Testimony of Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

For the U.S. House Committee on Education and Workforce Hearing Entitled
"Building an AI-Ready America"
Wednesday, January 14, 2026

I. Introduction

Chair Walberg, Ranking Member Scott, and Members of the Committee: thank you for the opportunity to testify on the impacts of artificial intelligence on the workforce and in education, especially its implications for the rights, safety, and well-being of workers, students, and their families.

I am the President & CEO of the Center for Democracy & Technology (CDT), a 30-year old nonprofit, nonpartisan organization that works to protect people's civil rights, civil liberties and democratic values in the digital age. CDT works on many issues involving AI, including how AI companies should respect users' privacy and access to information; the use of AI in consequential decisions such as employment, housing, and lending; and the government's use of AI in public services and by law enforcement. Relevant to today's hearing, we have dedicated projects focused on how technology impacts workers' rights in the modern age, and the evolving use of data and technology in K-12 education. We produce original research, advise federal and state policymakers on legislation and regulations, develop resources for impacted communities such as workers and school administrators, and advocate directly to companies to protect their users' rights and interests.

Artificial intelligence is rapidly reshaping how Americans learn, work, and are evaluated. If deployed responsibly, AI has the potential to expand opportunity, improve access to services, and support educators and workers in meaningful ways. But without clear guardrails, transparency, and accountability, AI systems risk reinforcing existing inequalities, eroding civil rights protections, and shifting power further away from students, workers, and families.

Building an AI-ready America means more than accelerating adoption. It means ensuring that AI's use lifts up *all* communities, and helps reduce social divides rather than deepening them. Congress and other policymakers have an important role to play — through passing legislation that protects the American people; by ensuring the proper functioning of the U.S. Department of Education, Equal Employment Opportunity Commission, and other agencies; and by providing the resources that workers, educators, and families need as they navigate the major changes brought about by AI.

II. AI in the Workforce: Risks to Workers' Rights, Safety, and Opportunity

1. AI Across the Employment Lifecycle

Employers are increasingly relying on AI at every stage of the employment cycle, from recruitment and hiring to performance management, promotion, and termination. AI products are used to promote job postings to particular users, screen resumes, assess applicants' skills and personalities, and monitor workers' behavior both inside and outside the workplace. Many of these tools are designed to evaluate job candidates or workers based on criteria derived from historical employment data, including by analyzing the characteristics of previously hired or "top-performing" employees. While vendors often claim these systems improve efficiency and productivity, tools that are not designed to represent the entire workforce can simply reproduce prior trends in employers' hiring and promotion practices instead of evaluating workers' own abilities. We are already seeing examples of these systems being used in ways that discriminate, decrease workers' autonomy, erode job quality, and threaten workers' health and safety.

a. Recruitment, Screening, and Hiring

A growing number of HR recruiting platforms use AI to match job seekers with job postings based on profiles, inferred characteristics, and behavioral data.[1] AI-based content and ad recommendation systems affect the job postings applicants see and are invited to apply to. While these tools may help expedite recruitment if used properly, the systems that identify "matches" can cause qualified candidates to be overlooked.[2]

For applicants who make it past the recruitment stage, AI tools are now widely used to screen resumes and assess applicants' skills. Resume screening tools learn patterns from prior hiring decisions, and thus may prioritize keywords or experiences that have frequently appeared in prior successful applications, regardless of the relevance to the position. These tools can also learn to filter out resumes that make references associated with protected characteristics, or that indicate an employment gap that may be due to childcare or medical leave. For example, a 2024 study found that ChatGPT consistently ranked resumes containing disability-related honors and credentials lower than the same resumes without these credentials.[3] In 2023, the EEOC settled a case against an employer whose resume screening tool was automatically rejecting applicants over 55 or 60 years of age.[4] And, studies conducted by the Harvard Business Review found that

---

[1] Jack Kelly, *Indeed's New AI Tool Enhances Job Matches Between Employers And Candidates*, Indeed (Apr. 11, 2024), https://perma.cc/CF2U-C8QD; Indeed Employer Content Team, *How Indeed Uses AI: Employer Tools and Responsible Use*, Indeed (Dec. 5, 2025), https://perma.cc/2V8X-FEH8; Simran Jaiswal, *How LinkedIn Uses AI for Job Matching & Content Curation,* Linkedin (Aug. 1, 2025), https://perma.cc/ZN27-RBCD.

[2] Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove & Aaron Rieke, *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes,* Proceedings of the ACM on Human-Computer Interaction Volume 3, Issue CSCW, 1-30 (Nov. 2019), https://perma.cc/LP6N-9TRU.

[3] Stefan Milne, *ChatGPT is Biased Against Resumes with Credentials That Imply a Disability — But It Can Improve*, UW News (June 21, 2024), https://perma.cc/3N6Z-WDTW.

[4] Press Release, *iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit,* U.S. Equal Opportunity Commission (Sept. 11, 2023), https://perma.cc/C2VY-FMQW.

certain hiring tools evaluated applicants with four year college degrees as having higher work ethic and self-efficacy compared to those that do not, overlooking workers with alternative backgrounds.[5]

The use of AI that overlooks workers does not stop there. Employers also use AI to analyze video interviews, questionnaires, and gamified assessments that claim to infer applicants' skills or personality traits.[6] These traits are often only loosely, or not at all, related to the job's requirements, or purport to assess complex, amorphous traits such as "appetite for risk" and "emotional stability" based on simple games.[7] Researchers have questioned relying on such subjective and abstract traits, and whether these tools even measure what they claim to.[8] In one such test, a researcher conducted her portion of an English-language AI video assessment *in German*, and yet was still determined to be a 73% personality match for the job (a psychologist working with the company said that the AI "pulled personality traits from her voice").[9] The AI video assessment was not evaluating the content that applicants were saying, but instead was scoring them on arbitrary features.

Notably, many of the workers subject to these inadequate, AI-powered employment decisions are kept in the dark. Job applicants often have no idea that an AI tool is being used to assess their candidacy, let alone how that tool may work – or how they can correct the record with the employer to get the fair consideration they deserve.[10]

Such examples undermine the supposed benefits of AI in these settings, and raise questions about the suitability and legality of tools that are being used to make significant decisions impacting the American workforce. When these tools are poorly or carelessly designed, measure bogus and irrelevant characteristics, or perpetuate an unfair status quo, the harm is felt not just by the workers who are treated unfairly by the system, but by employers who assume that these systems work. Those businesses are now bought into hiring tools that are unfit for purpose and may not identify the best candidates for a job, and they may face legal, financial, and

---

[5] Joseph B. Fuller, Manjari Raman, Eva Sage-Gavin & Kristen Hines, *Hidden Workers: Untapped Talent*, Harvard Business Review (Sept. 2021), https://perma.cc/43FZ-Q24R.
[6] Ly Xīnzhèn M. Zhǎngsūn Brown, Ridhi Shetty & Michelle Richardson, *Report – Algorithm-Driven Hiring Tools: Innovative Recruitment Or Expedited Disability Discrimination?,* Center for Democracy & Technology (Dec. 3, 2020), https://perma.cc/S3CS-ERYX.
[7] Wilneida Negrón, Henry Claypool, Ariana Aboulafia, Dhanaraj Thakur, Matt Scherer & Michal Luria, *Screened Out: The Impact of Digitized Hiring Assessments on Disabled Workers*, Center for Democracy & Technology (Nov. 20, 2024), https://perma.cc/3CFK-FMCG; Aaron Konopasky, *Pre-Employment Tests of Fit Under the Americans with Disabilities Act*, 30 Southern California Review of Law and Social Justice 209, 213-215 (2021), https://perma.cc/8TGF-Q2TC .
[8] *See, e.g.*, Alene Rhea, Kelsey Markey, Lauren D'Arinzo, Hilke Schellmann, Mona Sloane, Paul Squires & Julia Stoyanovich, *Resume Format, LinkedIn URLs and Other Unexpected Influences on AI Personality Prediction in Hiring: Results of an Audit,* AIES '22: Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (July 27, 2022), available at https://perma.cc/3RUW-3YE9.
[9] *Id.*
[10] See, e.g. Aaron Rieke, Urmila Janardan, Mingwei Hsu & Natasha Duarte, *Essential Work: Analyzing the Hiring Technologies of Large Hourly Employers,* Upturn (July 6, 2021), https://perma.cc/ZQ5Q-KNQK ("It is simply impossible to fully assess employers' digital hiring practices from the outside."); Ifeoma Ajunwa, *An Auditing Imperative for Automated Hiring*, 34 Harv. J.L. & Tech. 1 (Mar. 15, 2021), https://perma.cc/KL2N-NGJQ.

reputational harm. This is why it benefits *everyone* to acknowledge the potential risks in certain AI uses and address them through rigorous testing and transparency.

Despite these concerns, adoption of AI-enabled HR tools is accelerating. In a 2024 survey of business leaders, the majority reported plans to use AI in hiring by 2025, and seven in ten said they would let AI systems reject candidates without human oversight, despite the risk of adverse outcomes.[11] This trajectory risks reshaping the labor market around opaque assessments that, without testing and guardrails, can easily treat workers unfairly and break the law — underscoring the importance of this issue for legislators, and the need for a well-functioning Equal Employment Opportunity Commission capable of addressing these developments.

b. Automated Management and Worker Surveillance

Moving to the next step in the worker lifecycle, AI is also increasingly used to manage and monitor workers. Automated systems track and analyze a range of data, including workers' location and movements, productivity, keystrokes, breaks, and perceived sentiments in customer interactions.[12] These data are used in a variety of ways, from making compensation decisions and triggering disciplinary actions to scheduling and tasking on the job.

While these tools are expanding into white-collar workplaces, their impacts are most heavily felt by low-wage and hourly workers, including warehouse workers, home care providers, and gig workers, who already face intense surveillance.[13] While AI systems may support efficiencies in these settings, and enable popular services such as matching customers with drivers and other service providers willing to work, they can also significantly erode job quality and strip workers of autonomy. Factory workers have complained that "it's the automatically enforced pace of work, rather than the physical difficulty of the work itself, that makes the job so grueling. Any slack is perpetually being optimized out of the system, and with it any opportunity to rest or recover."[14] Call center workers have noted that they "now face an environment where everything from the amount of time they spend completing forms to the perceived empathy they express to callers is continuously monitored and evaluated by automated systems, eliminating whatever small sense of control and independence they once had over how they perform their jobs."[15] For over a decade, news reports have highlighted how delivery drivers routinely cut corners on safety procedures to keep up with algorithmically-tracked quotas.[16]

---

[11] Rachel Wells, *65% Of Employers To Use AI To Reject Candidates In 2025,* Forbes (Oct. 28, 2024), https://perma.cc/6NB6-QJMP.
[12] Matt Scherer, *Report – Warning: Bossware May Be Hazardous to Your Health*, Center for Democracy & Technology (July 24, 2021), https://perma.cc/G7MG-LAFS.
[13] Id.; Alexandra Mateescu, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, Data & Society (Nov. 16, 2021), https://perma.cc/3NJ5-4W5J; Elizabeth Anne Watkins, *Face Work: A Human-Centered Investigation into Facial Verification in Gig Work*, Proc. ACM Hum.-Comput. Interact., Vol. 7, No. CSCW1, Article 52, (Apr. 2023), https://perma.cc/2LXP-KEAT.
[14] Matt Scherer, *Report – Warning: Bossware May Be Hazardous To Your Health*, Center for Democracy and Technology (July 24, 2021), at page 10, https://perma.cc/2ELZ-MRME .
[15] Id. at 12.
[16] Esther Kaplan, *The Spy Who Fired Me*, Harper's (Mar. 2015), at 31, 33-34, https://perma.cc/G3UL-4QGG. See also Sam Adler-Bell & Michelle Miller, *The Datafication of Employment: How Surveillance and Capitalism are Shaping Workers' Futures Without Their Knowledge* 13, The Century Foundation (2018), https://perma.cc/KKG5-4U7L ("The devices score

As these examples show, automated tasking, management, and evaluation can unfairly harm workers by penalizing them for taking breaks, pressuring them to perform at an unsafe pace, and stripping workers' agency over their jobs. Without the ability to rest, or by being forced to work faster than they can reasonably handle, workers are at much higher risk of injury and long-term medical conditions,[17] and it can also lead to discrimination against older workers, disabled workers, and workers who are pregnant or breastfeeding, who can perform the job for which they were hired but need to take more breaks or work at a different pace.

As in the case of AI-powered hiring tools, the use of automated management systems is often opaque, with workers knowing they are being monitored, but not knowing the data being collected or the metrics used to analyze and assess them, or how employers may use this information.[18] This lack of transparency places workers in a powerless situation, and prevents them from providing feedback on the accuracy and appropriateness of the systems' guidance — which is against the interests of both workers and managers alike.

2. Policy Interventions

Policymakers at the state and federal level are rightly considering interventions to address the risks when AI systems are used in these high-risk employment contexts. These policy interventions include the following:

- Ensuring that AI may only be used in employment decisions when it is clearly measuring a job applicant's ability to perform essential job functions or evaluating whether a worker is fulfilling essential functions.
- Requiring meaningful transparency that informs workers about the AI tool that is assessing them, including the types of decisions it is used to make, the personal data and attributes it analyzes, how that data is used to make decisions, and how workers may access any available disability accommodations.
- Requiring employers to explain the basis for adverse decisions to workers.
- Mandating pre-deployment and ongoing impact assessments through independent auditors that examine the validity of an AI tool; risks to workers' civil rights, privacy, and safety; and the availability and utility of alternative tools and accommodations.[19]

---

workers against an ideal of productivity that relies on consistent external factors, while the reality is that many work days include varying disruptions. As a result, workers are penalized for external factors over which they have little control and are pushed to make up for them through invisible sacrifices—such as to their health and personal time."); Aimee Picchi, *Amazon Apologizes for Denying That Its Drivers Pee in Bottles*, CBS News (Apr. 5, 2021), https://perma.cc/FF8L-RUZJ.

[17] Ariana Aboulafia, *Somebody's Watching Me: How Tech Tools Can Facilitate Worker Surveillance and Impact Workers with Disabilities*, American Bar Association Human Rights Magazine (July 18, 2025), https://perma.cc/FQP6-2Z8C.

[18] Matt Scherer, *Bossware: CDT and GFI Lead Broad Coalition Warning White House of Risks of Workplace Electronic Surveillance and Automated Management*, Center for Democracy & Technology (June 29. 2023), https://perma.cc/YMY2-EZEE.

[19] Matt Scherer & Ridhi Shetty, *Civil Rights Standards for 21st Century Employment Selection Procedures*, Center for Democracy & Technology (Dec. 5, 2022), https://perma.cc/Z6ZN-SSPG.

Comprehensive definitions of "AI", clear transparency requirements, and strong enforcement provisions are key to effectively protecting workers.[20] For example, New York City's Local Law 144, enacted in 2021, sought to create notice and auditing requirements for the use of AI in employment decisions, but is ineffectual because AI companies have substantial discretion to determine whether they need to comply.[21]

In contrast, several more effective approaches have recently been proposed. For example, the federal No Robot Bosses Act would regulate employers' use of automated decision systems and require specific disclosures to workers, validation, and testing for compliance with civil rights laws.[22] The Colorado AI Act,[23] new California regulations,[24] proposed regulations in Illinois,[25] and similar bills proposed in other states also mandate transparency and testing when AI systems are used in high-risk settings such as employment.[26] Meanwhile, New York's Bossware and Oppressive Technologies (BOT) Act, and the federal Stop Spying Bosses Act, both set out effective interventions for the use of automated management. Additionally, both bills restrict the types of worker data that employers may use and the circumstances in which they may do so.[27]

Research shows that workers strongly support these protections. In a 2025 deliberative poll conducted by CDT, Coworker.org, and Stanford's Deliberative Democracy Lab, workers expressed strong support for greater transparency in employers' surveillance practices, including disclosures about the data used and the purposes for which employers use it.[28]

---

[20] Matt Scherer, *Report – Regulating Robo-Bosses: Surveying the Civil Rights Policy Landscape for Automated Employment Decision Systems*, Center for Democracy & Technology (July 23. 2024), https://perma.cc/XAC8-JACV.

[21] Researchers found that in the first 5 months following LL 144's enactment, out of 391 employers, only 3% provided transparency notices and only 5% provided bias audits, despite evidence suggesting that a far higher percentage of employers use automated hiring tools. Noncompliance is exacerbated because employers self-determine whether their AI tools meet LL 144's disclosure requirements, and employees/job applicants typically lack the relevant information to contest any such a decision. Lucas Wright, Roxana Mika Muenster, Briana Vecchione, Tianyao Qu, Pika Cai, Alan Smith, Comm 2450 Student Investigators, Jacob Metcalf & J. Nathan Matias, *Null Compliance: NYC Local Law 144 and the Challenges of Algorithm Accountability*, In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, pp. 1701-1713 (2024), https://perma.cc/LS9W-DXCC.

[22] No Robot Bosses Act, H.R. 6371, 119th Cong. (2025), https://perma.cc/RG7G-2KKD .

[23] Consumer Protections for Artificial Intelligence, SB24-205, 2024 Leg., Reg. Sess. (Colo. 2024), https://perma.cc/Q3VY-W6HN.

[24] *California Finalizes Regulations to Strengthen Consumers' Privacy*, California Privacy Protection Agency (Sept. 23, 2025), https://perma.cc/5N2J-LPQ4.

[25] Title 56: Labor and Employment Chapter II: Department of Human Rights Part 2520: Procedure of the Department of Human Rights, Illinois Department of Human Rights (last visited Jan. 2026), https://perma.cc/4JQR-4E5D.

[26] Consumer Protections for Artificial Intelligence, SB24-205, 2024 Leg., Reg. Sess. (Colo. 2024), https://perma.cc/Q3VY-W6HN. See also Fostering Artificial Intelligence Responsibility Act, H.77, 194th Leg., Reg. Sess. (Mass. 2025), https://perma.cc/RT95-NHTY; Texas Responsible Artificial Intelligence Governance Act, H.B.149, 2025 Leg., 89(R) Sess. (Tex. 2025), https://perma.cc/HS9G-TSAM.

[27] Bossware and Oppressive Technologies Act, S.7623, 2023 Leg., Reg. Sess. (N.Y. 2023), https://perma.cc/3PLV-9R9Z; Stop Spying Bosses Act, S. 262, 118th Cong. (2023), https://perma.cc/VQ5N-5K96.

[28] Matt Scherer, Wilneida Negrón & Lindsey Schwartz, *What Do Workers Want? A CDT/Coworker Deliberative Poll on Workplace Surveillance and Datafication*, Center for Democracy & Technology (Mar 6. 2025), https://perma.cc/4TYD-LCML.

Participants also support limiting certain types of tracking, including location tracking and productivity monitoring that can harm mental or physical health.[29]

Companies can and should adopt these practices voluntarily. They can also lead by meaningfully incorporating worker voice — allowing applicants to raise concerns regarding the tools used to evaluate them and provide additional information, and consulting employees and worker advocates in the design and evaluation of AI systems.[30]

The Equal Employment Opportunity Commission also has an important role to play guiding employers and workers on best practices, as well as enforcing federal employment laws. After years of examining the issue of technology in employment decisions, the EEOC launched an initiative in 2021 to help employers ensure that their use of AI tools complies with the law.[31] The EEOC and Department of Justice produced technical assistance explaining how employers can prevent disparate impact so that they adhere to the Americans with Disabilities Act.[32] The EEOC followed up with technical assistance regarding Title VII of the Civil Rights Act,[33] and the Department of Labor published guidance for employers to ensure their use of AI in the workplace safeguards employee rights and well-being.[34] The general counsel of the National Labor Relations Board also published guidance cautioning employers against using automated management tools in a manner that interferes with employees' right to engage in protected organizing activities.[35] These documents, which became unavailable on the agencies' websites in 2025, continued those agencies' valuable work advising employers how to avoid illegal and discriminatory hiring and employment practices. Employers need to be responsible for scrutinizing the design and development of the AI they adopt, and ensure that decisions made using AI are only tied to essential job functions. Where employers fail to monitor and address disparate impact risks in their AI tools, robust enforcement is required.

II. AI in Education: Impacts on Students' Privacy, Safety, and Development

1. Expanding Use of AI in Schools

AI use in K–12 education has reached record levels, and the federal government, from the White House's Office of the First Lady and the Office of Science and Technology Policy to the U.S. Department of Education, is dedicating unprecedented resources to accelerating its deployment

[29] *Id.*
[30] Matt Scherer & Ridhi Shetty, *Civil Rights Standards for 21st Century Employment Selection Procedures*, Center for Democracy & Technology (Dec. 5, 2022), https://perma.cc/74HA-PS6Q.
[31] Press Release, EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness,U.S. Equal Opportunity Commission (Oct. 28, 2021), https://perma.cc/T5EY-5JSQ.
[32] Equal Employment Opportunity Commission, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees* (2022), copy available at https://perma.cc/79ZC-37XZ.
[33] Equal Employment Opportunity Commission, *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964* (2023), copy available at https://perma.cc/KU5C-CZ2N.
[34] Department of Labor, *Artificial Intelligence And Worker Well-being: Principles And Best Practices For Developers And Employers* (2024), copy available at https://perma.cc/V6AK-D38P.
[35] National Labor Relations Board, *Memorandum GC 23-02, Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights* (rescinded 2025).

in the classroom. Schools are turning to educational technology (edtech) products that use AI for a range of purposes, from using generative AI to develop curriculum and instructional materials, to facial recognition software to proctor remote exams, to predictive tools that assess students' behavioral risks and potential academic trajectory, to student activity monitoring software that tracks and reports "red flags" from students' online browsing, messages, and documents.

For the past six years, CDT has conducted nationwide polling to ask students, parents and teachers about their first-hand experiences with AI and how they feel about this technology, which informs my testimony today.[36] Both CDT's and others' research shows that the use of AI in the classroom has never been higher — and that this innovation raises significant questions about school readiness, appropriate guardrails and legal protections, and the need for greater transparency in how these tools are developed and used.

CDT's most recent polling shows that a significant majority of teachers and students (85% of teachers and 86% of students) report having used AI during the 2024-25 school year, with half of students reporting that they used AI for school-related reasons.[37] Students are using generative AI to learn more about topics taught in class, for tutoring and feedback, and for college and career advice. At the same time, we see that AI use in the classroom is not without its drawbacks: half of students agreed that using AI in class makes them feel less connected to their teacher, and seven in ten teachers worried that AI weakens important skills that students need to learn.

Our research also revealed significant geographic and income-based divides: parents and students in urban and suburban areas, and those from higher-income households, report substantially greater AI use than their peers in rural or lower-income communities — raising concerns about uneven exposure to both benefits and risks.

Four high-impact uses of AI in schools warrant additional attention and discussion.

a. Interactions between students and chatbots

The use of AI in K-12 schools is not only affecting students' relationships with their teachers, but also their parents and peers. In CDT's survey research about the 2024-25 school year, students reported that they (or a friend of theirs) have had back-and-forth conversations with AI in these ways:

- 42% to get mental health support
- 42% as friend or companion
- 19% to have a romantic relationship
- 42% as a way to escape from real life

[36] See *Original Research on EdTech, Student Privacy, & Civil Rights*, Center for Democracy and Technology (last visited Jan. 2026), https://perma.cc/E4VL-KMTW.
[37] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.

Each of these uses increased among students whose school frequently uses AI. While nearly one-third of students report having personal conversations with AI using school-provided devices or platforms, very few teachers (only one in ten) report receiving training or information on how to respond if they suspect a student's AI use is detrimental to their well-being.

These dynamics raise urgent questions about how the use of AI in schools directly impacts students' emotional development, dependency, and safety — as well as the privacy protections for these tools that can now see so much of our children's digital lives.

b. Deepfake technology and nonconsensual intimate imagery

Deepfakes and nonconsensual intimate imagery (NCII) have emerged as a serious problem in schools, exacerbated by easy access to generative AI tools. Thirty-six percent of students report having heard of a deepfake[38] that depicts someone associated with their school, and this rises to 61% in schools that frequently use AI.[39] Twelve percent of students report having heard of deepfake NCII that depicts someone associated with their school (this rises to 21% in schools that frequently use AI).[40] To be clear, these students are not reporting having seen just any deepfake (such as viral images depicting celebrities online), but deepfake NCII depicting someone within their school community like a student, parent, or teacher.

Despite this prevalence, fewer than a quarter of teachers report that their schools have clear policies for responding to such incidents. Where responses exist, they often focus on discipline rather than prevention, reporting, and victim support, despite the severe and lasting harm this conduct can cause.

c. Use of AI to educate students with disabilities

Licensed special education teachers are increasingly using AI to develop individualized education programs (IEP) and 504 plans. In CDT's survey, 57% reported using AI for this purpose during the 2024-2025 school year, an 18 point increase from the previous school year.[41] The majority of students with an IEP or 504 plan, as well as their parents, agree that it is a good idea to use AI in this way.[42] However, this particular use of AI raises legal concerns, including

[38] Deepfakes are videos, photos, or audio recordings that seem real but have been digitally manipulated – or faked – to make it seem as though a person has said or done something they have not actually done. Deepfakes are created with AI and are incredibly realistic, making it difficult for humans to distinguish between real-life and fake content.
[39] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[40] Sometimes referred to as "deepfake revenge porn" or "synthetic NCII," deepfake NCII are videos, photos, or audio recordings that seem real but have been digitally manipulated – or faked – to show someone in a sexually explicit or intimate manner that they have not actually done. Deepfake NCII is shared without the consent of the person who is depicted and is incredibly realistic.
[41] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[42] *Id.*

compliance with disability rights laws like the Individuals with Disabilities Education Act (IDEA) and student privacy laws like the Family Educational Rights and Privacy Act (FERPA).[43]

As an initial matter, IDEA requires that each eligible student with a disability receive a unique plan that meets their educational needs; however, 15% of licensed special education teachers report that they have used AI to write an IEP plan in full, raising questions about whether the IEP is truly individualized. Second, FERPA prohibits the disclosure of personally identifiable information about students without parental consent, so it is essential that school administrators ensure that the appropriate agreements and privacy guardrails are in place.

Risks can vary depending on whether a teacher is using a purpose-built tool or a general-purpose tool, as well as whether a district has an agreement with the company that provides the AI tool to schools. Additionally, use of these tools also comes with risks of inaccuracy[44] and bias.[45] These all raise questions of legal compliance and could impact the ability of students with disabilities to access quality educational services.

d. Student activity monitoring

Most public schools are now using AI-powered software to monitor students' activity online. Student activity monitoring software gives schools unprecedented glimpses into students' lives, from analyzing students' browsing habits to scanning their messages and documents, to even viewing what students are doing in real-time.

In polling research conducted by CDT, nine out of 10 teachers reported that their schools use student activity monitoring software, including 39% that monitor outside of school hours, and 29% that monitor personal (e.g. non-school-issued) devices.[46] However, the deployment of this technology has outpaced comfort among both parents and students, as only 63% of parents and 57% of students are comfortable with student activity monitoring software.

Typically framed as a tool to help protect students' safety (for example by detecting signs of distress or threatening behavior), teachers and students confirm that these tools are often used for discipline, and can catalyze behavior issues and increase students' interactions with law enforcement.[47] Teachers whose schools use this technology report the following consequences as a result of student activity monitoring:

- 51% know of a student who got in trouble

[43] Ariana Aboulafia, *From Personalized to Programmed: The Use of Generative AI to Develop Individualized Education Programs for Students with Disabilities,* Center for Democracy & Technology (Oct. 28, 2025), https://perma.cc/3DM6-P6BT.
[44] See Ziwei Xu et. al., *Hallucination Is Inevitable: An Innate Limitation of Large Language Models*, arxiv (Feb. 13, 2025), https://perma.cc/GG74-3HPQ.
[45] Norah Rami, *AI Teacher Tools Display Racial Bias When Generating Student Behavior Plans, Study Finds*, Chalkbeat (Aug. 6, 2025), https://perma.cc/GS8Y-FNCY.
[46] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[47] *Id.* at 48.

- 27% know of a student who got in trouble for how they reacted when a teacher, principal, or other adult at the school confronted them about something found through student activity monitoring
- 25% know of a student who was contacted by law enforcement (e.g., a police officer or school resource officer)
- 6% know of a student who was contacted by immigration enforcement (e.g., Immigration and Customs Enforcement)

Prior years of CDT research reveal additional troubling outcomes. In interview-based research CDT conducted in 2023, multiple parents recounted incidents where the police were alerted outside of school hours by the monitoring software, only to conclude students' online activity was permissible.[48] Moreover, CDT's most detailed exploration of this technology, based on the 2021-22 school year, revealed that protected classes of students disproportionately experience harms of this technology.[49]

Student activity monitoring can undermine students' privacy and have chilling effects on their free expression and freedom to learn. Approximately five in ten students who report that their school uses monitoring software agreed with the statement, "I do not share my true thoughts or ideas because I know what I do online is being monitored."[50] This grows to over six in ten students if they have a learning difference or physical disability.[51] In 2022, 29% of LGBTQ+ students reported that they or someone they know were involuntarily outed (i.e. when a student's gender identity or sexual orientation is shared without their consent or approval) due to this technology, and LGBTQ+ students were more likely to report getting in trouble or being contacted by law enforcement than their peers.[52] Despite these risks, only 31% of teachers whose school uses student activity monitoring reported having received guidance about how to use these systems privately and securely.[53]

2. Policy Interventions

There is undoubtedly potential for AI to enhance the delivery of education in ways that improve student outcomes. However, this promise can only be realized if we recognize the novel risks that this technology introduces, and implement meaningful and robust policies and practices that minimize these harms. Potential intervention points include the following:

---

[48] Dhanaraj Thakur & Elizabeth Laird, *Report – Beyond the Screen: Parents' Experiences with Student Activity Monitoring in K-12 Schools*, Center for Democracy & Technology (July 31, 2025), https://perma.cc/8SCH-3UMP.
[49] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke & Hannah Quay-de la Vallee, *Hidden Harms - The Misleading Promise of Monitoring Students Online*, Center for Democracy & Technology (Aug. 2022), https://perma.cc/8DPG-GFH3.
[50] *Id.*
[51] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke & Hannah Quay-de la Vallee, *Research Slide Deck, Hidden Harms: The Misleading Promise of Monitoring Students Online*, Center for Democracy & Technology (Aug. 2022), https://perma.cc/8DPG-GFH3.
[52] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke & Hannah Quay-de la Vallee, *Hidden Harms - The Misleading Promise of Monitoring Students Online*, Center for Democracy & Technology (Aug. 2022), https://perma.cc/8DPG-GFH3.
[53] *Id.*

- Increase transparency of edtech tools that incorporate AI.
- Provide robust AI literacy training, guidance, and information to teachers, school administrators, and students.
- Embed privacy-forward and safety-oriented principles into federal grants and research.
- Restore and maintain resources to strengthen schools' privacy and security protections.
- Encourage the adoption of policies that address deepfake NCII and provide resources to victims.
- Engage parents and community members in decisions about whether and how to use AI in the classroom.
- Ensure compliance with long-standing student privacy and civil rights laws.

a. Increase transparency of edtech tools that incorporate AI

A key area in which schools are adopting AI is through the use of third-party edtech tools, and there are many open questions about how well these systems work, whether they are worth the investment, whether they introduce bias or other harms, and more.[54]

One commonly recommended, broadly endorsed approach to support the responsible use of third-party edtech products is greater public transparency from the developers and designers of these systems. Improved transparency can help school administrators choose systems with the functionality they need, ensure those systems are suited for their contexts, identify potential risks and ways to mitigate them, and push the field at large towards improved development practices and educational outcomes. Recognizing these potential benefits, different edtech industry associations have begun pushing their members to commit to transparency about the use of AI in their products.[55]

However, little guidance is available about what constitutes meaningful transparency in this context. CDT has developed an eight-part rubric, based on best practices in AI governance across sectors, to define what robust and meaningful public transparency looks like.[56] It includes foundational elements like what the product is intended to do, how the company protects student privacy, and whether there are any limitations to how the product should be appropriately used.

Using this rubric, CDT recently evaluated over 100 edtech products that incorporate AI to assess the current state of transparency about these tools.[57] Unfortunately, we found that edtech

[54] Hannah Quay-de la Vallee, *A for Effort, Needs Improvement on Execution: Lessons Learned from Failures of AI EdTech Tools,* Center for Democracy & Technology (Aug. 19, 2025), https://perma.cc/7V5B-NX3K.
[55] EDSAFE AI, *S.A.F.E. Benchmarks* (accessed Oct 2025) https://perma.cc/LM2A-CVEV; Software & Information Industry Association, *SIIA Releases Principles for the Future of AI in Education* (Oct. 2023) https://perma.cc/2UEA-SSGA.
[56] Hannah Quay-de la Vallee, Morgan Badurak & Dhanaraj Thakur, *Opening the Book: A Rubric to Support Effective Transparency for EdTech Products that Incorporate AI*, Center for Democracy & Technology (Nov. 4, 2025), https://perma.cc/28YV-F72W.
[57] *Id.*

companies currently offer little public transparency about their products, particularly related to how they have been tested and evaluated for efficacy and other key performance indicators, and whether the product has been adapted to work well in K-12 schools. This leaves school administrators making high-stakes procurement decisions with little information — and is an area in which clear progress can and should be made.

b. Provide robust AI literacy training, guidance, and information for teachers, school administrators, and students

Efforts to develop AI literacy (the ability to understand, assess, and use AI systems effectively and responsibly) in schools have gained significant momentum, supercharged by policy directives and an influx of funding.[58] However, the education sector has not waited for this training and guidance to use AI — fewer than half of teachers and students report that they have received some training or information on AI use in class, well below the reported use of this technology.[59] When a school provides guidance or information on AI, approximately nine in 10 teachers and students say they found this guidance or information helpful, underscoring the demand for AI literacy.[60]

Moreover, parents, students, and teachers have different priorities when it comes to what AI guidance and training should cover. Teachers are more likely to prioritize training and guidance related to issues of academic integrity, like how to detect if a student used AI inappropriately and how to respond if they suspect a student cheated, whereas parents and students are more interested in receiving guidance about risks related to AI, such as what to do if they encounter issues with AI tools (e.g. bias, incorrect information) and how student privacy is protected.

These disconnects risk leaving teachers, students, and parents unaware of the harms that can stem from AI use, and ill-prepared to handle failures of the technology. It is critical that AI literacy efforts account for the needs and priorities of diverse stakeholders, all of whom seek guidance and information beyond what AI is capable of and how to engineer prompts.

c. Embed privacy-forward and safety-oriented principles into federal grants and research

In July 2025, the Department of Education released guidance on the use of AI in schools, including *Principles for Responsible Use* that were aimed at protecting privacy, civil liberties,

[58] Jocelyn Gecker, *Big Tech is Paying Millions to Train Teachers on AI, in a Push to Bring Chatbots into Classrooms,* Associated Press (Oct. 20, 2025), https://perma.cc/X8CW-3FEB*;* Press Release*, AFT to Launch National Academy for AI Instruction with Microsoft, OpenAI, Anthropic and United Federation of Teachers*, American Federation of Teachers (July 8, 2025), https://perma.cc/E49J-VE9A; Exec. Order No. 14277, 90 Fed. Reg. 17519 (Apr. 23, 2025), https://perma.cc/ZDM2-K8DU.
[59] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[60] *Id.*

and fostering responsible use of AI in the classroom.[61] These principles stated that AI in schools should be educator-led, ethical, accessible, transparent and explainable, and data-protective.

As the White House and the U.S. Department of Education (ED) continue advocating for AI adoption in schools, including the implementation of Executive Order 14277 on Advancing AI Education for American Youth, they should incorporate these *Principles for Responsible Use*, particularly related to their role in administering grant funding and supporting research.[62]

In addition, the Administration and Congress should ensure that AI-related grantmaking protects student privacy and civil liberties. These goals align with guidance issued by ED and the Office of Management and Budget, both of which provide important principles and practices that should be reflected in grantmaking priorities to ensure agencywide alignment and advance responsible AI use. Guidance and related funding criteria can help coherently align priorities across the federal government for school administrators and the edtech providers with which they work, reinforcing a single vision in which innovation is encouraged to ensure privacy-preserving, rights-respecting practices.

d. Restore and maintain resources to strengthen schools' privacy and security protections

Resources are also needed to strengthen schools' privacy and security protections, as the education sector faces growing cyberthreats that can debilitate schools and their communities. In CDT's research, 23% of teachers reported that their school experienced a large-scale data breach during the 2024-2025 school year.[63] Cybersecurity analysts report that the education sector was the most attacked sector globally in 2025, with schools facing over 4000 attacks per week.[64]

Unfortunately, the federal government's push to accelerate the deployment of AI in the classroom is occurring at the same time that the Administration is providing fewer resources to schools to protect student privacy and keep their data secure. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) previously produced valuable recommendations and resources for school districts, but the Administration recently ended its funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provided crucial cybersecurity support to schools and other government agencies.[65] At the same time, the U.S. Department of Education has undergone historic downsizing, including the elimination of the

---

[61] Press Release, *U.S. Department of Education Issues Guidance on Artificial Intelligence Use in Schools, Proposes Additional Supplemental Priority*, U.S. Dep't of Educ. (July 22, 2025), https://perma.cc/DHV6-QGXG.

[62] Kristin Woelfel & Elizabeth Laird, *Letter to U.S. Department of Education Regarding Responsible Integration of AI in K-12 Education*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/F837-T3VR.

[63] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.

[64] Mohammed Khalil, *Data Breaches in Education 2025: Why Schools Are the #1 Cyber Target,* DeepStrike (Aug. 18, 2025), https://perma.cc/7MEU-RYGZ.

[65] Eric Geller, *Federal Cuts Force Many State and Local Governments Out of Cyber Collaboration Group,* Cybersecurity Dive (Oct. 1, 2025), https://perma.cc/WLW5-63U6.

Office of Educational Technology, that affects the federal support upon which school administrators have relied for guidance and best practices related to privacy and security.[66]

Given the connection between increased AI use in schools and data incidents, policymakers and practitioners should dedicate commensurate resources to address the expanded threats that accompany AI use in schools. This includes restoring funding for the MS-ISAC program, continuing to allocate funding to ED's long-standing Privacy Technical Assistance Center, and maintaining sufficient technology expertise and staffing capacity at ED such that their efforts to accelerate AI deployment are commensurate with increased privacy and security risks.[67]

e. Encourage the adoption of policies that address deepfake NCII and provide resources to victims

The current status of school policies and guidance on deepfake nonconsensual intimate imagery (NCII) also leaves much to be desired.[68] Schools and teachers need more robust guidance on issues such as how the school or school district's discipline policy applies to students who share deepfake NCII depicting another student; who to tell within the school or school district if a student receives or views such content; how to protect the privacy of a student who was depicted; and how to communicate with students' families. Currently, only one in ten teachers reports having received information on these foundational topics, which are essential to supporting students if this occurs.[69]

Although addressing NCII requires a long-term, multistakeholder approach, existing resources can bolster schools' efforts to create a learning environment that is free from bullying and sexual harassment. For example, CDT convened a taskforce of diverse stakeholders and advocates to create a Model NCII Policy for K-12 schools as a first step toward filling these gaps, addressing topics like the school's role in circumstances where deepfake NCII has been shared by or of a member of the school community, reporting mechanisms, and supportive measures for those impacted by deepfake NCII.[70] Additionally, the Future of Privacy Forum published another helpful resource in the form of an infographic and deepfakes readiness checklist to help schools better understand and prepare for the risks posed by this conduct.[71]

Because NCII is not a new issue, CDT also created an infographic to connect victims with resources that currently exist and of which schools should avail themselves to prevent, respond to, and support victims. These include those provided by the National Center for Missing and

---

[66] Lauraine Langreo & Arianna Prothero, *The Ed. Dept. Axed Its Office of Ed Tech. What That Means for Schools*, Education Week (Mar. 18, 2025), https://perma.cc/9M4R-RBCX.
[67] Brandi Vesco, *CoSN 2025: Protecting Data Is Protecting Children*, Government Technology (Apr. 18, 2025), https://perma.cc/EW9D-R3QQ.
[68] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[69] *Id.*
[70] Kristin Woelfel, *Model Policy and Infographic: Non-Consensual Intimate Imagery (NCII) for K-12 Schools*, Center for Democracy & Technology (July 9, 2025), https://perma.cc/7W4X-FSTH.
[71] *Deepfakes in School: Risks and Readiness*, Future of Privacy Forum (Mar. 31, 2025), https://perma.cc/CU6B-MMV2.

Exploited Children (NCMEC), Rape Abuse and Incest National Network (RAINN), Cyber Civil Rights Initiative, and the National Center for Victims of Crime.

Congress should encourage the adoption of deepfake NCII policies by schools, building on existing requirements in civil rights laws like Title IX aimed at preventing sexual harassment. These policies are a crucial first step toward maintaing a learning environment free from sexual harassment and bullying, including deepfake NCII.

f. Engage parents and community members in decisions about whether and how to use AI in the classroom

Teachers who use AI for many school-related reasons are more likely to report negative consequences that harm students and undermine trust. For example, 10% of teachers report that an AI system damaged the school's trust with the community, and this number increases to 17% when a teacher uses AI in many ways. Additionally, half of parents and students agree that a teacher who uses AI is not adequately doing their job. Both of these findings underscore the necessity for schools to engage community members in charting their course with AI use, or risk significant backlash.[72]

In the same way that the Office of Management and Budget currently requires that federal agencies "consult and incorporate feedback from end users and the public" on their AI uses,[73] schools should also be required to engage parents and community members in "the design, development, and use of the AI and use such feedback to inform agency decision-making regarding the AI." This would not only hold state and local agencies to the same standard as federal agencies, but would benefit schools and communities.[74]

g. Ensure compliance with long-standing student privacy and civil rights laws

Schools are legally responsible for protecting student privacy and the civil rights of their students, including when deploying AI.[75] Existing student privacy and civil rights laws provide an important foundation to ensure that data and technology practices in schools achieve their intended function without inadvertently violating student privacy or having discriminatory effects. Best practices that schools should adopt include auditing their existing privacy, security, and nondiscrimination policies, practices, and notices to ensure their applicability to newly-adopted tools; making such communications readily available and posted in school

---

[72] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Center for Democracy & Technology (Oct. 8, 2025), https://perma.cc/GT7F-WKS7.
[73] *M-25-21: Memorandum for the Heads of Executive Departments and Agencies re: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, Office of Management and Budget, Apr. 3, 2025), https://perma.cc/EC5R-L9M5.
[74] Elizabeth Laird & Hugh Grant-Chapman, *Report – Sharing Student Data Across Public Sectors: Importance of Community Engagement to Support Responsible and Equitable Use*, Center for Democracy & Technology (Dec. 2, 2021), https://perma.cc/N6J2-9R3K.
[75] Kristin Woelfel, Ariana Aboulafia, Sydney Brinker & Elizabeth Laird, *Late Applications: Protecting Students' Civil Rights in the Digital Age*, Center for Democracy & Technology (Sept. 2023), https://perma.cc/X5UF-B6YB.

buildings and websites; and designating personnel to be responsible for ensuring compliance with student privacy and civil rights laws.

It is important to note that, while legal requirements have not changed, the Department of Education's capacity to rigorously enforce student privacy and civil rights laws is under threat given its recent significant downsizing. Prior to ED's recent sweeping layoffs, ED already suffered from a significant backlog in FERPA complaints. In fact, ED revised its investigation process during the first Trump Administration based on a report from the Office of the Inspector General finding that, "The Privacy Office is not meeting its statutory obligation to appropriately enforce FERPA and resolve FERPA complaints."[76] ED's Office of Civil Rights is similarly endangered. The recent backlog in civil rights complaints became so severe that ED recently sought to rehire attorneys whom it had laid off.[77] This backlog will only worsen as civil rights complaints increasingly include claims of AI-driven discrimination.

Congress should exercise its oversight role to ensure that ED is meeting its statutory obligations to enforce student privacy laws like FERPA and the Protection of Pupil Rights Amendment, as well as civil rights laws like Titles VI and IX and IDEA.

III. Conclusion

AI is already transforming the institutions that most directly shape Americans' economic futures — our workplaces and our schools. As my testimony has outlined, these changes bring promise, but also real and measurable risks to civil rights, privacy, safety, equality, and human dignity.

In both employment and education, AI systems are increasingly used in high-stakes contexts that affect people's access to economic opportunity, autonomy, and well-being, often with little transparency, limited oversight, and insufficient input from the people most affected by these tools. Building an AI-ready America cannot be reduced to rapid AI adoption or technological enthusiasm. It requires intentional policy choices that ensure AI systems are lawful, fit for purpose, and aligned with our country's longstanding commitments to fairness, accountability, and equal opportunity.

Congress has a critical role to play in setting these guardrails — by ensuring federal agencies are doing their job to serve America's workers, students, and educators, and by advancing targeted legislation that promotes transparency, testing, and meaningful accountability for high-impact AI uses. Congress also must not stand in the way of states seeking to protect their residents from the risks posed by unregulated or inadequately governed AI technologies, such as through the

[76] *Improving the Effectiveness and Efficiency of FERPA Enforcement*, U.S. Dep't. Of Educ. (Dec. 20, 2018), https://perma.cc/RTE7-AE2Q; Benjamin Herold, *Inspector General Blasts Ed. Dept. on FERPA Enforcement*, Education Week (Dec. 11, 2018), https://perma.cc/SB3G-GXVZ.
[77] Cory Turner, *Education Department Recalls Fired Attorneys Amid Civil Rights Complaint Backlog*, National Public Radio (Dec. 10, 2025), https://perma.cc/PS9R-9BMY.

ill-advised "AI moratorium" that Congress has now correctly rejected twice on a strong bipartisan basis.[78]

With the right safeguards in place, AI can empower workers, support teachers, prepare students for future careers, and expand Americans' access to opportunity. Without them, it risks deepening inequality, eroding trust, and leaving people behind.

At the Center for Democracy & Technology, we stand ready to work with this Committee and other policymakers to help ensure that the future of AI in America is broadly innovative, including leading the world in rights-respecting and inclusive AI use that is worthy of the people it is meant to serve.

[78] Eric Null, *CDT Opposes Attempts by Congress to Preempt State AI Laws as Harmful to Consumers and to States*, Center for Democracy and Technology (Nov. 24, 2025), https://perma.cc/94FE-TFWJ.