization of Black, brown, and Indigenous youth and other marginalized young people.[i] Earlier this year, the U.S. Department of Education (ED) released two long-awaited publications, *A Resource on Confronting Racial Discrimination in Student Discipline*[ii] and *Artificial Intelligence and the Future of Teaching and Learning*.[iii] Both documents fell woefully short of the expectations of youth justice and civil rights advocates by failing to meaningfully address the role of data-driven technologies in violating the civil and human rights of youth from marginalized communities, including Black, Brown, and Indigenous youth, youth with disabilities, LGBTQIA+ youth, immigrant youth, and systems-impacted youth.[iv]

Executive Order 14110 requires the Department of Education to develop "resources, policies, and guidance on the use of AI [in schools]" that emphasize safety, responsibility, and civil rights.[v] To that end, we urge the Department of Education to use its existing legal authority to ban federal grantmaking activities that allow schools to purchase or use artificial intelligence and big data technologies to violate students' fundamental rights, including their civil and human rights, data

privacy rights, and other relevant federal legal protections. Further, we urge your agency to embrace the recommendations outlined in this letter, which offers holistic strategies to protect students against technology-enabled rights abuses, including:

- ❖ Banning the use of federal grants to procure or otherwise use police surveillance technologies in public schools;
- ❖ Divesting all discretionary agency appropriations from funding police surveillance technologies in schools;
- ❖ Issuing technical guidance and offering technical assistance to support school districts in conducting and disclosing algorithmic impact assessments and audits to determine scientific validation and legal compliance of AI and big data technologies that implicate students' fundamental rights and/or may disparately harm students due to preexisting biases embedded in training datasets;
- ❖ Studying the prevalence of police surveillance and other high-risk algorithmic technologies in public schools;
- ❖ Prioritizing enforcement actions against algorithmic discrimination alongside other unethical and unlawful uses of AI and other data-driven technologies in public schools; and,
- ❖ Centering the leadership and vision of youth and young adults alongside caregivers, people with disabilities, and other marginalized groups and community-based organizations in AI and data privacy governance.

We welcome the opportunity to engage with your office at your earliest convenience.

I. Growing Use of Artificial Intelligence & Data-driven Technologies by Schools that Impact Student's Civil and Human Rights

In recent years, school districts nationwide have adopted a wide range of controversial AI-enabled and data-driven technologies that are transforming public education. Driven by concerns about school safety, schools have embraced a suite of problematic technologies, including facial recognition, automated weapons detection, social media surveillance, automated license plate readers, behavioral threat assessments, police-networked smart cameras, predictive policing, and aerial drone surveillance, among others.[vi] 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 said their school uses predictive analytics to identify children who might commit future criminal behavior;
- 36 percent said their school tracks students' physical location through their phones and other digital devices;
- 37 percent said their school monitors students' personal social media accounts and
- 33 percent reported their school uses facial recognition to regulate access to schools.[vii]

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

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 30 percent increase in schools' use of surveillance cameras since the 2007-08 school year.[ix]

The drastic expansion of youth data criminalization is radically transforming schools nationwide. For example:

- In Philadelphia, local leaders are considering deploying aerial surveillance drones to monitor "high-crime areas" near public schools and expanding automated weapons detection systems and police networked cameras in schools.[x]

- 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.[xi] Children detected by the AI system are disciplined in school and must appear before a local juvenile court judge who may impose probation, fines, and fees on impacted students.[xii]

- In Florida, a local school district shared confidential student records–including histories of childhood abuse, grades, and attendance records–with local law enforcement officials, enabling them to build a secret predictive policing system to surveil and punish students "destined for a life of crime."[xiii] That law enforcement agency built a database of up to 18,000 students in recent years. School-based police were instructed to surveil and gather "intelligence" on vulnerable children while in school, which could be later used to push those children and their families out of the community.

- In Minnesota, local policymakers attempted to develop a predictive policing system to identify students allegedly at risk of future contact with the juvenile legal system.[xiv] 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.[xv]

- In Boston, local school-based police officers shared an estimated 135 student incident reports with the Boston Regional Intelligence Center–a data and intelligence sharing hub for local, state, and federal law enforcement agencies, including the Department of Homeland Security and Immigration and Customs Enforcement (ICE).[xvi] At least one student was detained and subsequently deported due to the school's data-sharing practices with law enforcement.[xvii]

Schools often procure these technologies from private vendors in the $3.1 billion school surveillance industry–often using federal and state grants.[xviii] Privately owned technologies in

public schools raise many concerns about transparency and accountability. Tech companies can obscure access to critical information by claiming proprietary interests related to the design and use of their technologies. Even when data is made publicly available, communities confront the "black box dilemma" of algorithmic technologies.[xix] Many AI models' lack of transparency and technical inscrutability raises ethical and legal concerns, especially in sensitive contexts such as public education.

II. Youth Data Criminalization Harms Students

The expansion of surveillance technologies in schools has devastating consequences for young people. While many of these technologies are presented as "school safety" solutions that improve student safety and well-being, a growing body of evidence suggests otherwise. For example, researchers have found that students in schools with heightened surveillance tend to face harsher disciplinary decisions and experience worse academic outcomes.[xx] Surveillance technology in schools can lead to increased contact between students and law enforcement[xxi] and exacerbate the school-to-prison pipeline.[xxii] Students who are Black, LGBTQ+, and/or who have disabilities tend to bear the burden of these harms disproportionately.[xxiii]

Evidence also demonstrates that deploying these technologies in school settings can worsen academic and economic outcomes for students of color, increase the outing of queer and trans students, and undermine free expression rights for student protestors and activists.[xxiv] Students have shared that surveillance technologies, such as student device monitoring, can make them less willing to seek support for their mental and behavioral health needs, including substance misuse.[xxv] School surveillance technologies also negatively impact students' families through data-sharing practices with immigration enforcement and child welfare services.[xxvi]

Researchers have also found that militarized school security measures can adversely impact youth health and wellness while eroding their sense of safety in school. For example, researchers have found that the presence of metal detectors and surveillance cameras can heighten students' fear for their safety at school while evoking perceptions that they are potential perpetrators who deserve to be surveilled.[xxvii] The National Association of School Psychologists cautions schools against extreme school security measures, citing the impact of surveillance on student wellness and safety.[xxviii] These insights fit within the more extensive research literature, which finds that young people's exposure to law enforcement leads to heightened emotional distress, trauma, and post-traumatic stress.[xxix] These effects are present within multigenerational contexts as well. For example, researchers have found significant increases in student absenteeism and parental disengagement after ICE raids or similar dragnet police enforcement actions.[xxx] Related research draws connections between racialized patterns of policing and adverse neighborhood-level public health outcomes, including smoking, physical inactivity, poor physical health, and interpersonal violence.[xxxi]

III. School Surveillance Technologies are Scientifically Flawed, Unethical, and Disproportionately Harm Students from Marginalized Communities

Many of the technologies embraced by school districts today have historically raised serious concerns related to equity, ethics, and scientific validity. For example, school-based policing and "threat assessment" programs have been shown to make schools less safe for children of color and those with disabilities.[xxxii] In addition, researchers have found consistent racial disparities related to predictive policing, risk assessments, and firearm detection technologies–each placing disadvantages on Black and Hispanic communities.[xxxiii] Several factors drive these racial disparities. Guidance from the National Institute of Standards and Technology acknowledge that racialized harms occur across the "lifecycle" of algorithmic technologies.[xxxiv] For example, during the pre-deployment and design phase, developers may train their models on "dirty" datasets—sources that contain and reflect historic patterns of racial and social inequality and civil rights abuses.[xxxv] During the deployment phase, developers and end users may implement algorithmic systems in ways that result in bias, discrimination or others forms of demographic disadvantage.[xxxvi]

In the most alarming cases, data-driven technologies are founded on histories of explicit scientific racism. For example, some biometric AI technologies are rooted in theories of scientific racism and eugenics.[xxxvii] 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.[xxxviii] These methods derive from 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.[xxxix] Nonetheless, these pseudo-scientific ideas have regained prominence with the advent of new AI technologies, including those deployed by schools nationwide.

IV. School Districts Lack the Expertise and Resources to Assess AI and Algorithmic Technologies for Civil Rights and Data Privacy Legal Compliance

Many school districts lack the technical expertise to comprehensively evaluate school surveillance technologies before deployment.[xl] Schools rarely, if ever, conduct rigorous assessments of AI and algorithmic technologies to determine scientific validation, legal compliance, privacy protections, or other vital considerations.[xli] Schools often deploy these technologies without notice or informed consent from students, parents/caregivers, or educators.[xlii] Often, schools lack the resources to ensure that student data is protected from cyberattacks and other harmful actors, even though K-12 schools are the most targeted entities for organized cyberattacks.[xliii]

The Biden administration has previously offered guidance on assessing algorithmic technologies for equity, fairness, and legal compliance in other domains.[xliv] That guidance has generally called for private and public entities using AI in sensitive domains to conduct robust, sociotechnical evaluations of algorithmic technologies across the system's lifecycle using various evaluative tools, including audits, impact assessments, and ongoing monitoring.[xlv] In addition, global AI policy frameworks often call for policymakers to create categories of "prohibited technologies" and "prohibited uses," which effectively ban the use of select AI systems and algorithmic technologies that present an impermissible risk of systematically violating fundamental rights.[xlvi]

Few states or school districts have established formal policies to determine how algorithmic and AI technologies are procured, evaluated, or used in schools–tacitly permitting a broad swathe of controversial technologies to be used at will.[xlvii] Similarly, policymakers at all levels of government have failed to articulate how existing civil and human rights legal standards apply in the context of new data-driven technologies, especially in the context of school discipline.

V. Existing Civil Rights Law Protects Against the Use of Discriminatory AI and Related Data-driven Practices

Schools' use of AI and algorithmic technologies directly implicate a range of federal antidiscrimination and privacy protections, including:

- Title VI and Title 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.

These practices also implicate a range of rights protected under the First, Fourth, and Fourteenth Amendments of the United States Constitution. Additionally, the Bipartisan Safer Communities Act and the Every Student Succeeds Act impose obligations on public schools to embrace only school safety services and evidence-informed educational technologies.[xlviii]

These legal provisions provide federal agencies like the Department of Education (ED) a sufficient basis to take decisive action against rights-abusing technologies in public education.

VI. Recommendations

Given the abovementioned challenges, the Department of Education must embrace the following recommendations.

1. ***Ban public schools from using federal grants to purchase or otherwise use police surveillance technologies.*** School districts are already obligated by federal law to refrain from using discriminatory technologies that violate federal civil rights and privacy laws. ED can leverage its existing authority under federal civil rights law to issue guidance and pursue rulemaking that imposes a ban on grantmaking for school surveillance technologies like facial recognition, social media surveillance, and predictive policing.

2. ***Divest all discretionary agency appropriations from funding police surveillance technologies in schools.*** The Department should conduct civil rights and digital privacy

reviews of existing grant programs and suspend all discretionary grantmaking activities that enable rights-impacting technologies and data practices.

3. ***Issue technical guidance and offer technical assistance to support school districts in conducting and disclosing algorithmic impact assessments and audits to determine scientific validation and legal compliance of AI and big data technologies that implicate students' fundamental rights and/or may disparately harm students due to preexisting biases embedded in training datasets;***. School districts lack the resources and expertise to independently assess EdTech products for scientific validation and legal compliance with federal antidiscrimination and privacy law. The Department should develop practical tools that school districts can use to evaluate the civil and human rights impacts of AI and algorithmic technologies. The Department can begin this process by translating existing federal guidance, including NIST Special Publication 1270 and the White House AI Bill of Rights, into user-friendly, plain-language guidance that can be used by local policymakers, school district officials, technology officers, educators, caregivers, and youth.[xlix]

4. ***Study the prevalence of police surveillance and other high-risk algorithmic technologies in public schools***. The Department should begin measuring the prevalence of high-risk AI and algorithmic technologies in schools. For example, the Department can incorporate questions about the use of technology in school discipline as part of its annual Office of Civil Rights data collection process. The Department can also initiate a special survey through the National Center for Education Statistics Digest of Education Statistics focused on the prevalence of these technologies in school security measures.[l] Any study or survey should focus on the impact of these technologies on the learning environment and student wellness, especially for students from marginalized communities. The Department should incorporate routine data collection related to school surveillance and safety infrastructure and report such data annually.

5. ***Prioritize enforcement actions against algorithmic discrimination alongside other unethical and unlawful uses of AI and data-driven technologies in public schools.*** The Department has existing authority under a range of federal antidiscrimination and student privacy laws to investigate and take enforcement actions against school districts that use AI technologies to abuse student rights. Given the rapid proliferation of these systems and the potential scale of algorithmic harms against marginalized student populations, the Department must commit to vindicating students' rights in the digital age by opening investigations, issuing findings, terminating funding, and taking other available enforcement actions, as well as by referring appropriate matters to the U.S. Department of Justice for litigation.

6. ***Center the leadership and vision of youth and young adults alongside caregivers, people with disabilities, other marginalized voices, and community-based organizations in AI and data privacy governance.*** Unfortunately, recent AI policy development in the U.S. has largely excluded the voices, expertise, and leadership of local

communities, grassroots organizations, marginalized groups, people with disabilities, and youth leaders. As the agency continues to retrofit student and family rights protections for the digital age, these voices must be included and positioned to shape policy outcomes. Communities have pursued strategies, including community data advisory boards, roundtables, town halls, public comment opportunities, and related strategies that allow impacted communities to share their insights, concerns, and solutions. The Department should provide guidance that outlines strategies for states and school districts to ensure that students, parents, marginalized groups, people with disabilities, and community voices are integrated into data policy governance.

VII. Conclusion

Several states and localities have demonstrated how policymakers can take decisive action to end the surveillance state in our public schools. New York State made history last year by announcing a statewide ban on using facial recognition technology in schools.[li] New York State joins several localities around the country that have enacted ordinances that have banned or limited the use of facial recognition technologies by law enforcement.[lii]

Students, families, educators, advocates, and lawmakers have continuously raised concerns about the pervasive use of school surveillance technologies, including student device monitoring technologies.[liii] We join their voices in urging the Department to take immediate action to end this dangerous transformation of America's public schools.

Sincerely,
The NOTICE Coalition

ACLU-MN
ACT 4 SA
Advancement Project
Advocating 4 Kids Inc
API Equality-LA
Asian Americans Advancing Justice | AAJC
Aspen Institute: Forum For Community Solutions
Austin Justice Coalition
Autistic Self Advocacy Network
Black Lives Matter Sacramento
Borealis Philanthropy
Center for Law and Social Policy
Communities Transforming Policing Fund
Community Catalyst
Dignity in Schools Campaign

Disability Rights Florida
Education for Liberation MN
Education Justice Alliance
Education Law Center
Education Law Center Pennsylvania
Encode Justice
Encode Justice Florida
Federal School Discipline Coalition
GLSEN
InterReligious Task Force on Central America
Jessica Wright
Juvenile Law Center
NAACP Florida State Conference
NAACP Legal Defense and Educational Fund, Inc.
National Action Network
National Immigration Law Center
National Women's Law Center
PASCO Coalition: People Against the Surveillance of Children and Overpolicing
Pasco Democratic Public Education Caucus
Sayra and Neil Meyerhoff Center for Families, Children and the Courts
Surveillance Resistance Lab
Surveillance Technology Oversight Project
Teachers Unite
The Gault Center
True Colors United
Twin Cities Innovation Alliance
United School Employees of Pasco - Retired

ENDNOTES

[i] Deanie Anyangwe & Clarence Okoh, *The Bipartisan Safer Communities Act: A Dangerous New Chapter in the War on Black Youth*. Center for Law and Social Policy, (August 2023), https://www.clasp.org/publications/report/brief/the-bipartisan-safer-communities-act-a-dangerous-new-chapter-in-the-war-on-black-youth/.

[ii] *Resource on Confronting Racial Discrimination in Student Discipline*, U.S. Department of Education Office for Civil Rights, (May 2023), https://www2.ed.gov/about/offices/list/ocr/docs/tvi-student-discipline-resource-202305.pdf.

[iii] *Artificial Intelligence and the Future of Teaching and Learning*, U.S. Department of Education Office of Educational Technology, (May 2023), https://tech.ed.gov/ai/.

[iv] "Systems-impacted youth" is used here to describe young people who have direct or familial experience with punitive systems including family policing and the juvenile legal system, among others.

[v] 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

[vi] *Department of Education Announces the Florida Student Safety Portal*, Florida Department of Education (August 2019), https://www.fldoe.org/newsroom/latest-news/department-of-education-announces-the-florida-schools-safety-portal.stml; 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 (last accessed August 2023), 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 (September 2023), 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 (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 (2023),https://nces.ed.gov/programs/digest/d21/tables/dt21_233.50.asp?current=yes; Neil Bedi & Kathleen McGrory, *Targeted*, Tampa Bay Times (November 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/; Cradle to Prison Algorithm, Twin Cities Innovation Alliance (last accessed August 2023), 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, #PoliceFreeSchools (June 2023), https://policefreeschools.org/resources/school-surveillance-fact-sheet/; Stefanie Coyle & Simon McCormack, *A NY School is Using Face Surveillance on Its Students*, NYCLU (last accessed August 2023), https://www.nyclu.org/en/news/ny-school-using-face-surveillance-its-students; Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, (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/.

[vii] *EdTech Threats to Student Privacy and Equity in the Age of AI*, Center for Democracy and Technology, pp. 14-15 (October 2023), https://cdt.org/wp-content/uploads/2023/09/FINAL-Off-Task-Report-Slides.pdf.

[viii] *Id*. at 15.

[ix] *Table 233.50. Percentage of public schools with various safety and security measures: Selected years, 1999-2000 through 2019-20*, National Center on Education Statistics, (2021) https://nces.ed.gov/programs/digest/d21/tables/dt21_233.50.asp.
[x] Kristen Graham, *AI powered gun detection will be installed at all of the Philadelphia district's middle schools*, Philadelphia Inquirer (September 2023), https://www.inquirer.com/education/philadelphia-school-district-safety-drones-gun-detection-police-20230830.html.
[xi] Amy Yurkanin & Savannah Tyrens-Fernandes, *Alabama launches vape court for students busted in school*, AL.com (October 2023), https://www.al.com/news/2023/10/alabama-launches-vape-courts-for-students-busted-at-school.html
[xii] *Id*.
[xiii] Neil Bedi & Kathleen McGrory, *Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals*, Tampa Bay Times (November 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/.
[xiv] *The Cradle to Prison Algorithm Journey Page*, Twin Cities Innovation Alliance (last retrieved November 2023), https://www.tciamn.org/cpa-journey.
[xv] *Id*.
[xvi] 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.
[xvii] Officers with the Pasco County Sheriff's Office have expressed that the purpose of the agency's predictive policing program was to "Make their lives so miserable that they would move or sue." *See* Neil Bedi & Kathleen McGrory, *Targeted*, Tampa Bay Times (November 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/.
[xviii] Natasha Singer, *Schools Are Spending Billions on High-Tech Defense for Mass Shootings*, New York Times (June 2022), https://www.nytimes.com/2022/06/26/business/school-safety-technology.html.
[xix] Saurabh Bagchi, *Why We Need to See Inside AI's Black Box*, Scientific American (May 2023), https://www.scientificamerican.com/article/why-we-need-to-see-inside-ais-black-box/.
[xx] Sarah D. Sparks, *'High-Surveillance' Schools Lead to More Suspensions, Lower Achievement*, Education Weekly (April 21, 2021), https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04.
[xxi] Elizabeth Laird & Aaron Spitler, Hidden Harms: Increased Law Enforcement Interactions, Center for Democracy and Technology (November 2022), https://cdt.org/insights/brief-hidden-harms-increased-law-enforcement-interactions/.
[xxii] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, American Civil Liberties Union (2023), https://www.aclu.org/sites/default/files/field_document/digital_dystopia_report_aclu.pdf.
[xxiii] *Id.;* Sparks, *supra* note 19.
[xxiv]Laird, *supra* note 20. https://cdt.org/insights/brief-hidden-harms-increased-law-enforcement-interactions/; Sarah Sparks, *High Surveillance Schools Lead to More Suspensions, Lower Achievement*, Education Week (April 2021), https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04.
[xxv] Elizabeth Laird & Maddy Dwyer, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, Center for Democracy and Technology (September 2023), https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/.
[xxvi] ACLU, *supra* note 21.
[xxvii] https://journals.sagepub.com/doi/10.1177/0044118X10366674; https://pubmed.ncbi.nlm.nih.gov/30197197/
[xxviii] *Research Summaries: School Security Measures and Their Impact on Students*, National Association of School Pshycologists (2018), https://www.nasponline.org/Documents/Research%20and%20Policy/Research%20Center/School_Security_Measures_Impact.pdf

[xxix] *See e.g.*, Lindsey Webb, *Anticipation of racially motivated police brutality and youth mental health*, Journal of Criminal Justice (Dec. 2022), https://www.sciencedirect.com/science/article/abs/pii/S0047235222000873; Juan Del Toro 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 et. al., *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/.

[xxx] Wendy Cervantes, Rebecca Ullrich & Vanessa Meraz, *The Day That ICE Came: How Worksite Raids Are Once Again Harming Children and Families*, Center for Law and Social Policy (July 2020), https://www.clasp.org/publications/report/brief/day-ice-came-how-worksite-raids-are-once-again-harming-children-and/.

[xxxi] Katherine P. Theall, et. al., *Neighborhood Police Encounters, Health and Violence in a Southern City*, Healthline (February 2022), https://www.healthaffairs.org/doi/10.1377/hlthaff.2021.01428.

[xxxii] See Bazelon Center for Mental Health Law, *Replacing School Police with Services that Work* (August 2021), http://www.bazelon.org/wp-content/uploads/2021/08/Replacing-Police-in-Schools-1.pdf; National Disability Rights Network (NDRN), *K-12 Threat Assessment Processes: Civil Rights Impacts* (February 2022), https://www.ndrn.org/wp-content/uploads/2022/02/K-12-Threat-Assessment-Processes-Civil-Rights-Impacts-1.pdf.

[xxxiii] Elizabeth Laird & Maddy Dwyer, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI* at, Center for Democracy and Technology (September 2023), https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/.

[xxxiv] Reva Schwartz et. al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, National Institute for Standards and Technology Special Publication 1270 at 12 (March 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[xxxv] Rashida Richardson, Jason M. Schultz, Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. 15 (2019), https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact- police-data-predictive-policing-systems-and-justice/.

[xxxvi] *See e.g.*, Dell Cameron & Dhruv Mehrotra, *US Justice Department Urged to Investigate Gunshot Detector Purchases*, Wired (September 2023), https://www.wired.com/story/shotspotter-doj-letter-epic/#:~:text=Attorneys%20for%20the%20nonprofit%20Electronic,ShotSpotter%20in%20majority%2Dminority%20neighborhoods.

[xxxvii] Catherine Stinson, *The Dark Past of Algorithms That Associate Appearance and Criminality*, American Scientist (Feb. 2021), https://www.americanscientist.org/article/the-dark-past-of-algorithms-that-associate-appearance-and-criminality; Seth Colaner, *AI Weekly: AI Phrenology is Racist Nonsense, Of Course it Does Not Work*, Venture Beat (June 2020), https://venturebeat.com/business/ai-weekly-ai-phrenology-is-racist-nonsense-so-of-course-it-doesnt-work/.

[xxxviii] John Cusick & Clarence Okoh, *Why Schools Need to Abandon Facial Recognition, Not Double Down On It*, FastCompany (July 2021), https://www.fastcompany.com/90657769/schools-facial-recognition.

[xxxix] *Id.*

[xl] Greg Toppo, *Survey: AI is Here, but Only California and Oregon Guide Schools on its Use*, The 74 Million (Nov. 2023), https://www.the74million.org/article/survey-ai-is-here-but-only-california-and-oregon-guide-schools-on-its-use/?utm_source=pocket_saves.

[xli] *Id*.

[xlii] *See e.g.*, Neil Bedi & Kathleen McGrory, Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals, Tampa Bay Times (November 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/.

[xliii] Mark Keierleber, Schools Are Now the Leading Target for Cyber Gangs as Ransom Payments Encourage Attacks, The 74 Million (August 2023), https://www.the74million.org/article/schools-are-now-the-leading-target-for-cyber-gangs-as-ransom-payments-encourage-attacks/.

[xliv] *See, e.g.*, FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety, The White House (May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-

admini stration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and- safety/; Exec. Order No. 14091, 3 C.F.R. 10825 (2023), https://www.govinfo.gov/content/pkg/FR-2023-02-22/pdf/2023-03779.pdf; Blueprint for an AI Bill of Rights, The White House (October 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/; Reva Schwartz et. al., Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, National Institute of Science and Technology (March 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[xlv] Reva Schwartz et. al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, National Institute for Standards and Technology Special Publication 1270 (March 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf; *Blueprint for an AI Bill of RIghts*, The White House (last accessed August 2023), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[xlvi] Caterini Rodeli, The EU AI Act: How to (truly) protect people on the move, Access Now, (March 2023), https://www.accessnow.org/eu-ai-act-migration/; James Vincent, EU draft legislation will ban AI for mass biometric surveillance and predictive policing, Wired (May 2023), https://www.theverge.com/2023/5/11/23719694/eu-ai-act-draft-approved-prohibitions-surveillance-predictive-policing.

[xlvii] Greg Toppo, Survey: 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/.

[xlviii] *Artificial Intelligence and the Future of Teaching and Learning* at 9, U.S. Department of Education Office of Educational Technology, (May 2023), https://tech.ed.gov/ai/.

[xlix] Reva Schwartz et. al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, National Institute for Standards and Technology Special Publication 1270 (March 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf; *Blueprint for an AI Bill of RIghts*, The White House (last accessed August 2023), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[l] *Table 233.50. Percentage of public schools with various safety and security measures: Selected years, 1999-2000 through 2019-20,* Digest of Education Statistics (2023),https://nces.ed.gov/programs/digest/d21/tables/dt21_233.50.asp?current=yes.

[li] Carolyn Thompson, New York bans facial recognition in schools after report finds risks outweigh potential benefits, Associated Press (September 2023), https://apnews.com/article/facial-recognition-banned-new-york-schools-ddd35e004254d316beabf70453b1a6a2.

lii *Ban Facial Recognition*, Fight for the Future (last accessed February 2023), https://www.banfacialrecognition.com/map/.

[liii] Mark Keierleber, *Exclusive: Dems Urge Federal Action on Student Surveillance Citing Bias Fears*, The 74, https://www.the74million.org/article/exclusive-dems-urge-federal-action-on-student-surveillance-citing-discrimination-fears/; Letter from Center on Democarcy and Technology to the United Staets Department of Education (September 2023), https://cdt.org/insights/letter-to-ed-office-for-civil-rights-on-discriminatory-effects-of-online-monitoring-of-students/.