



OUR TECH, OUR FUTURE:

HOW TO BUILD A TECH INDUSTRY ACCOUNTABLE TO

We the People



A SNAPSHOT FROM THE CENTER FOR CIVIL RIGHTS AND TECHNOLOGY

Acknowledgements

This brief is a continuation of the Snapshot series, an initiative of The Leadership Conference's Center for Civil Rights and Technology (Center) meant to educate and empower civil and human rights organizations looking to engage on technology policy issues.

The Center is a joint project of The Leadership Conference on Civil and Human Rights and The Leadership Conference Education Fund. The Center, launched in September 2023, serves as a hub for advocacy, education, and research at the intersection of civil rights and technology policy. Our experts dive into the most pressing policy issues in three key areas: AI and privacy, voting and platform accountability, and broadband access.

The Center is grateful to the authors who penned essays in this brief. Michael Akinwumi, Charlotte Burrows, Damon Hewitt, Juan Proaño, Maria Town, John C. Yang, and The Leadership Conference's Alejandra Montoya-Boyer — thank you for sharing your insights on how we build a technology industry that is truly accountable to we the people, not politics or profit. The Center would also like to thank staff for their assistance for this Snapshot, including Mariah Wildgen and Madeline Chawla. The Leadership Conference's Christian Andrew Madison was the lead designer, and Mark Ricks designed the web version.

Table of Contents

A Letter from The Leadership Conference's Center for Civil Rights and Technology	5
<i>by Alejandra Montoya-Boyer</i>	
Automated Gatekeepers:	7
Equal Opportunity to Jobs in the Digital Age	
<i>by Charlotte Burrows</i>	
Access and Independence, But at What Cost?	11
<i>by Maria Town</i>	
From the Interstate Highway Era to AI Data Centers:	15
Safeguarding Housing and Health in Infrastructure Placement	
<i>by Michael Akinwumi</i>	
How ICE and Big Tech are Normalizing Mass Surveillance	19
<i>by John C. Yang</i>	
The Digital Frontier:	25
Protecting Latino Civil Rights in the Age of Algorithms	
<i>by Juan Proaño</i>	
Why State Law is Critical to Holding Tech Companies Accountable and Protecting Civil Rights...	29
<i>by Damon Hewitt</i>	
Bots and Ballot Boxes:	35
What Today's Technology Means for Voters and Our Democracy	
<i>by Alejandra Montoya-Boyer</i>	

The opinions of the authors are their own and do not reflect any advocacy or positions of The Leadership Conference's Center for Civil Rights and Technology, unless otherwise noted.

TECH, EMERGING THREATS IN THE AGE OF TECH INDUSTRY DO

ENTER
Rights and Technology



The Leadership
Conference
Education Fund

The Leadership
Conference



the
CENTER
for Civil Rights and Technology



A Letter from The Leadership Conference's Center for Civil Rights and Technology

The role of the tech industry in our society has never been greater. It influences the information, news, and entertainment we consume, how and where we work and live, how we experience, connect, and participate in our communities, and our certainty that we can trust what we read. These companies and the products they create impact how our government interacts with us: they have an outsized influence on how people access opportunities and the promises of our nation — multiracial democracy, stable housing, dignified employment, affordable health care, fair criminal justice systems, and more.

The success of these tech companies — of *any* company — is based on trust, trust from consumers that what they're being sold is safe and fair. But that trust must be earned; it can't be freely given. It's up to these companies to prove they can be trusted by upholding the values we all share.

The decisions companies make now will be remembered by civil rights advocates and the communities we represent.

The authors of the following essays are experts in the field. They are advocates on the frontlines of today's civil rights movement. They hear directly from communities too often pushed to the margins. And they know the steps that companies can take to ensure that their technologies benefit all of us. They know what advocates in local communities can do and can demand of private enterprise.

Tech companies must make sure that no matter the color of our skin, our abilities, or our immigration status, that we all have equal opportunity and equal access — access to jobs, to housing, to health care, to privacy, and to due process. That's the only way that these companies build lasting trust with their consumers and ensure that their technologies work for all of us.

It's critical that these companies realize that civil rights are not a constraint; they're a catalyst for growth.

In solidarity,

Alejandra Montoya-Boyer

*Vice President
The Leadership Conference's Center for Civil Rights and Technology*



OUR TECH, OUR FUTURE: HOW TO BUILD A TECH INDUSTRY ACCOUNTABLE TO *We the People*



Automated Gatekeepers:

Equal Opportunity to Jobs in the Digital Age

Charlotte Burrows

Former Chair

U.S. Equal Employment Opportunity Commission

Over its 250-year history, America has made real — if still incomplete — progress toward realizing its founding principles of equality and justice for all. Federal civil rights laws have been an important part of that progress, helping to expand economic opportunity for all workers. Today, the rush toward rapid adoption of AI in nearly every aspect of our lives is challenging that progress, creating a new frontier in the efforts to safeguard civil rights and ensure equal opportunity. Corporate fear of missing out on AI's benefits has been particularly pronounced in employment, where automated systems now increasingly serve as gatekeepers to myriad job opportunities — influencing hiring, firing, evaluation, pay-setting, and other employment-related decisions. There is a better way. Employers can and must center workers' voices and needs in the adoption of AI in their jobs.

It has been well-documented that because AI makes predictions based on historical data, it can recreate and amplify prior patterns of discrimination in high-stakes decisions affecting workers' futures, all based on training data that encode biases.^{1, 2, 3} These automated decisions disproportionately harm women, religious workers, people of color, older workers, and people with disabilities. Further, new forms of wearable AI technologies can infringe on workers' privacy and potentially violate the Americans with Disabilities Act by collecting information that could reveal a disability. Unchecked, this rush to adopt AI systems threatens to turn back the clock on America's hard-won progress on civil rights.

Current discussions regarding AI are limited almost exclusively to the competition for profits and the race for global AI dominance. Adjusting the focus to put workers and their voices at the center of the conversation would benefit everyone. Workers' insights about the kinds of technology that would improve their work lives, and those that would not, are key to realizing AI's promise of efficiency. Critically, those insights could help tech developers better understand which products will be needed over the long-term. Additionally, incorporating workers' perspectives into their decisions could help employers better evaluate whether AI deployment will lead to measurable internal adoption and related productivity gains and avoid employment discrimination.

Most importantly, allowing working people the dignity and respect of influencing the development of automated tools that will be integral to the workplace is the only way to ensure that AI technology delivers on its promise to improve our lives.



- 1 Pauline T. Kim, "Data-Driven Discrimination at Work," *William and Mary Law Review* (2017), <https://scholarship.lawwm.edu/wmlr/vol58/iss3/4/>.
- 2 Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* (2016), <http://dx.doi.org/10.15779/Z38BG31>.
- 3 Rishi Bommasani, Sarah H. Bana, Kathleen A. Creel, Dan Jurafsky, and Percy Liang, "Algorithmic Monocultures in Hiring," *The Proceedings of the 2026 ACM Conference on Fairness, Accountability, and Transparency* (May 26, 2026), <https://arxiv.org/pdf/2605.27371>.

Employers that choose to adopt AI tools for key employment decisions, such as hiring and recruitment, should begin with a clear picture of the relevant business needs, what tasks the AI might perform, its impact on workers, and how the use of a particular tool can implicate obligations under civil rights laws. Because AI tools must comply with existing federal and state law. Decisions about adoption of employment-related AI should involve the organization's attorneys, who, together with human resources personnel and internal experts who best understand operational needs, can assess how automated tools would be used and whether that use complies with civil rights laws. Although AI vendors are unlikely to reveal many proprietary details, employers should not be deterred from asking questions to evaluate AI products before investing in them. Employers that decide to adopt automated tools should evaluate how they perform using the employer's own data and carefully monitor their effects after deployment.

Employers should also examine these tools for accessibility to people with disabilities and ensure that AI use would not gather disability-related information or family medical history about employees.⁴ They also must have a clear, detailed plan to meet their obligations to provide reasonable accommodations for applicants or employees who need them for reasons related to a disability, religion, or medical conditions.

In this year of the nation's 250th anniversary, we need a new approach to equal employment opportunity in the digital age — one that proactively aligns AI adoption with our shared values of fairness, justice, and respect for human dignity. While this will also require additional guardrails, including transparency and accountability requirements for the use of AI, replacing the current AI adoption panic with a thoughtful approach centering workers' perspectives, and protecting their civil rights is a necessary first step.

Charlotte A. Burrows served as Chair of the U.S. Equal Employment Opportunity Commission (EEOC) from 2021-2025. Initially appointed by President Obama and confirmed by the U.S. Senate as a Commissioner in 2015, she served in that role until she was designated Chair by President Biden. As Chair, she launched the EEOC's ground-breaking Initiative on Artificial Intelligence and Algorithmic Fairness to help ensure that the use of AI in employment complies with workplace civil rights laws. Before joining the Commission, Burrows was an Associate Deputy Attorney General with the U.S. Department of Justice, providing legal advice on a variety of litigation, policy, oversight, and legislative matters. She previously served as an advisor to the late Senator Edward M. Kennedy on the Senate Judiciary Committee and Senate Committee on Health, Education, Labor, and Pensions, helping to pass the Genetic Information Nondiscrimination Act, the Americans with Disabilities Act Amendments Act, and the Lilly Ledbetter Fair Pay Act, among other laws. Before working on Capitol Hill, Burrows held litigation roles in the Department of Justice's Civil Rights Division and in private practice.

• • • • •

⁴ Both employers that deploy AI and AI vendors may be liable for employment discrimination resulting from AI models. See, e.g., *Mobley v. Workday*, US District Court for the Northern District of California No. 3:23-cv-00770-RFL (July 12, 2024), <https://www.eeoc.gov/sites/default/files/2024-04/Mobley%20v%20Workday%20NDCal%20am-brf%2004-24%20sjw.pdf>.





**OUR TECH,
OUR FUTURE:** HOW TO BUILD
A TECH INDUSTRY
ACCOUNTABLE TO

We the People



Access and Independence, But at What Cost?

Maria Town

*President and Chief Executive Officer
American Association of People with Disabilities*

Technology creates opportunities for people with disabilities. Full stop. Some technologies, like automated captioning, screen readers, and augmented or alternative communication devices are often used as reasonable accommodations for people with disabilities, opening up opportunities for gainful employment, quality healthcare, and community connection. Some tech companies claim that some of their products, like AI glasses and virtual assistants, are “life changing” or even “magical” for people with disabilities because of the increased independence and ease of access they can facilitate.¹ However, with the recognition of the benefits for disabled people, and the frequent representation of disabled people in their advertisements and marketing, tech companies often fail to consider privacy protections for these very users. Further, while they are happy to feature people with disabilities in their commercials and their user testing, tech companies hire very few disabled people to design, engineer, program, or govern these tools ourselves, denying us opportunities that could truly increase access, independence, and economic security.²

While tools like virtual assistants and AI glasses are available for use by anyone, some of the applications that these tools connect to in order to facilitate greater independence are used almost exclusively by people with disabilities. Many apps that facilitate navigation services for blind or low-vision people and some wearable technologies for people who are Deaf collect sensitive data from their users in order to be effective. Users are oftentimes not provided information about what the companies that create and sell these technologies do with the information that they collect, including whether they sell it to third parties.³ Users who are provided with this sort of information rarely receive it in plain language, which can make it even more difficult for people with certain disabilities to understand privacy practices.⁴

Companies may offer “opt out” choices to users, which users may choose to engage when interacting with sensitive information or activities. But disabled people who are using these technologies in healthcare settings to fluently read prescription medicines, accurately communicate confidential information, or confidently monitor symptoms may not feel like they can safely opt out. In fact, the reverse may be true, wherein the higher-stakes the interaction, the more a disabled person may want to rely on their technology, even if it compromises their privacy.



- 1 Tom Whipple, “Sceptical of Meta Glasses? They’re ‘Magical’ if You’re Blind,” *The Times* (Dec. 25, 2025), <https://www.thetimes.com/uk/science/article/meta-glasses-visual-impairment-audio-description-ai-Opvtczdsq>.
- 2 Stack Overflow, “2022 Developer Survey,” (June 22, 2022), <https://survey.stackoverflow.co/2022#developer-profile-demographics>.
- 3 Emile Ayoub and Elizabeth Goitein, “Closing the Data Broker Loophole,” *The Brennan Center for Justice* (Feb. 13, 2024), <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>.
- 4 Joel R. Reidenberg, Jaspreet Bhatia, Travis Breaux, and Thomas Norton, “Ambiguity in Privacy Policies and the Impact of Regulation,” *Journal of Legal Studies* (March 22, 2016), <https://ssrn.com/abstract=2715164>.

These privacy tradeoffs put people with disabilities in a difficult position where they must choose whether to protect their privacy or access the services and technologies that they need to live an accessible and independent life. With that, I must wonder: these technologies offer access and independence, but at what cost?

Technology has also transformed the workplace. From the types of jobs available, where and how those jobs can be done, the types of tasks one can complete independently, to the ways one can communicate daily, technology has specifically moved career ambitions that used to be out of reach for disabled people into the realm of possibility. Even with these enormous shifts in how work is accomplished, less than 23% of working-aged adults with disabilities were employed in 2025.⁵ Further, working-age adults with disabilities experience poverty at twice the rate of non-disabled adults.⁶

Within the science, technology, engineering, and mathematics (STEM) fields, the disability employment numbers are even worse: according to the National Science Foundation, only 3% of the STEM workforce are people with disabilities, and this number has not changed in the past decade.⁷ Given that most Americans will experience a disability at some point during their lives,⁸ increasing the employment of people with disabilities in STEM fields should be a matter of national importance.

If we want better research, better products, and better solutions, we need more disabled people in STEM.

The lack of hiring of disabled people in the tech industry is not just an issue of limited career options, but also represents a potential long-term barrier to increasing disabled people's economic security. The tech industry is poised to grow by more than 8% over the next 10 years, far outpacing the growth of non-STEM fields.⁹ Additionally, employment in the tech industry offers substantial economic opportunity: the median annual wage in the tech industry was \$105,990 in May 2024, more than twice the median annual wage for all other occupations.¹⁰ If the current trend of limited hiring of disabled people persists, the financial stability and security of people with disabilities will continue to erode.

This lack of opportunity is especially concerning as people with disabilities experience significant occupational segregation and are over-represented in low-wage occupations that are among the highest risk for automation, such as sales, office support, service occupations, production, transportation, and material-moving occupations.¹¹

- 
- 5 US Bureau of Labor Statistics, "People with a Disability: Labor Force Characteristics — 2025." *US Department of Labor* (March 3, 2026), www.bls.gov/news.release/pdf/disabl.pdf.
- 6 Patrick Drake and Alice Burns, "Working-Age Adults with Disabilities Living in the Community," *KFF* (Jan. 4, 2024), <https://www.kff.org/medicaid/working-age-adults-with-disabilities-living-in-the-community/>.
- 7 Lenore K. Pedicord, "NSF Supports Efforts to Emphasize the Ability in 'Disability,'" *US National Science Foundation* (Oct. 24, 2024), <https://www.nsf.gov/science-matters/nsf-supports-efforts-emphasize-ability-disability>.
- 8 US Centers for Disease Control and Prevention, "Disability and Health Overview," (April 2, 2025), <https://www.cdc.gov/disability-and-health/about/>.
- 9 US Bureau of Labor Statistics, "The Economics Daily: Numbers, Research, and Discovery: STEM Employment Projected to Take Off!" *US Department of Labor* (Dec. 9, 2025), <https://www.bls.gov/opub/ted/2025/numbers-research-and-discovery-stem-employment-projected-to-take-off.htm>.
- 10 US Bureau of Labor Statistics, "Computer and Information Technology Occupations," *US Department of Labor* (Aug. 28, 2025), <https://www.bls.gov/ooh/computer-and-information-technology/>.
- 11 Taylor M. Shockey, Kelsie Fox, Guixiang Zhao, and NaTasha Hollis, "Prevalence of Disability by Occupation Group — United States, 2016–2020," *US Centers for Disease Control and Prevention* (May 19, 2023), <http://dx.doi.org/10.15585/mmwr.mm7220a1>.

The very tools and technologies that have the ability and potential to increase independence, quality of life, and opportunities for disabled people may also cause the very few job opportunities available to us to vanish. Again, I ask: access and independence, but at what cost?

Maria Town is the President and CEO of the American Association of People with Disabilities. In this role, she works to increase the political and economic power of people with disabilities. Town previously served as Director of the City of Houston Mayor's Office for People with Disabilities, advocating for citizens with disabilities. Town also was the Senior Associate Director in the Obama White House Office of Public Engagement, managing disability community engagement and coordinating federal engagement. Town has expertise in areas of youth development, leadership, and promoting college and career readiness.



OUR TECH, HOW TO BUILD
OUR FUTURE: A TECH INDUSTRY
ACCOUNTABLE TO

We're People



From the Interstate Highway Era to AI Data Centers:

Safeguarding Housing and Health in Infrastructure Placement

Michael Akinwumi

*Chief AI Officer & Head of the Responsible AI Lab
National Fair Housing Alliance (NFHA)*

Today, the U.S. stands at another infrastructure inflection point: not asphalt and concrete, but fiber, substations, and data centers. The AI Action Plan positions digital infrastructure as a pillar of national competitiveness and geopolitical leadership.¹ Just as the Interstate Highway System, a significant infrastructure project established via the Federal-Aid Highway Act of 1956, was justified based on the need to modernize our travelways, enhance national defense, and promote economic growth. Highways promised mobility, suburban expansion, and commercial development. Yet routing decisions often cut directly through Black neighborhoods, displacing families, depressing property values, disconnecting people from job and economic centers, and fragmenting social networks. These projects were frequently framed as neutral exercises in engineering and progress. The harms were not always explicitly articulated as intentional discrimination. But their effects were durable: concentrated wealth extraction, reduced access to opportunity, and generational racial disparities in housing and health.²

Federal momentum toward AI dominance coincides with regulatory shifts that attempt to concentrate federal AI policy, weaken environmental guardrails, and usurp local- and state-level authority to make AI infrastructure decisions. Hence, the question is not whether AI infrastructure should be built. It is how and where it is built, lest we repeat the intentional displacement and economic harm inflicted on Black communities in the 1950s. AI infrastructure projects should proceed only after a mandatory environmental and social impact assessment and the adoption of a legally binding community benefit agreement, ensuring that marginalized communities are not disproportionately burdened by their development.

AI data centers are expanding rapidly across the country to meet escalating computational demand, and their environmental impact is clearer every day. AI systems could generate between 32.6 and 79.7 million tons of CO₂ emissions and consume 312.5–764.6 billion liters of water in 2025 — levels comparable to New York City’s annual carbon output and roughly equivalent to the world’s yearly bottled-water consumption.³

Water consumption at hyperscale facilities can reach millions of gallons per day for cooling alone, exacerbating local water scarcity.^{4,5} These facilities require substantial site footprints that can contribute to resource-intensive

- • • • •
- 1 Michael J. Kratsios, David O. Sacks, and Marco A. Rubio, “Winning the Race: America’s AI Action Plan,” *The White House* (July 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.
 - 2 Deborah N. Archer, “White Men’s Roads through Black Men’s Homes: Advancing Racial Equity through Highway Reconstruction,” *The Vanderbilt Law Review* (2020), <https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/1>.
 - 3 Alex de Vries-Gao, “The Carbon and Water Footprints of Data Centers and What This Could Mean for Artificial Intelligence,” *Patterns* (2026), <https://doi.org/10.1016/j.patter.2025.101430>.
 - 4 Yu Tao and Peng Gao, “Global Data Center Expansion and Human Health: A Call for Empirical Research,” *Eco-Environment & Health* (Sept. 2025), <https://doi.org/10.1016/j.eehl.2025.100157>.
 - 5 David Mytton, “Data Centre Water Consumption,” *npj Clean Water* (Feb. 15, 2021), <https://doi.org/10.1038/s41545-021-00101-w>.

infrastructure expansion.⁶ Depending on their design and construction, data centers can also release toxins into nearby communities with devastating health, economic, and other impacts.⁷

Decisions on where large-scale AI data centers are ultimately located carry material consequences for property values, health outcomes, housing affordability and accessibility, and public services.

Industrial adjacency and environmental stigma can influence real estate markets. Research shows that proximity to pollution sources is not randomly distributed: Black residents face 1.54 times higher particulate matter (PM^{2.5})⁸ burdens than the overall population, with those in poverty facing 1.35 times higher impacts.⁹ These disparities operate across national, state, and county levels. Environmental risk can depress home values, and because housing is the primary asset for most American families, property value suppression translates directly into intergenerational wealth loss. Health burdens compound this dynamic. Exposure to particulate matter is associated with cardiovascular and respiratory disease.¹⁰ While all of the causes of asthma remain unclear and may be related to increased exposure to pollution, in 2019, non-Hispanic Black individuals were almost three times more likely to die from asthma-related causes than their non-Hispanic White counterparts, and non-Hispanic Black children faced an even more severe disparity, with asthma death rates eight times higher than those of non-Hispanic White children.¹¹

Civil rights law provides a framework for understanding these structural dynamics. The Fair Housing Act's disparate impact doctrine recognizes that policies may violate the law when they produce unjustified discriminatory effects, regardless of intent. Environmental justice scholarship has long demonstrated that hazardous facilities disproportionately burden people of color and low-income neighborhoods. Studies of hazardous waste siting and air pollution reveal systematic targeting or tolerance of risk in communities with less political power.¹² Cheryl Harris's theory of "whiteness as property" underscores how property rights and racial hierarchy have historically intersected to secure advantage for some communities while constraining others.¹³ Decisions on where AI data centers are located are no different. Even facially neutral criteria can replicate patterns of structural vulnerability

The risk of repeating harms to marginalized communities based on infrastructure decisions is clear.

Highway construction was justified as a national imperative. Newly-constructed highways and bridges often ran through communities with the least political leverage — not by accident, but by design. Local governments and industry allow data centers to be placed in locations where land is cheaper and historically divested communities have less concerted political power to push back on the decisions. Generous tax incentives may attract facilities without guaranteeing durable local benefit. Environmental and grid costs can be externalized onto surrounding

6 Can Hankendi, Ayse K. Coskun, and Benjamin K. Sovacool, "Why Transparency Matters for Sustainable Data Centers and Carbon-Neutral Artificial Intelligence (AI)," *iScience* (Nov. 21, 2025), <https://doi.org/10.1016/j.isci.2025.113705>.

7 The Kapor Foundation, "The Unequal Burden of Data Centers: An Examination of the Environmental and Public Health Impacts on Communities in California," (Dec. 9, 2025), <https://kaporfoundation.org/datacenters-envt-health>.

8 Particulate matter (PM) refers to a mixture of solid particles and liquid droplets suspended in the air that are small enough to be inhaled and, in some cases, absorbed into the bloodstream. PM^{2.5} refers to particulate matter 2.5 micrometers or smaller, linked to respiratory and cardiovascular disease and increased risk of premature death.

9 Ihab Mikati, Adam F. Benson, Thomas J. Luben, Jason D. Sacks, and Jennifer Richmond-Bryant, "Disparities in Distribution of Particulate Matter Emission Sources by Race and Poverty Status," *The American Journal of Public Health* (March 7, 2018), <https://doi.org/10.2105/AJPH.2017.304297>.

10 *Id.*

11 Office of Minority Health, "Asthma and African Americans," *U.S. Department of Health and Human Services* (Feb. 2021), <https://minorityhealth.hhs.gov/node/39/revisions/39/view>.

12 Paul Mohai and Robin Saha, "Which Came First, People or Pollution? Assessing the Disparate Siting and Post-Siting Demographic Change Hypotheses of Environmental Injustice," *Environmental Research Letters* (Nov. 18, 2015), <https://doi.org/10.1088/1748-9326/10/11/115008>.

13 Cheryl I. Harris, "Whiteness as Property," *The Harvard Law Review* (June 1993), <https://www.jstor.org/stable/1341787>.

communities. The through-line may not be explicit racial intent; it is the predictable distribution of burdens along lines shaped by past racial segregation and ongoing disinvestment in marginalized communities.

This moment calls not for opposition to AI infrastructure, but for integrating fair housing analysis, environmental burden mapping, and housing impact modeling into infrastructure permitting decisions and design. Infrastructure is never neutral; it can either build or break communities. Civil-rights-informed decisions on how the burdens of innovation will be shouldered for large-scale AI infrastructure should include:

- 1. Mandatory cumulative impact assessments.** Evaluating how the design, construction, and resource needs of new data centers interact with and impact existing environmental burdens in a neighborhood.
- 2. Fair housing impact assessments.** Modeling how large-scale infrastructure projects will affect local land prices, utility rates, housing accessibility, and housing affordability before permits are granted.
- 3. Community benefit agreements.** Tying tax abatements and land-use approvals to enforceable commitments for local infrastructure improvements and funding to promote fair and affordable housing.

The Interstate Highway Era taught us that when "national interest" is defined without a civil rights lens, communities that are already marginalized pay the highest price. As we build the infrastructure of the AI age, we have a responsibility to ensure that the "golden age of human flourishing" promised by technological dominance is not built upon the displacement, isolation, economic destruction, and disinvestment of the same communities we have failed before. We must apply these lessons now, before new choices become embedded for generations.

Dr. Michael Akinwumi is an executive leader at the intersection of technology, civil rights, and equity — working to ensure that the systems shaping tomorrow do not replicate the injustices of yesterday. Grounded in a computational justice framework, he guides organizations in developing and deploying technology toward solutions that meet rigorous standards of alignment, safety, security, and policy compliance. Michael is widely recognized for strengthening institutional standards for trustworthy technology deployment, guiding organizations integrating alignment, risk management, and accountability into operational AI systems. He partners with policymakers, industry leaders, and community stakeholders to advance innovation that protects and expands opportunity for communities that have historically been marginalized.



OUR TECH, OUR FUTURE: HOW TO BUILD A TECH INDUSTRY ACCOUNTABLE TO *We the People*



How ICE and Big Tech are Normalizing Mass Surveillance

John C. Yang

President & Executive Director

Asian Americans Advancing Justice | AAJC

Large-scale immigrant surveillance in the U.S. across recent decades would not be possible without Big Tech. Tech companies quietly contribute various technological and logistical infrastructure — everything from databases on immigrants to communications systems — for agencies like U.S. Immigrations and Customs Enforcement (ICE) and U.S. Customs and Border Patrol (CBP). ICE and CBP collectively have approximately \$515 million in contracts with Microsoft, Amazon, Google, and Palantir; many additional companies have indirect or subcontracted relationships with ICE that are not as well documented.¹

The tech industry’s enablement of government surveillance for immigration enforcement threatens democracy by normalizing heightened surveillance, escalating the use of biased, imperfect technology, and suppressing dissenting voices.

Asian Americans, who have historically been disproportionately targeted by government surveillance and viewed as “perpetual foreigners,” are especially vulnerable to these threats. Tech companies should consider how their active roles in immigration enforcement-related activities directly undermine the safety and wellbeing of their foreign-born workers and contribute to climates of fear and apprehension across the country.² Many of these companies’ own employees and the general public have called on these corporations to roll back their involvement in the U.S. government’s immigrant surveillance apparatus.^{3, 4} Big Tech should take these concerns seriously. Common-sense reforms like increased transparency around government contracts, delineation of organizational red lines, and anti-retaliation protections for workers will ultimately serve these companies’ best interests and create goodwill among stakeholders like shareholders and customers.

Normalization of mass surveillance: ICE’s immigration crackdown and the mass surveillance it powers have ingrained surveillance into Americans’ everyday lives. Recent evidence showing the targeting of American citizens as part of this operation underscores that everyone in the U.S., regardless of immigration status, experiences the negative consequences of large-scale monitoring.^{5, 6}



- 1 Carolin Haskins, “All the Ways Big Tech Fuels ICE and CBP,” *WIRED* (March 3, 2026), <https://www.wired.com/story/how-big-tech-is-powering-trumps-immigration-crackdown/>.
- 2 Alison Snyder, “Foreign-Born STEM Talent Remains Key to U.S. Research,” *Axios* (March 13, 2024), <https://www.axios.com/2024/03/13/us-workforce-foreign-born-stem-research>.
- 3 Jessica Guynn, “Tech CEOs Have Been Quiet on ICE. Their Workers Want Them to Speak Up,” *USA TODAY* (Jan. 21, 2026), <https://www.usatoday.com/story/money/2026/01/21/tech-workers-ice-trump-protest/88285079007/>.
- 4 #NoTechForICE, “About,” *Mijente*, <https://notechforice.com/about/>.
- 5 Autumn Billing, “ICE Is Mounting a Mass Surveillance Campaign on American Citizens,” *Reason* (Oct. 23, 2025), <https://reason.com/2025/10/23/ice-is-mounting-a-mass-surveillance-campaign-on-american-citizens/>.
- 6 Nicole Foy, “We Found That More Than 170 U.S. Citizens Have Been Held by Immigration Agents. They’ve Been Kicked, Dragged and Detained for Days,” *ProPublica* (Oct, 16, 2025), <https://www.propublica.org/article/immigration-dhs-american-citizens-arrested-detained-against-will>.

Historical examples highlight the perils of the U.S. government spying on its own people. In the lead up to, throughout, and following the incarceration of Japanese Americans during World War II, various federal agencies tracked the daily activities of and compiled files on thousands of individuals of Japanese descent, a majority of whom were U.S. citizens.⁷ Beginning in 1967 and into the 1970s, the FBI operated a classified program that surveilled thousands of Chinese scientists and science students through tactics like informants and wiretapping.⁸ While these surveillance methodologies are low-tech by today's standards, they helped to lay the groundwork for racially discriminatory programs like the more recent "China Initiative" and the growth of modern surveillance technology.⁹

Growth of imperfect, often biased, technology: Surges in immigration enforcement have also led to the explosive growth of various surveillance technologies like biometric tracking, including through facial recognition and fingerprint scanning. Though these types of technology can be beneficial under certain circumstances and with proper guardrails in place, they have troubling historical roots and can be ineffective, particularly on Asian faces.¹⁰ Much of America's modern biometric security empire can trace its beginnings back to the monitoring of Arab, Middle Eastern, Muslim, and South Asian communities after the September 11 terrorist attacks by the then newly created Department of Homeland Security.¹¹ In the immediate aftermath, biometrics was presented as a "scientific," evidence-based solution to prevent future atrocities; when the 9/11 Commission published its final report, it urged the installation of biometric screening systems at all U.S. borders. Under the guise of fighting the "War on Terror," **nascent forms of the same technologies deployed against immigrants today were used to surveil and discriminate against Arab, Middle Eastern, Muslim, and South Asian communities decades ago.** Now, for example, ICE can use facial recognition technology powered by companies like Clearview AI to identify immigrants within a matter of seconds.¹² Automatic license plate readers represent another disturbing frontier of mass surveillance made possible by tech companies. Flock Safety has allowed ICE to access tens of thousands of its AI-enabled license plate readers across the country.¹³ These cameras capture the license plate, make, and model of *all* passing vehicles; as such, **"immigrant" surveillance is increasingly mass domestic surveillance.** As the government pumps billions of dollars into these companies that continue to expand their capabilities, Americans become more and more used to scanning their faces to board flights, using their fingerprints to unlock electronic devices, and being constantly monitored by omnipresent security cameras. As Emily Tucker, executive director of the Center on Privacy and Technology at Georgetown Law says, "Immigration powers are being used to justify mass surveillance of everybody."¹⁴

- ● ● ● ● ● ● ●
- 7 National Archives, "World War II Japanese American Incarceration: Pre-War Surveillance and Planning," *Asian American and Pacific Islander Records at the National Archives* (Feb. 13, 2025), <https://www.archives.gov/research/aapi/ww2/planning>.
 - 8 Andrea Widener, "70 Years of US Suspicion toward Chinese Scientists — and What Those Caught In the Middle Should Do Now," *Chemical & Engineering News* (March 22, 2020), <https://cen.acs.org/policy/research-funding/70-years-US-suspicion-toward/98/i11>.
 - 9 Mike German, "The 'China Initiative' Failed U.S. Research and National Security. Don't Bring It Back," *The Brennan Center for Justice* (Sept. 23, 2024), <https://www.brennancenter.org/our-work/analysis-opinion/china-initiative-failed-us-research-and-national-security-dont-bring-it>.
 - 10 Natasha Singer and Cade Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study," *The New York Times* (Dec. 19, 2019), <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>.
 - 11 Nina Dewi Toft Djanegara, "How 9/11 Sparked the Rise of America's Biometrics Security Empire," *Fast Company* (Sept. 10, 2021), <https://www.fastcompany.com/90674661/how-9-11-sparked-the-rise-of-americas-biometrics-security-empire>.
 - 12 Lorenzo Franceschi-Bicchieri and Zack Whittaker, "Here's the Tech Powering ICE's Deportation Crackdown," *TechCrunch* (Jan. 26, 2026), <https://techcrunch.com/2026/01/26/heres-the-tech-powering-ices-deportation-crackdown/>.
 - 13 Jay Stanley, "Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance," *The American Civil Liberties Union* Aug. 18, 2025), <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-roundup>.
 - 14 Jude Joffe-Block, "Immigration agents have new technology to identify and track people," *NPR* (Nov. 8, 2025), <https://www.npr.org/2025/11/08/nx-s1-5585691/ice-facial-recognition-immigration-tracking-spyware>.

Suppression of critical voices: The latest immigration crackdown has also highlighted First Amendment concerns. Google (whose parent company Alphabet owns YouTube), Meta, and Reddit have complied with DHS subpoenas looking to identify users on its platforms who have been critical of ICE.¹⁵ Apple and Google have also removed apps like ICEBlock that track the presence of ICE agents in neighborhoods from their app stores.¹⁶ Similar reporting has identified documents outlining ICE plans to hire contractors to scan social media platforms like X, Facebook, and Instagram to identify individuals for deportation.¹⁷ And under a new rule by the U.S. Citizenship and Immigration Services (USCIS), any individual applying for a change in immigration status (e.g., someone seeking a green card or applying for citizenship) must present their social media handles, as well as those of their family members, to the government.¹⁸ These examples show how deeply tech companies have become enmeshed with immigration enforcement efforts by the U.S. government.

Recommendations for tech companies:

1. **Increase transparency.** Tech companies should publish detailed transparency reports that include information such as all federal, state, and local immigration enforcement contracts (including the scope and financial value of these agreements) and the types of information shared with government agencies.
2. **Establish clear lines in the sand for prohibited uses.** These companies should also delineate clear boundaries that prohibit certain uses of their technologies for purposes like dragnet social media monitoring and mass surveillance of people in the United States not tied to individualized suspicion¹⁹
3. **Strengthen anti-retaliation protections.** Employees at tech companies who raise concerns about the involvement of their employers with immigration enforcement and other activities through actions like participating in protests or signing open letters to their CEOs should be protected from retaliation.

Recent immigration enforcement operations have been explicitly race-based, targeting those who speak English with an accent, have darker skin, or work certain jobs.²⁰ This has an outsized negative impact on Asian Americans and other people of color who are consistently otherized and branded as “not fully American,” even if they themselves have legal status in the U.S..²¹

The decision of tech companies, who have historically championed progressive values like equality and sustainability, to work directly with ICE’s “deportation machine” is a betrayal of their principles and the very people who keep their businesses afloat.

15 Kevin Haynes, “Big Tech Confirms DHS Subpoenas: Meta and Google Users Targeted Over Anti-ICE Posts,” *Inc.* (Feb. 15, 2026), <https://www.inc.com/kevin-haynes/big-tech-confirms-dhs-subpoenas-meta-and-google-users-targeted-over-anti-ice-posts/91303363>.

16 Wyatt Grantham-Philips, Matt O’Brien, and Kelvin Chan, “Apple and Google Block Apps that Crowdsource ICE Sightings. Some Warn of Chilling Effects,” *AP News* (Oct. 3, 2025), <https://apnews.com/article/apple-ice-iphone-app-immigration-fb6a404d3e977516d66d470585071bcc>.

17 Dell Cameron, “ICE Wants to Build Out a 24/7 Social Media Surveillance Team,” *WIRED* (Oct. 3, 2025), <https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/>.

18 Julia Malleck, “USCIS Aims to Expand Social Media Surveillance of Immigrants and US Citizens,” *Truthout* (Feb. 20, 2026), <https://truthout.org/articles/uscis-aims-to-expand-social-media-surveillance-of-immigrants-and-us-citizens/>.

19 Katya Schwenk, “ICE Just Spent Millions on a Social Media Surveillance AI Program,” *Truthout* (Oct. 25, 2025), <https://truthout.org/articles/ice-just-spent-millions-on-a-social-media-surveillance-ai-program/>.

20 Erin Mansfield, “Supreme Court said ICE Can Stop You Based on Race, Accent, Job and Location. What We Know,” *USA TODAY* (Sept. 10, 2025), <https://www.usatoday.com/story/news/politics/2025/09/10/immigration-enforcement-stops-race-language-job/86048527007/>.

21 Nicole Foy, “We Found That More Than 170 U.S. Citizens Have Been Held by Immigration Agents. They’ve Been Kicked, Dragged and Detained for Days,” *ProPublica* (Oct. 16, 2025), <https://www.propublica.org/article/immigration-dhs-american-citizens-arrested-detained-against-will>.

If these companies cannot commit to refusing to work with the current administration's sweeping mass deportation campaign, then they should — at the very least — be transparent to their employees, customers, shareholders, and other stakeholders about the nature of the services they are providing for these purposes. They should also adopt firm red lines and provide their employees with means of speaking out when they feel their employers have crossed these lines. If major tech giants continue to put profits over people, keep granting the government unfettered access to its technologies, and remain complicit in attacks on immigrant rights, the impacts for all Americans will be devastating.

John C. Yang is the President and Executive Director of Asian Americans Advancing Justice | AAJC in Washington, D.C., where he leads the organization's mission to advance the civil and human rights of Asian Americans and to build and promote a fair and equitable society for all through policy advocacy, litigation, education, and community empowerment. Because of his extensive legal experience and expertise, John has testified before Congress and appeared regularly in national media on issues of importance to the Asian American community. He has served in leadership positions for the American Bar Association, the National Asian Pacific American Bar Association, and the National Council of Asian Pacific Americans, among many others. Prior to Advancing Justice | AAJC, John had served as a political appointee in the Obama Administration, the Asia-Pacific Legal Director of a Fortune 200 company, and as a partner at a large D.C.-based law firm. He also serves on the diversity council for several Fortune 500 U.S. companies.





OUR TECH,
OUR FUTURE:

HOW TO BUILD
A TECH INDUSTRY
ACCOUNTABLE TO

We the People



The Digital Frontier:

Protecting Latino Civil Rights in the Age of Algorithms

Juan Proaño

Chief Executive Officer

League of United Latin American Citizens (LULAC)

The tech industry likes to imagine itself above politics. Engineers design tools. Companies sell them. Governments decide how they will be used. It is a comforting story. It allows everyone to believe responsibility lives somewhere else. But technology does not exist outside society. It exists inside it — inside police departments, immigration agencies, courtrooms, and bureaucracies. It operates in the same landscape where power, race, and inequality already shape outcomes. For Latino communities and other racial and ethnic minorities, that reality is impossible to ignore.

No doubt, innovation can expand opportunity, but at the same time, it can also expand surveillance. When powerful data systems intersect with policing or immigration enforcement, the stakes are no longer theoretical: they become practical questions about civil rights.

Consider the debate surrounding Amazon's facial recognition system, Rekognition. In 2018, civil rights advocates began warning that facial recognition tools could easily become inaccurate and biased instruments of mass surveillance, especially in communities already watched closely by the state. Their concerns were grounded in evidence: researchers at the Massachusetts Institute of Technology found that several facial recognition systems were far less accurate when identifying people with darker skin tones.¹ That same year, the American Civil Liberties Union ran a public test and discovered that Rekognition incorrectly matched 28 members of Congress to mugshot databases, and most of those false matches involved lawmakers from racial and ethnic minority groups.²

The technology was not neutral. It carried bias in its design and in its outcomes. By 2020, the controversy had grown large enough that Amazon announced a moratorium on police use of Rekognition in criminal investigations.³ The company imposed what was supposed to be a one-year pause on the program, but the pause is still in effect six years later.⁴

The moment revealed something important: companies do have the power to draw lines when civil rights are at stake. Those lines should not appear only when controversy erupts. They should exist from the beginning.



1 Larry Hardesty, "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems," *MIT News* (Feb. 11, 2018), <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>.

2 Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," *The American Civil Liberties Union* (July 26, 2018), <https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28>.

3 Bobby Allyn, "Amazon Halts Police Use of Its Facial Recognition Technology," *NPR* (June 10, 2020), <https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology>.

4 Fangzhou Cheng and Marcel Pividal, "Transitioning from Amazon Rekognition People Pathing: Exploring Other Alternatives," *Amazon Web Services Blog* (Oct. 24, 2024), <https://aws.amazon.com/blogs/machine-learning/transitioning-from-amazon-rekognition-people-pathing-exploring-other-alternatives/>.

Simply put, companies have a responsibility to consider the civil rights impacts of the technology they create or use. Tech companies should establish firm rules about how their tools can and cannot be used in immigration enforcement. Without those boundaries, technologies drift into new purposes. A system designed for identity verification can become a surveillance device. A database intended for security can quietly become an instrument of immigration control.

The danger lies not only in the technology itself but in the quiet way systems expand. Tools migrate. Databases merge. Information moves between agencies. Surveillance grows gradually, often without public debate.

We have already seen how small errors can carry enormous consequences. In one immigration enforcement encounter, officers using facial recognition software received only a “possible match.” The system did not confirm the identity; it merely suggested one. Yet the suggestion influenced the decision to detain the individual. The machine hesitated, but the human officers moved forward anyway.⁵

The same pattern has appeared in the federal government’s CBP One application that asylum seekers must use to request appointments at the border. Migrants have reported repeated failures when attempting to verify their identities through the app’s facial recognition system.⁶ Applicants with darker skin tones have described difficulty submitting photographs that the system will accept.⁷ What appears to the programmer as a technical inconvenience becomes, in practice, a barrier to asylum. **In such moments, technology becomes policy.**

That is why companies must take due diligence before selling surveillance technologies to government agencies. The tech industry often moves quickly. Products are built, released, and refined in the name of innovation while ethical questions are postponed until they become an emergency, and by then, the damage is done. But biometric systems are not ordinary software tools. When they fail, they do not simply crash. They reshape lives.

There is a path forward. Tech companies should conduct and publish civil rights impact assessments before deploying surveillance tools. They should study how their products perform across racial and ethnic groups. They should analyze how those tools might be used in immigration enforcement. And they should make those findings public. Transparency is not an inconvenience. It is a responsibility. And that means prohibiting the use of technology or not developing it in the first place where the risks to civil rights are too high.

Pressure for this kind of accountability has begun to emerge from within the technology industry itself. In 2018, thousands of employees at Google protested the company’s participation in Project Maven, a Pentagon initiative using AI to analyze drone footage.⁸ According to the 2018 article “Google Employees Quit in Protest Over Military Artificial Intelligence Program,” more than 3,000 employees signed a petition opposing the project and several engineers resigned in protest.⁹ Their actions forced the company to reconsider its role. Google ultimately declined to renew the contract and later adopted internal principles governing how its AI technologies could be used.¹⁰ The protest revealed something important: the people who build these technologies understand their moral weight.



5 Dell Cameron and Maddy Varner, “ICE and CBP’s Face-Recognition App Can’t Actually Verify Who People Are,” *WIRED* (Feb. 5, 2026), <https://www.wired.com/story/cbp-ice-dhs-mobile-fortify-face-recognition-verify-identity/>.

6 Bernd Debusmann Jr, “At US Border, Tech Issues Plague New Migrant Applications,” *The BBC* (March 8, 2023), <https://www.bbc.com/news/world-us-canada-64814095>.

7 *Id.*

8 Scott Shane and Daisuke Wakabayashi, “The Business of War: Google Employees Protest Work for the Pentagon,” *The New York Times* (April 4, 2018), <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>.

9 Sam Harnett, “Google Employees Quit in Protest Over Military Artificial Intelligence Program,” *KQED* (May 17, 2018), <https://www.kqed.org/news/11668872/google-employees-quit-in-protest-over-military-artificial-intelligence-program>.

10 Erin Griffith, “Google Won’t Renew Controversial Pentagon AI Project,” *WIRED* (June 1, 2018), <https://www.wired.com/story/google-wont-renew-controversial-pentagon-ai-project/>.

Shareholders are beginning to recognize that weight as well. Tech companies depend on trust as much as innovation. When a firm becomes associated with civil rights violations, whether through wrongful identification, immigration surveillance, or discriminatory algorithms, public trust erodes quickly — not just trust of that company, but of AI as a whole. **Reputation is not simply a public relations issue. It is a market reality.**

For Latino communities, these debates are not abstract policy arguments. Immigration enforcement in the U.S. already relies heavily on digital infrastructure, including databases, biometric records, and information sharing between agencies. When technologies such as facial recognition and predictive analytics are layered onto that infrastructure, the result can resemble a new form of policing. It is quieter and more automated, but it remains powerful.

Innovation itself is not the enemy. Technology can serve the public good: it can locate missing children, expose corruption, and strengthen democratic institutions. But innovation without restraint risks magnifying the inequalities that already exist within our institutions.

In the end, the question is not whether technology will advance. It will. The real question is whether the people who build it will pause long enough to ask who pays the price when it fails.

For many Latino families, that question carries an old and familiar anxiety. It is the fear of being mistaken for someone else in the eyes of the government. Once that mistake came from a paper file or a clerical error. Today, it may come from an algorithm. Machines may calculate quickly. Justice still requires judgment. And judgment in a democracy requires humility.

Juan Proaño is an entrepreneur, technologist, and business leader who is active in civic affairs, social impact, and politics. In his two decades of entrepreneurship, Juan has founded and managed three companies in the tech industry, including Plus Three, a tech-company– serving nonprofit, advocacy, membership, and political organizations. Juan has been recognized for his pioneering work in technology and online fundraising fields. He has been featured in Time Magazine and has been recognized by the United States Hispanic Chamber of Commerce as one of the top 100 Latino CEOs. Active in civic and community affairs, Juan has been a bridge builder between various underrepresented communities: at the NAACP, he served as the first Latino on the CEO Advisory Committee, led their response to Hurricane Katrina, worked on the Voting Rights Reauthorization Act, and worked on a major campaign against capital punishment.



OUR TECH, OUR FUTURE: HOW TO BUILD A TECH INDUSTRY ACCOUNTABLE TO *We the People*



Why State Law is Critical to Holding Tech Companies Accountable and Protecting Civil Rights

Damon Hewitt

President and Executive Director

The Lawyers' Committee for Civil Rights Under Law

The use of AI has expanded rapidly, now being used in workplaces, homes, and even in government. Many people find this technology useful in their daily lives. It has become so commonplace that some people don't really know they are using it in devices and on platforms at the tips of their fingers. However, this period of growth and expanded reliance, like the technology itself, has no guardrails at the federal level to protect us when things go wrong.

Unregulated technology poses significant risks. Just like other products and devices we take for granted today, AI can also cause harm if not built and suited for how people live and work. This is especially true for Black people and other communities of color.

We know AI has been used in ways that have created or compounded racial discrimination across every sector of American life, including in law enforcement, education, delivery of healthcare, and access to credit.

Violations of privacy, proliferation of online hate, digital surveillance, targeted disinformation, and algorithmic bias are all too commonplace.^{1, 2, 3, 4, 5} For example, a 2019 Berkeley study found that biases in “algorithmic strategic pricing” have resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans as compared to White and Asian borrowers.⁶ And universal technological risks, like privacy abuses, often disproportionately impact communities of color. When companies track cell phone location data without consent, and then sell this data to debt collectors, bail bondsmen, and other predatory actors, the harms are disproportionately felt by low-income Black and Brown communities.⁷

- • • • •
- 1 Spencer Overton, “Overcoming Racial Harms to Democracy from Artificial Intelligence,” *The Iowa Law Review* (Jan. 15, 2025), <https://ilr.law.uiowa.edu/volume-110-issue-2/overcoming-racial-harms-democracy-artificial-intelligence>.
 - 2 NAACP, “Stop Dirty Data Centers,” (2026), <https://naacp.org/campaigns/stop-dirty-data-centers>.
 - 3 Ivey Dyson, “How AI Threatens Civil Rights and Economic Opportunities,” *The Brennan Center for Justice* (Nov. 16, 2023), <https://www.brennancenter.org/our-work/analysis-opinion/how-ai-threatens-civil-rights-and-economic-opportunities>.
 - 4 United Nations High Commissioner for Human Rights, “Racism, and AI: Bias From the Past Leads to Bias in the Future,” *United Nations* (July 30, 2024), <https://www.ohchr.org/en/stories/2024/07/racism-and-ai-bias-past-leads-bias-future>.
 - 5 Kimberly Holmes-Iverson, “Your Computer Might Be Racist,” *Howard Magazine* (2023), <https://magazine.howard.edu/stories/your-computer-might-be-racist>.
 - 6 Laura Counts, “Minority Homebuyers Face Widespread Statistical Lending Discrimination, Study Finds,” *UC Berkeley Haas School of Business* (Nov. 13, 2018), <https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>.
 - 7 Joseph Cox, “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” *Vice News* (Jan. 8, 2019), <https://www.vice.com/en/article/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile/>.

We need a variety of tools to limit the harm from emerging technology. State civil rights and consumer protection laws have been among the most effective tools for accountability, supplementing federal civil rights protections in various contexts, such as disability⁸ and employment discrimination.⁹ In fact, state laws have often been ahead of federal law, providing greater protection and opportunities to pilot novel regulatory solutions, particularly those solutions addressing emerging technologies.

In recent years, states across the nation have been rapidly passing laws to fill gaps in tech regulation.^{10, 11} As of 2026, nineteen states have adopted comprehensive data privacy laws to protect residents¹² and some have adopted laws to regulate data brokers that rabidly collect data about consumer behavior and sell it for profit.¹³ Many states and cities have also adopted laws regulating the use of biometric and facial recognition tools.¹⁴ Also, every state has a law that requires companies to notify people when their data has been breached, and many states' laws include obligations to provide further protections.¹⁵

Longstanding state consumer protection and civil rights laws have also been crucial in holding tech companies accountable even without specific tech and AI laws. For example, state regulators^{16, 17} and private parties regularly use consumer protection laws^{18, 19} to sue tech companies and hold them accountable in state courts. In fact, the Lawyers' Committee for Civil Rights Under Law, representing the Equal Rights Center, filed a lawsuit challenging Meta's racially discriminatory advertising practices, using claims under Washington, D.C.'s consumer protection and public accommodations laws.²⁰ Parties have also leveraged traditional state tort laws, such as products liability²¹ and public nuisance laws,²² in actions against tech companies. An added benefit of state laws is that

- • • • •
- 8 Bloomberg Law, "State Disability Discrimination Laws," (March 18, 2024), <https://pro.bloomberglaw.com/insights/labor-employment/state-disability-discrimination-laws/#california>.
 - 9 Justia, "Employment Discrimination Laws: 50-State Survey," (Sept. 2022), <https://www.justia.com/employment/employment-laws-50-state-surveys/employment-discrimination-laws-50-state-survey/>.
 - 10 The Business Software Alliance, "2025 State AI Wave Building After 700 Bills in 2024," (Oct. 22, 2024), <https://www.bsa.org/news-events/news/2025-state-ai-wave-building-after-700-bills-in-2024>.
 - 11 The National Conference of State Legislatures, "Artificial Intelligence 2025 Legislation," (July 10, 2025), <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation>.
 - 12 The National Conference of State Legislatures, "Consumer Privacy 2025 Legislation," (July 28, 2025), <https://www.ncsl.org/technology-and-communication/consumer-privacy-2025-legislation>.
 - 13 Rachel Melissa and Tonkon Torp LLP, "States Increase Regulation on Data Brokers," *JD Supra* (Nov. 4, 2025), <https://www.jdsupra.com/legalnews/states-increase-regulation-on-data-3931680/>.
 - 14 Jake Laperruque, "Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations," *Tech Policy Press* (Jan. 6, 2025), <https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/>.
 - 15 Ashhurst Perkins Coie, "Security Breach Notification Chart," (Sept. 2025), <https://www.ashurstperkinscoie.com/en/insights/publication/security-breach-notification-chart/>.
 - 16 "Complaint for Injunctive and Other Relief," *Arizona ex. rel. Mayes v. Meta Platforms, Inc.*, U.S. District Court for the Northern District of California No. 4:23-cv-05448 (Oct. 24, 2023), [https://www.nj.gov/oag/newsreleases23/2023-1024_Meta-Multistate-Federal-Complaint-\(N.D.-Cal.\)-FINAL-REDACTED.pdf](https://www.nj.gov/oag/newsreleases23/2023-1024_Meta-Multistate-Federal-Complaint-(N.D.-Cal.)-FINAL-REDACTED.pdf).
 - 17 "Complaint," *People v. Tiktok, Inc.*, Supreme Court of the State of New York No. 452749/2024 (Oct. 7, 2024), https://ag.ny.gov/sites/default/files/court-filings/3_redacted_complaint_signed-003.pdf.
 - 18 Justia, "Consumer Protection Laws: 50-State Survey," (Oct. 2023), <https://www.justia.com/consumer/consumer-protection-laws-50-state-survey/>.
 - 19 The National Consumer Law Center, "Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws, Appendix C," (March 1, 2018), <https://www.nclc.org/wp-content/uploads/2022/08/udap-appC-1.pdf>.
 - 20 "Complaint," *Equal Rights Center v. Meta Platforms, Inc.*, Superior Court of the District of Columbia No. 2025-CAB-000814 (Feb. 11, 2025), <https://equalrightscenter.org/wp-content/uploads/2025.02.11-1-complaint.pdf>.
 - 21 Ariel Fox Johnson, "From Dolls to Downloads: Courts Reimagine Product Liability for the Digital Age," *Tech Policy Press* (June 12, 2025), <https://www.techpolicy.press/from-dolls-to-downloads-courts-reimagine-product-liability-for-the-digital-age/>.
 - 22 "Order re Motions to Certify Interlocutory Appeal" *In re Soc. Media Adolescent Addiction/Personal Injury Products Liability Litigation*, U.S. District Court for the Northern District of California No. 4:22-md-3047-YGR (March 11, 2025), https://www.bloomberglaw.com/public/desktop/document/INRESOCIALMEDIAADOLESCENTADDICTIONPERSONALINJURYPRODUCTSLIABILITY/13?doc_id=X445LSM1R8L975844C4DL6KJ5G9.

they more closely reflect the norms and preferences of local communities, as they are often the product of community organizing and local advocacy.²³

There are opportunities to expand the work being done at the state level to protect against technology's greatest risks and the harms most likely to impact communities of color. By adopting disparate impact protections and codifying the application of public accommodations law to digital contexts, existing antidiscrimination protections are strengthened.²⁴ State law provides a promising opportunity in this moment, as many of these laws include private rights of action that allow individual residents to directly hold companies accountable in court.

As powerful as state laws are, we also need stronger federal civil rights tools to protect Black communities and other communities of color from the harms of emerging technology.

The Artificial Intelligence Civil Rights Act,²⁵ currently before Congress, provides a workable framework for regulating the use of AI for consequential decisions with strong anti-discrimination language, a robust auditing framework, and transparency requirements for companies.^{26, 27} Yet, instead of passing common-sense measures like the AI Civil Rights Act, in the past year, the federal government has repeatedly attempted to block any state law protections that might apply to AI without even offering federal regulation to fill the resulting void.^{28, 29, 30, 31, 32, 33} This comes after years of failed attempts to pass a comprehensive federal privacy law that would establish transparency requirements and provide basic consumer rights.^{34, 35}



23 The Institute for Family Studies, “New Poll Shows Americans Overwhelmingly Oppose Federal Preemption of State AI Regulations,” (Nov. 21, 2025), <https://ifstudies.org/press-release/new-poll-shows-americans-overwhelmingly-oppose-federal-preemption-of-state-ai-regulations>.

24 David Brody & Sean Bickford, “Discriminatory Denial of Service: Applying State Public Accommodations Laws to Online Commerce,” *The Lawyers’ Committee for Civil Rights Under Law* (Jan. 2020), <https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf>.

25 The Lawyers’ Committee for Civil Rights Under Law, “AI Civil Rights Act,” (2025), <https://www.lawyerscommittee.org/ai-civil-rights-act/>.

26 Office of Senator Ed Markey, “Senator Markey Introduces AI Civil Rights Act to Eliminate AI Bias, Enact Guardrails on Use of Algorithms in Decisions Impacting People’s Rights, Civil Liberties, and Livelihoods,” (Sept. 24, 2024), <https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-ai-civil-rights-act-to-eliminate-ai-bias-enact-guardrails-on-use-of-algorithms-in-decisions-impacting-peoples-rights-civil-liberties-livelihoods>.

27 Jo Gasior-Kavishe, “AI Is Infringing on Your Civil Rights. Here’s How We Can Stop That,” *The American Civil Liberties Union* (Dec. 3, 2025), <https://www.aclu.org/news/racial-justice/ai-is-infringing-on-your-civil-rights-heres-how-we-can-stop-that>.

28 Julia Shapero, “State Lawmakers Press Congress on Plan to Preempt AI Laws,” *The Hill* (Nov. 24, 2025), <https://thehill.com/policy/technology/5620185-lawmakers-oppose-federal-ai-preemption/>.

29 Donald J. Trump, “Executive Order 14365: Ensuring a National Policy Framework for Artificial Intelligence,” *Executive Office of the President* (Dec. 11, 2025), <https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence>.

30 Yiqin Fu and Alasdair Phillips-Robins, “When Should Congress Preempt State AI Law? The Lessons of Past Technologies,” *The Carnegie Endowment for International Peace* (Sept. 9, 2025), <https://carnegieendowment.org/research/2025/09/congress-preempt-state-ai-law-the-lessons-of-past-technologies>.

31 Jule Pattison-Gordon, “Are Efforts to Pre-empt State AI Regulation Actually Dead?,” *Governing* (Aug. 18, 2025), <https://www.governing.com/artificial-intelligence/are-efforts-to-pre-empt-state-ai-regulation-actually-dead>.

32 J.B. Branch, “Federal Preemption of State AI Laws Is Dangerous and Reckless,” *Public Citizen* (May 21, 2025), <https://www.citizen.org/article/federal-preemption-of-state-ai-laws-is-dangerous-and-reckless/>.

33 Yasmin Abusaif, “Congress Shouldn’t Stop States from Regulating AI — Especially with No Alternative,” *The Brennan Center for Justice* (July 1, 2025), <https://www.brennancenter.org/our-work/analysis-opinion/congress-shouldnt-stop-states-regulating-ai-especially-no-alternative>.

34 Robert Gellman, “Is There Any Way Forward for Privacy Legislation in the United States?,” *Tech Policy Press* (July 30, 2025), <https://www.techpolicy.press/is-there-any-way-forward-for-privacy-legislation-in-the-united-states/>.

35 Jessica Rich, “After 20 Years of Debate, It’s Time for Congress to Finally Pass a Baseline Privacy Law,” *Brookings* (Jan. 14, 2021), <https://www.brookings.edu/articles/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/>.

While state laws are a key component of tech accountability, we also need robust federal laws to protect our communities across the nation. We need a multifaceted approach to regulating novel technologies, one that reinforces civil rights protections and that empowers communities of color to demand representation in design and accountability for harm.

One of the nation's foremost experts in civil rights litigation and policy, Damon T. Hewitt has more than 20 years of experience, including prior leadership roles in the nonprofit, philanthropic, and public sectors. Prior to joining the Lawyers' Committee, he was the inaugural executive director of the Executives' Alliance for Boys and Men of Color and was the chief liaison from the philanthropic community to the White House on policy issues impacting young men of color. Hewitt previously worked for more than a decade as an attorney at the NAACP Legal Defense and Educational Fund. Hewitt joined the Lawyers' Committee as Executive Vice President in 2019 and was named its President and Executive Director in 2021. Since then, he has led the organization to victories on a range of critical issues, including affirmative action, race-conscious programs, and diversity, equity and inclusion; election protection and voter disinformation; redistricting; fair housing; algorithmic bias and AI; and police accountability. Hewitt's work has been widely cited in a number of news outlets, including the New York Times, The Washington Post, The Guardian, Bloomberg News, CNN, MSNBC, NBC, and CBS. He holds a B.A. in Political Science from Louisiana State University and a J.D. from the University of Pennsylvania Law School.





OUR TECH, OUR FUTURE: HOW TO BUILD A TECH INDUSTRY ACCOUNTABLE TO *We the People*



Bots and Ballot Boxes:

What Today's Technology Means for Voters and Our Democracy

Alejandra Montoya-Boyer

Vice President, the Center for Civil Rights and Technology
The Leadership Conference on Civil and Human Rights

The threats AI presents to elections are neither new nor unexpected. Bad actors have used social media platforms to influence U.S. elections for over a decade, using dishonest and manipulative content to spread lies, sow hate, and encourage suspicion of our neighbors. Even as advocates have spent years raising alarms, the problems persist. This is not a matter of ignorance — major tech companies have acknowledged the proliferation of disinformation on their platforms^{1,2,3} — but of willingness to make effective changes.

Not only have platforms failed to pursue meaningful improvements, they have *backtracked*, abandoning key elements of content moderation. In recent years, some have shifted away from traditional moderation and fact-checking by professionals to community notes that rely on volunteers. Community notes are ineffective in addressing election falsehoods: they are too slow, have limited reach, and don't effectively refute lies.⁴ These failings are particularly dangerous when election falsehoods are part of a strategic disinformation campaign meant to sow distrust.

Not only is it imperative that the companies making and using AI technologies take responsibility for the threats AI poses to elections, it is in their best interests to do so.

Injecting AI, which can reproduce and personalize content at a massive scale, into the current content moderation landscape will further weaken trust in our elections:

AI makes it harder to tell what is true. As more of the internet has become AI-generated, people have grown increasingly skeptical of online information. In the first quarter of 2026, an estimated 49.9% of articles published online were AI-generated.⁵ An information ecosystem in which *half* of new text is produced by error-prone algorithms is not reputable. The sheer volume of AI-generated content online, on top of the chatbots' improving ability to mimic human writing, is making it progressively difficult to know what to trust.

1 Nathaniel Gleicher, "Coordinated Inauthentic Behavior," *Meta Newsroom* (July 8, 2020), <https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/>.

2 Vanessa Pappas, "Combating Misinformation and Election Interference on TikTok," *TikTok Newsroom* (Aug. 5, 2020), <https://newsroom.tiktok.com/combating-misinformation-and-election-interference-on-tiktok>.

3 , "Expanding our Politics to Further Protect the Civic Conversation," *X Blog* (Sept. 10, 2020) https://blog.x.com/en_us/topics/company/2020/civic-integrity-policy-update.

4 Center for Countering Digital Hate, "Rated Not Helpful: How X's Community Notes System Falls Short on Misleading Election Claims," (Oct. 30, 2024), <https://counterhate.com/research/rated-not-helpful-x-community-notes/>.

5 Greg Druck, "AI Now Writes as Many Online Articles as Humans," *Graphite.io* (May 15, 2026), <https://graphite.io/five-percent/ai-now-writes-as-many-online-articles-as-humans-do>

In this environment, platforms could develop a trustworthy reputation by increasing the visibility of accurate, helpful information. But instead, some of the most influential social media platforms have retreated, leaving the choice of which information to highlight up to opaque algorithms that reward engagement over truth. Some platforms have even *deprioritized* official sources by making verification status available to anyone who pays for it.

AI content moderation allows dangerous content. AI is hastening platforms' retreat from traditional content moderation by enabling them to replace human moderators with algorithms. Even as companies tout efficiency, replacing human content moderators results in worse moderation.⁶ Automated content moderators miss context and subtext that humans catch — the practice of replacing letters, words, and even phrases specifically to evade automated moderation is widespread on social media. AI moderation is even worse in languages besides English: since large language models (LLMs) are trained on content written by humans, AI is worse at moderating content in other languages.⁷

AI makes it easy to generate fake content. AI is a dangerously powerful tool for bad actors seeking to disrupt elections. Creating fake content used to be labor intensive; now, AI makes it easy. AI-generated or manipulated images, audio, and video can create a narrative out of thin air: a bad actor could easily make a fake audio clip of an election official rigging results or a deepfake video of a governor announcing last-minute voting changes. Something as simple as an AI-generated image of ICE agents at the polls could damage people's confidence that they and their neighbors can vote safely.

Another serious concern is how easily AI can make fake versions of official websites. A cloned version of a secretary of state's website could easily spread false voting information, and a clone of a local news site could corroborate it. A voter trying to verify a rumor could be presented with seemingly incontrovertible evidence that the lie was true.

AI makes lies travel faster and further. Beyond using AI to fake evidence, a bad actor can use AI to spread election lies faster and more efficiently. Crafting targeted political messaging for specific communities, which used to require significant time and expertise, can now be accomplished in minutes: an AI chatbot could generate an election influence strategy, write social media content, identify hyper-specific audiences, and customize content. AI agents could even autonomously purchase ads and use bots to mimic engagement. The result is a disinformation machine that is faster, cheaper, and more convincing than ever.

AI makes cyber attacks easy. One of the areas in which AI is most capable is software engineering. Even someone with no technical background could "vibe code" malware to attack election infrastructure. An attack could be as simple as phishing an election administrator with an official-seeming email, or as complex hacking voting machines. An attack wouldn't even need to break laws: AI agents could disable official communications by overwhelming phone lines or email servers.

These threats are not insurmountable. Until there are comprehensive, civil-rights-protective federal AI safeguards, there are steps tech companies can take to ensure our elections are safe and accessible for all:

- 1. Promote verified, legitimate sources of information**, and ensure that an account's verification status (or lack thereof) is blatantly obvious.
- 2. Down-rank accounts with a history of spreading election lies.** Terminate repeat offender accounts.
- 3. Invest in professional human content moderation.** Neither AI nor crowd-sourced models can replace the judgment, context-awareness, and cultural competency that professionals bring to the job.

• • • • •

6 Adi Levi, Or Levina, Sardhendu Mishra, and Jonathan Morra, "AI vs. Human Moderators: A Comparative Evaluation of Multimodal LLMs in Content Moderation for Brand Safety," *ArXiv* (Aug. 7, 2025), <https://arxiv.org/html/2508.05527v1#S5/>.

7 Gabriel Nicholas and Aliya Bhatia, "The Dire Defect of 'Multilingual' AI Content Moderation." *WIRED* (May 23, 2023), <https://www.wired.com/story/content-moderation-language-artificial-intelligence/>.

4. Do not integrate AI generation and content modification capabilities into advertising systems.

5. Label all AI-generated and AI-modified content. Do not allow users to remove content provenance information from election-related content.

6. Publicly and repeatedly acknowledge the threats AI poses to voters and election officials. Include this warning in all AI products.

7. Actively support election officials. Provide cybersecurity resources, multi-factor authentication, and AI literacy and anti-phishing training to election officials, and help them build rapid-response infrastructure.

8. Discourage the use of consumer platforms for internal election administration communications. Election officials should not coordinate sensitive matters over social media.

Some in the industry may view these as burdens. They are investments. User trust, once lost, cannot be recovered via press release. People are deeply skeptical of both AI and the companies creating it: Pew reports that in 2025, 50% of Americans are concerned about increased use of AI in daily life, up from 37% in 2021,⁸ and our own polling indicates 68% of Hispanic Americans, 62% of Asian Americans, and 60% of Black Americans agree that AI is a threat to democracy.⁹ The companies that take these concerns seriously and make AI as safe as possible will earn loyalty that no marketing budget can buy.

Another point to consider is that AI regulation is coming: 80% of Americans support rules for AI safety and data security, even if it means developing AI capabilities at a slower rate.¹⁰ Very few issues in this country are as bipartisanship popular as protecting people from harmful AI. When that regulation comes, companies that are already investing in AI safety and responsibility will be far ahead of those that are rushing to comply. It should also be said that despite the current administration's stance, disparate impact liability — the legal concept that entities can be held responsible for *unintentional* discrimination against marginalized groups — remains the law of the land. Future administrations may not be as welcoming to those who violate it.¹¹

Both our elections and our *faith* that our votes matters have long been under attack. Without safeguards, AI is a powerful tool to further those attacks. It is time for AI companies to be accountable for their role in our democracy, the foundation for their business and its success.

An environment in which voters no longer believe their ballots count is not an environment under which innovation can thrive. This moment calls for leadership — and history will remember who stepped up, and who stepped aside.

Alejandra Montoya-Boyer is the Vice President of the Center for Civil Rights and Technology, where she focuses on research, policy solutions, and advocacy that responds to the growing opportunities and challenges from AI and emerging technologies and their impact on marginalized communities. Previously, Alejandra was the Director of Policy at Prosperity Now and has also worked at the National Association of Counties (NACo), the Bill & Melinda Gates Foundation, the Joint Center for Political and Economic Studies, and the Office of Ben Ray Luján (NM-03). She has a diverse background in policy, political campaigning, grassroots advocacy, and program management with deep content expertise in workforce development, tech policy, economic justice, and racial equity.

8 Brian Kennedy, Eileen Yam, Emma Kikuchi, Isabelle Pula, and Javier Fuentes, "How Americans View AI and its Impact on People and Society," Pew Research (Sept. 17, 2025), <https://www.pewresearch.org/science/2025/09/17/how-americans-view-ai-and-its-impact-on-people-and-society/>.

9 Cornell Belcher, "Leadership Conference Civil Rights Monitor," *The Leadership Conference on Civil and Human Rights* (Nov. 2025), <https://civilrights.org/edfund/resource/2025-civil-rights-monitor/>.

10 Benedict Vigers and Justin Lall, "Americans Prioritize AI Safety and Data Security," *Gallup* (Sept. 17, 2025), <https://news.gallup.com/poll/694685/americans-prioritize-safety-data-security.aspx>.

11 Chiraag Baines, "When Machines Discriminate: The Critical Role of Disparate Impact Liability in AI Accountability," *The Center for Civil Rights and Technology at The Leadership Conference for Civil and Human Rights* (Jan. 22, 2026), <https://civilrights.org/disperate-impact-ai/>.



1620 L Street NW, Suite 1100
Washington, DC 20036



(202) 466-3434



techcenter@civilrights.org



civilrights.org/value/center-civil-rights-technology/



@civilandhumanrights



@civilrightsorg



@civilrightsorg.bsky.social

OUR TECH, OUR FUTURE:

HOW TO BUILD
A TECH INDUSTRY
ACCOUNTABLE TO

We the People

Copyright © 2026

The Leadership Conference

Center for Civil Rights and Technology

All Rights Reserved

