STATEMENT OF

Cody Venzke

Senior Policy Counsel

National Political Advocacy Division

American Civil Liberties Union

For a Hearing on

"Artificial Intelligence and Criminal Exploitation: A New Era of Risk"

Before the

United States House of Representatives

House Judiciary Committee

Subcommittee on Crime and Federal Government Surveillance

July 16, 2025

Chairman Biggs, Ranking Member McBath, and members of the Subcommittee: Thank you for the opportunity to testify today on behalf of the American Civil Liberties Union (ACLU) regarding the risks posed by the rapidly advancing frontier of artificial intelligence (AI). The risk posed by malicious actors' use of artificial intelligence is real. The increasing prevalence of AI in our lives is accompanied by corresponding potential for harm. However, it is crucial that our response to those risks be consistent with civil rights and civil liberties. Likewise, Congress should ensure that the legislation it passes and the actions of the Administration do not open the door for malicious actors to abuse AI. Congress has already stepped up in this regard, ensuring that a "moratorium" on state regulation of AI was not included in the recent reconciliation package.

In addition to the threats posed by malicious actors, governmental use of AI carries concomitant risks. As with the private sector, governmental use of AI is pervasive, cutting across federal law enforcement, governmental benefits, and national security. Although some use cases may make governmental programs and services more effective and more efficient, the risks AI poses in this domain may, in some instances, be even more significant and consequential than those that arise from malicious actors outside the government. Indeed, as President Trump recognized during his first term, federal use of AI must "foster[] public trust and confidence while protecting privacy, civil rights, civil liberties, and American values."[1]

This statement addresses five issues:

- Congress should ensure that efforts to address malicious uses of artificial intelligence comport with civil rights and civil liberties
- Current rollbacks of AI safeguards threaten safety, civil rights and civil liberties
- AI is being deployed across governmental programs, including federal law enforcement, without adequate safeguards, and in some places, in violation of existing statutory or regulatory safeguards on governmental use of data collected on individuals
- The revised Office of Management and Budget Memorandum is an important milestone for safe, effective governmental AI, but key shortcomings should be addressed
- Congress should address the civil rights impacts of artificial intelligence in traditionally protected sectors

---

[1] Exec. Order No. 13960 of December 3, 2020, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 Fed. Reg. 78939 (Dec. 8, 2020); *see also* Exec. Order No. 13859 of February 11, 2019, "Maintaining American Leadership in Artificial Intelligence," 84 Fed. Reg. 3967 (Feb. 14, 2019) (recognizing that federal uses of AI mut protect "economic and national security, civil liberties, privacy, and American values").

I. Congress Should Ensure that Efforts to Address Malicious Uses of Artificial Intelligence Comport with Civil Rights and Civil Liberties

As Congress contemplates measures to address the use of AI in criminal, malicious, or fraudulent activity, it must ensure that those measures comport with basic Constitutional precepts of due process, privacy, civil rights, and civil liberties. This means protecting "open" AI to the extent possible, respecting the use of AI in First Amendment activities, and minimizing surveillance.

Preserving AI "Openness": Recent concerns have focused on how "open" AI might contribute to AI misuse.[2] "Openness" in AI is a gradient, encompassing a broad range of formats, from the availability of downloadable models to publicly available model weights and fully "open" models with publicly available code, weights, and data.[3] Consequently, "openness" should always be discussed with reference to the components of the AI system that are being made widely available — such as the model weights, architecture or coding, or training data. Each degree of openness may further civil rights goals of transparency and explainability, especially when bolstered by additional protections as necessary.

As others have observed, "Widely available model weights enable external researchers, auditors, and journalists to investigate and scrutinize foundation models more deeply," including to assess harms to marginalized communities, by better understanding the relationship among the parameters evaluated by the model, especially in the context of sample data used to derive the weights.[4] Additional degrees of "openness" can further goals around transparency and accountability.

Relatedly, there is little evidence to show that "open" AI systems meaningfully increase risks of harms from AI.[5] Consequently, policymakers should resist impulses to cut off the development of "open" AI systems that do not appreciably increase AI risks.

Protecting First Amendment Activities: Similarly, as generative AI raises new concerns, policymakers should be cognizant that traditional First Amendment activities do not lose their protections simply because a new tool such as artificial

---

[2] *See* National Telecommunications & Information Administration, Dual-Use Foundation Models with Widely Available Model Weights Report (2024), https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report [hereinafter "NTIA Report"].
[3] David Gray Widder et al., *Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI*, SSRN at 4 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4543807.
[4] Sayash Kapoor et al., *On the Societal Impact of Open Foundation Models*, arXiv at 4-5 (2024), https://arxiv.org/abs/2403.07918.
[5] NTIA Report at 36-37.

intelligence was used.[6] Thus, editorial content moderation using AI and algorithmic systems is not categorically exempted from First Amendment protections.[7] And critically, neither is commentary on politicians or candidates for office.[8]

Speech about politicians and candidates lies at the heart of the First Amendment and enjoys special protection.[9] The Supreme Court has emphasized, "Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution."[10] Consequently, "The First Amendment affords the broadest protection to such political expression in order 'to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'"[11]

Courts have readily overturned laws proscribing false speech about politicians and candidates, including on grounds that the laws are content discriminatory and that they lack narrow tailoring.[12]

For example, one court overturned a law punishing "derogatory" political speech, stating, "Under this statute, speakers may lie with impunity about businesspeople, celebrities, purely private citizens, or even government officials so long as the victim is not currently a" candidate.[13] "That is textbook content discrimination," subject to the highest levels of First Amendment scrutiny.[14] Laws seeking to limit AI-generated speech about politicians and candidates will likely raise the same concerns.

Of course, defamation, fraud, and child sexual abuse material are well-recognized exceptions to the First Amendment that apply equally to speech generated using AI, but many "deepfake" proposals extend beyond the traditional bounds of those

---

[6] *Cf.* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 793 (2011); Anderson v. City of Hermosa Beach, 621 F.3d 1051, 1061–62 (9th Cir. 2010).
[7] Moody v. NetChoice, 603 U.S. 707, 731-742 (2024).
[8] Kohls v. Bonta, 752 F. Supp. 3d 1187, 1193 (E.D. Cal. 2024).
[9] Grimmett v. Freeman, 59 F.4th 689, 695 & n.8 (4th Cir. 2023).
[10] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995).
[11] *Id.* (quoting Buckley v. Valeo, 424 U.S. 1, 14–15 (1976)); *accord* Roth v. United States, 354 U.S. 476, 484 (1957).
[12] Grimmett v. Freeman, 59 F.4th 689, 694 (4th Cir. 2023); Susan B. Anthony List v. Ohio Elections Comm'n, 45 F. Supp. 3d 765, 775 (S.D. Ohio 2014), aff'd sub nom. Susan B. Anthony List v. Driehaus, 814 F.3d 466 (6th Cir. 2016) ("While knowingly false speech may be an element of fraud or defamation, false political speech by itself does not implicate 'important private interests.' . . . As a result, knowingly false political speech does not fall entirely outside of First Amendment protection, and any attempt to limit such speech is a content-based restriction, subject to close review."); *accord* 281 Care Comm. v. Arneson, 766 F.3d 774 (8th Cir. 2014); *see also* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 57 (1988); New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964).
[13] Grimmett v. Freeman, 59 F.4th 689, 694 (4th Cir. 2023)
[14] *Id.*

exceptions or selectively regulate political speech.[15] Such proposals are likely to trigger rigorous judicial review.

Minimizing Surveillance: Finally, in efforts to mitigate criminal uses of AI, policymakers may consider imposing obligations on platforms that host and distribute AI models, weights, and tools. In considering that approach, policymakers should be cognizant of users' privacy rights. Privacy concerns may be triggered by requirements or incentives to search users' communications, monitor their online activity, restrict their publication of models, code, and data, report their activity to federal agencies, or to prohibit or undermine encryption. Those requirements undoubtedly increase governmental surveillance of private parties and, in some circumstances, may violate the Fourth Amendment.[16]

II. Current Rollbacks of AI Safeguards Threaten Safety, Civil Rights and Civil Liberties

Despite the concern about criminal uses of AI, some efforts by the Administration and Congress may either exacerbate those harms or hamper efforts to address them, including on matters within this Committee's jurisdiction.

a. A Federal Moratorium on State Regulation of AI Would Exacerbate the Risk of AI Harms

First, the ten-year "moratorium" that was included in earlier drafts of the recently enacted reconciliation package would have dramatically increased the risk of harms by artificial intelligence, including by criminal and fraudulent activity. The "moratorium" was publicly opposed by key members of both parties in the House, as well as by 17 Republican governors, before being defeated 99-1 in the Senate. The defeat of the moratorium underscored a bipartisan understanding that excluding states from AI regulation would be simply handing a blank check to bad actors.

Because some supporters of a moratorium have stated their goal of finding another legislative vehicle to enact a moratorium during this Congress, it is important for this Committee to understand the dangers of a moratorium in its various iterations. One component of the House reconciliation package would have imposed a ten-year "moratorium" on enforcement of state or local laws regulating AI. The moratorium was sweeping, affecting laws "regulating artificial intelligence models, artificial intelligence systems, or automated decision systems." Although the moratorium included limited exceptions for some state and local laws, serious questions arose

---

[15] United States v. Alvarez, 567 U.S. 709, 719 (2012) (false speech within traditional exceptions to the First Amendment may be regulated).
[16] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010);

about the scope of those exceptions. In particular, the draft passed by the House would not have exempted laws unless it met three requirements:[17]

- The law's purpose is to remove AI barriers or use AI to streamline zoning, licensing, or similar activities;
- The law does not impose "any substantive design, performance, data-handling, documentation, civil liability" or other obligations on AI unless it is a "generally applicable" law that applies to all technology evenly; "and"
- The law does not impose a fee or bond unless the fee or bond is reasonable and applies to all technology evenly.

The requirements were conjunctive, meaning a law would be exempted *only* if it satisfied all three. Few laws would have been able to meet that bar. Further, even after Senate redrafting clarified the relationship among these prongs, serious questions persisted over what laws *exactly* qualify as "generally applicable."

Those are serious questions and ambiguities that even further refined drafting will not be able to resolve. For example, dozens of states have passed laws regulating nonconsensual intimate imagery (NCII) created by generative AI, often by simply amending an existing NCII statute to clarify that it applies to images created with generative AI.[18] It is not clear if such laws, which specify their application to generative AI, qualify as "generally applicable." Similarly, Tennessee's ELVIS Act amends its existing right of publicity statute to extend to a person's "voice" — a concern that has risen in prominence due to AI voice-cloning technology.[19] The definition of "voice" specifically encompasses a "simulation." Although the amendment does not specify any type of AI technology, its intent to address emerging AI technology is clear.

Moreover, in many instances, addressing AI's harms requires legislating specifically on AI. Establishment of an AI moratorium will jeopardize these efforts, giving bad

---

[17] Cody Venzke et al., *Expert Perspectives on 10-Year Moratorium on Enforcement of US State AI Laws*, Tech Policy Press (May 23, 2025), https://www.techpolicy.press/expert-perspectives-on-10-year-moratorium-on-enforcement-of-us-state-ai-laws.

[18] *E.g.*, 84 Del. Laws ch. 479 (2024) (HB 353), https://legis.delaware.gov/BillDetail?LegislationId=141103; Md. Laws ch. 219 (2024) (SB 360E), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0360?ys=2025RS; N.Y. Laws Ch. 513 (2023) (S1042A), https://www.nysenate.gov/legislation/bills/2023/S1042/amendment/A; N.Y. Laws Ch. 58, part MM, subpart A, sec. 3 (2024) (A8808), https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A08808&term=2023&Summary=Y&Actions=Y&Text=Y;

[19] Tenn. Pub. Ch. No. 588 (2024) (HB 2091), https://publications.tnsosfiles.com/acts/113/pub/pc0588.pdf; Sy Damle et al, *The ELVIS Act: Tennessee Shakes Up Its Right of Publicity Law and Takes On Generative AI*, Latham & Watkins Client Alert (Apr. 8, 2024), https://www.lw.com/en/offices/admin/upload/SiteAttachments/The-ELVIS-Act-Tennessee-Shakes-Up-Its-Right-of-Publicity-Law-and-Takes-On-Generative-AI.pdf.

actors a blank check. Recognizing this, Congress stripped the moratorium from the reconciliation package in a 99-1 vote in the Senate. This Committee should oppose any renewed efforts to try to enact a moratorium preempting state laws.

b. Consolidation of Federal Databases Will Require Facilitation by Artificial Intelligence and Raises Questions About Compliance with Legal Requirements

The Administration's efforts to consolidate federal data also pose risk of AI harms, including supercharged domestic surveillance. On March 20, 2025, President Trump issued Executive Order 14243, titled "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos."[20] The Executive Order directs federal agencies to facilitate the sharing and consolidation of agency records, with the stated goal of combating waste and fraud. However, the broad and unregulated access to sensitive data not only violates privacy obligations but also risks the creation of a database that contains a single, searchable profile of every American, without transparency or clear legal limits. And while data consolidation and sharing could potentially improve certain government operations in limited circumstances, it must be done in a way that does not elevate efficiency over robust privacy protection. Otherwise, this could risk the eventual creation of a vast and unaccountable surveillance system capable of tracking every citizen's activities, movements, and associations, readily analyzable by large language models, machine learning, and other AI systems.

Implementation of the Executive Order raises significant concerns about compliance with legal restrictions on federal and state data. For example, the Privacy Act of 1974,[21] prohibits disclosure of records from any federal agency's "system of records," including to other agencies. The law includes a variety of exceptions, such as disclosures to agency employees for "performance of their duties" and for "routine uses" that are compatible with the original purpose of collection and published in the Federal Register. Similarly, the Social Security Act requires states participating in Medicaid to develop plans to ensure that Medicaid data is disclosed only for four purposes "directly related to the administration" of the Medicaid program:[22] (1) establishing eligibility; (2) determining the amount of medical assistance; (3) providing services for beneficiaries; and (4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan. Broad-based sharing and consolidation of federal records defies those restrictions.

---

[20] Exec. Order No. 14243 of March 20, 2025, 90 Fed. Reg. 13681 (Mar. 25, 2025).
[21] 5 U.S.C. § 552a.
[22] 42 U.S.C. § 1396a(a)(7) (requiring the state plan to limit disclosures to those "directly connected with administration" of the state plan); 42 C.F.R. § 431.301–02.

A similar program was pursued by the Department of Defense in the early 2000s. The Total Information Awareness (TIA) program was designed to mine vast amounts of personal data from a variety of sources, including commercial databases, travel records, and financial transactions, in the name of national security. This program was loudly criticized across the political spectrum, and in response to efforts led by Senator Wyden and with the support of Senator Grassley, Congress halted funding for TIA. Mission creep made even a purportedly limited database a serious threat to civil rights and civil liberties. As Senator Grassley observed then: "Like many people, I have been concerned that this program could be used to invade the privacy of Americans by snooping around in our bank accounts, personal Internet computers, phone records and the like."[23]

Senator Grassley ultimately concluded in opposing the program: "Without appropriate oversight and accountability standards, Total Information Awareness could infringe on [Constitutional] rights. Snooping around by the feds cannot go unchecked."[24] More than 20 years later, the new threat is from a potentially far more expansive and invasive program.

Building a centralized system for federal data, as envisioned under the Executive Order, creates similar risks, and threatens to create a single point of vulnerability where personal information could be exploited for improper surveillance or wrongful government action. Functionally this data consolidation will enable centralized dossiers on nearly everyone in the United States that would leap over the firewalls around agency data that prevent misuse and abuse.

Consolidating such data could lead to biometric information gathered by one law enforcement agency, or during air travel, being merged with or easily accessible to other law enforcement agencies, and the reverse could also be true. Records related to firearms, maintained by federal firearms licensees, the FBI, or the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), might be reviewed by other federal entities, potentially to assess eligibility for government programs such as Social Security or Medicare — and the FBI and ATF could similarly access Social Security and Medicare records, including medical files. Likewise, IRS data reflecting contributions to organizations like the ACLU, NAACP, NRA, or the Heritage Foundation could become accessible to law enforcement.

Such broad data sharing risks violating well-established privacy safeguards, and it is essential for Congress to actively monitor these practices and ensure that these

---

[23] Declan McCullagh, *Republican Senator Slams Database Plan*, CNET (Jan. 22, 2003), https://www.cnet.com/tech/services-and-software/republican-senator-slams-database-plan/.
[24] Sen. Chuck Grassley, *Pentagon Snoops Need Congressional Leash* (Jan. 31, 2003), https://www.grassley.senate.gov/news/news-releases/pentagon-snoops-need-congressional-leash.

privacy laws are upheld while blocking the creation of a centralized government dossier on nearly every individual in this country. Because significant amounts of federal data are being shared with components of the Departments of Justice and Homeland Security under this Committee's jurisdiction, the Committee has oversight authority to ensure that data sharing is not being used to build a centralized surveillance platform. If necessary, this Committee can — and should — consider legislation to limit agencies' collection, purchase, use, and consolidation of data.

c. Directives to Deploy AI, Including in Hiring, Raise Serious Concerns About Safety and Civil Rights

Efforts across the government to implement AI at a breakneck pace could mean that federal AI outstrips nascent safeguards, such as the "risk management practice" developed by the Office of Management and Budget (OMB).[25]

For example, the President directed the Assistant to the President for Domestic Policy and the Office of Personnel Management, in conjunction with OMB and the Department of Government Efficiency (DOGE), to develop a "Federal Hiring Plan."[26] The hiring plan was directed to "integrate modern technology to support the recruitment and selection process" of federal employees.[27] The subsequent Federal Hiring Plan directs agencies to adopt skills-based assessments and "rigorous candidate ranking."[28] Although the Hiring Plan contemplates use of validated assessments through USA Hire, it also permits use of "agency-developed and off-the-shelf assessments."[29] Under the plan and OPM's forthcoming "rule of many," agencies will be able to set "cut scores" for their assessment, based on analysis data, business necessity, or set numbers or percentages of applicants.[30] We fear these measures will lead to unproven products like gamified assessments, automated video interviews, and chatbots.[31] These technologies have been repeatedly demonstrated to lead to discriminatory harms, and many workers have reported that today's digital-application platforms are particularly confusing,

---

[25] OMB's safeguards for federal uses of AI are discussed in Section IV of this statement.
[26] Exec. Order No. 14170 of January 20, 2025, 90 Fed. Reg. 8621 (Jan. 30, 2025).
[27] *Id.* sec. 2(b)(vi)
[28] Vince Haley & Charles Ezell, Memorandum to Heads and Acting Heads of Departments and Agencies at 7 (May 29, 2025), https://chcoc.gov/sites/default/files/Merit%20Hiring%20Plan%205-29-2025%20FINAL.pdf.
[29] *Id.* at 17.
[30] *Id.* at 7.
[31] Olga Akselrod & Ricardo Mimbela, *The Long History of Discrimination in Job Hiring Assessments*, ACLU (May 30, 2024), https://www.aclu.org/news/racial-justice/the-long-history-of-discrimination-in-job-hiring-assessments.

inaccessible, and opaque.[32] Without safeguards, this influence will translate directly into real world harms.

Moreover, DOGE appears to be actively deploying AI across federal agencies, potentially without adhering to safeguards for federal uses of AI, such as OMB's risk management practices. For example, AI has been deployed at the federal Department of Education,[33] with access to grant and financial information, resulting in "a massive firehose of data being sent to [an] AI company's servers."[34] Similarly, data analytics and AI company Palantir has been contracted to build a portal to make highly protected IRS data available across the federal government.[35] This rapid deployment raises the risk that AI is being used without sufficient safeguards. This Committee should exercise its oversight authority, including by holding hearings if warranted, to determine how AI is being applied in agencies within the Committee's jurisdiction.

III. AI Is Being Deployed Across Governmental Programs, Including Federal Law Enforcement

In addition to being cognizant of the harms that may stem from criminal exploitation of AI, the Committee should use its jurisdiction to investigate and address harms that may arise from the government's own use of artificial intelligence in governmental benefits and administration, federal law enforcement, and national security.

a. Federal Law Enforcement

Artificial intelligence has become commonplace in federal law enforcement. The uses of AI in law enforcement are diverse, ranging from facial recognition technology to algorithmic decision-making and predictive policing. Despite the multiplicity of use cases across law enforcement, AI consistently undermines due process protections and poses threats to the public trust by exacerbating existing

---

[32] Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, ACLU (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.
[33] Hannah Natanson, *Elon Musk's DOGE Is Feeding Sensitive Federal Data Into AI to Target Cuts*, Washington Post (Feb. 6, 2025), https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education.
[34] *Ranking Member Connolly Demands Answers After Reports DOGE is Feeding Americans' Private Data Into Unapproved AI Systems, Using AI to Slash Programs*, House Committee on Oversight and Government Reform Democrats (Mar. 12, 2025), https://oversightdemocrats.house.gov/news/press-releases/ranking-member-connolly-demands-answers-after-reports-doge-feeding-americans.
[35] Makena Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, Wired (Apr. 11, 2025), https://www.wired.com/story/palantir-doge-irs-mega-api-data/.

disparities, operating without transparency, and being deployed without adequate auditing or risk mitigation.

i. Facial recognition technology

One example of such a tool is facial recognition technology (FRT). The ACLU has consistently taken the position that the use of face recognition technology poses serious threats to civil liberties and civil rights, making it dangerous both when it fails and when it functions.[36] Accordingly, the ACLU has repeatedly called for a federal moratorium on the use of facial recognition by federal law enforcement.[37]

The use of FRT is pervasive. For example, the Chairman of this Subcommittee recently sought information from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) on ATF's use of FRT to identify gun owners.[38] As Chairman Biggs noted, the use of FRT by federal agencies, including ATF, is marred by a lack of oversight and transparency, as federal agencies failed to systematically track their use of FRT systems. Often, federal use of FRT was not accompanied by established guidance or policies addressing civil rights and civil liberties.

Similarly, the Federal Bureau of Investigation has closely tied FRT to its larger domestic surveillance apparatus. The FBI employs facial recognition technology in intelligence gathering and national security contexts, including identifying individuals connected to open assessments — preliminary investigations that don't require any suspicion of wrongdoing — as long as they serve a recognized purpose such as preventing crime or terrorism.[39]

---

[36] ACLU, Re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e)), (Jan. 19, 2024), https://perma.cc/3FLB-Q54Z. ACLU, Response to U.S. Commission on Civil Rights Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology (April 8, 2024) https://www.aclu.org/wp-content/uploads/2024/04/ACLU-Comment-to-USCCR-re-FRT-4.8.2024.pdf.

[37] More than 20 jurisdictions — including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont — have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particular privacy-destroying system built on a database of tens of billions of non-consensually collected faceprints.

[38] Letter from Hon. Andy Biggs, Chairman, Subcommittee on Crime and Federal Government Surveillance, & Warren Davidson, Member of Congress, to Hon. Kash Patel, Acting Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives (Mar. 27, 2025), https://biggs.house.gov/sites/evo-subsites/biggs.house.gov/files/evo-media-document/biggs-letter-to-atf-acting-director-patel-re-atf-improper-facial-recognition-technology.pdf.

[39] House Oversight and Reform Committee: Facial Recognition Technology - Ensuring Transparency in Government Use (June 4, 2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, FBI), https://perma.cc/H56E-MUN3; U.S. Senate AI

This lack of oversight and transparency poses significant risks to civil rights and civil liberties. As an initial matter, facial recognition technology is often unreliable and frequently produces possible matches that are incorrect.[40] Even in best case scenarios, these systems are not designed to deliver definitive identifications. Instead, they generate what is essentially an "algorithmic best guess" of who a person might be, which often results in incorrect matches.[41] A variety of factors influence how accurate facial recognition technology is, including how the algorithm was trained, the composition of the image database it is matched against, and characteristics of the input image, such as the lighting, angle, and image quality.[42]

The most troubling issue is that facial recognition technology systems consistently demonstrate disproportionately high error rates when applied to people of color and women, compared to white men.[43] Related technologies that analyze faces to assign genders to a face can disproportionately fail for gender non-conforming individuals.[44] Efforts to test and improve the accuracy of facial recognition technology above some threshold rest on extremely shaky ground because current FRT accuracy tests do not reflect real-world conditions or the human factors in FRT use.

As explained in a 2022 report from the Georgetown Center on Privacy and Technology, existing FRT accuracy tests do not control for the many variables characterizing real-world law enforcement uses of FRT.[45] A study designed to assess accuracy rates of FRT algorithms *as actually used in police investigations* would need to account for both algorithmic and human factors in the FRT search process, as well as the tremendous variability in the quality of probe images, which often feature low resolution, poor lighting, and other deficiencies. But existing studies do not do so. For example, real-world uses of FRT searches will present dozens or

---

Insight Forum: National Security (Dec. 6, 2023) (statement of Patrick Toomey, Deputy Director, National Security Project, ACLU), https://perma.cc/C34K-8ECW.

[40] Because FRT systems conducting one-to-many searches are generally configured to produce multiple possible matches, even when the algorithm identifies a true match, it will also necessarily generate numerous false matches.

[41] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, The New Yorker (Nov. 13, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence; *see also Facial Recognition: Current Capabilities, Future Prospects, and Governance*, Nat'l Acad of Scis. at 48-49 (2024), https://perma.cc/K7PR-AJAS.

[42] *Facial Recognition: Current Capabilities, Future Prospects, and Governance* at 47.

[43] *Id*. at 24, 56–57.

[44] Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, ACM Digital Library (2019), https://dl.acm.org/doi/10.1145/3359246.

[45] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. on Privacy & Tech at 15-16 (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

hundreds of potential matches for a probe image;[46] human investigators must sift through the raft of potential matches to select leads for further investigation. As demonstrated by the known cases of misidentifications leading to wrongful arrests, that human review process is prone to error.[47]

Other human and technical factors further exacerbate the risk inherent in FRT. The probe image may be pixelated, grainy, taken from an angle, or with facial features obscured,[48] in contrast with the more ideal conditions used in laboratory tests. Humans must also select a similarity threshold for the FRT algorithm, which establishes cut-off of similarity for images in the dataset compared to the probe image. Choosing a lower threshold will lower the risk of missing a true match while raising the risk of overwhelming the examiner with false matches; a higher threshold will lower the number of false positives that are provided but increase the chance of missing a true match, which may have outsized impacts on different demographic groups.[49]

Predictably, police reliance on this technology has led to a number of wrongful arrests across the country.[50] Reflecting the demographic disparities in false-match rates from the technology, most of the people known to have been wrongfully arrested due to police reliance on incorrect FRT results are Black. This includes the ACLU's former client Robert Williams, who was wrongfully arrested by Detroit police in 2020 after police relied on an incorrect FRT result in a shoplifting investigation. But everyone is at risk. Just last year, a white Florida resident was wrongfully arrested after an incorrect FRT result led police in a city 300 miles from

---

[46] Dep. of Jennifer Coulson at 29, Williams v. City of Detroit, No. 21-cv-10827 (E.D. Mich.), ECF No. 60-2 (Michigan State Police analyst explaining that candidate list included 486 images generated by the FRT search).

[47] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. On Privacy & Tech. at 22-24 (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations ("A wealth of psychology research demonstrates that overall, humans are not innately good at identifying unfamiliar faces."); *Facial Recognition: Current Capabilities, Future Prospects, and Governance*, Nat'l Acad. of Scis. At 61-63, 83-84 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[48] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Geo. L. Ctr. on Privacy & Tech. (May 16, 2019), https://www.flawedfacedata.com.

[49] K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* 3, IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (2019), https://arxiv.org/abs/1904.07325 ("A specified FMR [false match rate] is usually realized by different threshold values relative to the African-American and the Caucasian impostor distributions.").

[50] *See* Douglas MacMillan, David Ovalle & Aaron Schaffer, *Arrested by AI: Police Ignore Standards after Facial Recognition Matches*, Wash. Post (Jan. 13, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition.

his home to charge him with luring or enticing a child.[51] Although police eventually admitted that the FRT result was wrong, it was too late to prevent the harms of being falsely accused of a reviled crime and held in jail.

Despite these significant shortcomings, facial recognition technology used by government agencies is on the rise. Most known deployments involve attempting to match individuals to still images or identifying them in photographs, often in criminal investigations. However, the prospect of continuous video surveillance using facial recognition is becoming more real, especially as federal agencies responsible for national and homeland security increasingly explore and adopt AI-powered facial recognition tools.[52]

Although use of FRT to identify or track people through real-time or stored video feeds has long remained taboo in American policing,[53] a recent Washington Post investigation revealed that the New Orleans Police Department has been secretly relying on a network of live FRT cameras that send real-time alerts to officers' phones when the cameras detect a purported match to someone on a privately assembled watch list.[54] In addition to critical risks of misidentifications and wrongful arrests from continuous untargeted FRT use, deploying FRT on a network of surveillance cameras enables automatic tracking of huge numbers of people as they go about their daily lives, raising acute constitutional concerns. Such surveillance threatens to chill the exercise of rights protected by the First Amendment, including the freedoms of speech, association, and of the press.

---

[51] Evan Dean, *AI Leads to Wrongful Arrest of Lee County Man*, Gulf Coast News (Feb. 11, 2025), https://www.gulfcoastnewsnow.com/article/ai-leads-to-wrongful-arrest-of-lee-county-man/63745255.

[52] See, e.g., ACLU, Comment re: DHS Information Collection Request (Dec. 6, 2021), https://www.aclu.org/documents/aclu-comment-dhs-st-information-collection-request-facial-recognition-and-artificial; see also GAO, Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections (GAO-22-106100) (June 29, 2022), https://perma.cc/9APH-CPUU (indicating that DOD, DHS, DOJ, and DOS had reported using facial recognition technology for national security and defense related purposes). Section 5708 of the FY2020 National Defense Authorization Act mandated that the Director of National Intelligence submit a report on the use of facial recognition technology. This report has never been made public despite it being required to have been submitted in an unclassified form.

[53] Even in jurisdictions that allow use of FRT to attempt to identify images of unknown suspects, continuous video FRT surveillance is prohibited. *See, e.g.*, Miami Police Dep't, Departmental Order 16, Chapter 4: Facial Recognition Technology, § 4.5.2(d), ("Facial recognition technology . . . shall not be used for . . . [m]onitoring persons in real time."); Detroit Police Dep't, Directive No. 307.5: Facial Recognition, § 3.2 ("Members shall not use Facial Recognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source."); Mont. Code Ann. § 44-15-104; Mass. Gen. Laws. Ann. ch. 6, § 220(a); Va. Code § 52-4.5(D); L.A. Cnty. Regional Identification System, Facial Recognition Policy ¶ E (Sept 1, 2021); Orlando Police Dep't Policy & Procedure 1147.2, Facial Recognition § 5.3 (June 6, 2022).

[54] Douglas MacMillan & Aaron Schaffer, *Police secretly monitored New Orleans with facial recognition cameras,* The Washington Post (May 19, 2025), https://www.washingtonpost.com/business/2025/05/19/live-facial-recognition-police-new-orleans/.

Further, the U.S. Supreme Court has made clear that using digital-age technologies to conduct pervasive surveillance of people's locations and movements implicates the Fourth Amendment.[55] A system that scans every face that passes by enables dangerous dragnet surveillance that is simply incompatible with our expectations in a free society.

And consequently, the ACLU continues to urge this Committee and Congress to enact a federal moratorium on the use of this technology in law enforcement, due to its inherent risk for civil rights and civil liberties. As an important step towards such a moratorium, we urge this Committee to schedule an oversight hearing on the use of facial recognition technology, and other AI, by federal law enforcement.

ii. Algorithmic Decision-Making & "Predictive Policing"

Law enforcement and the criminal legal systems also rely on algorithmic systems to make decisions about individuals or where to allocate policing resources. So-called "predictive policing" relies on technology that includes tools that are built using a wide array of inputs, including historical crime data, which are used to "to help decide where to deploy police" (place-based) or "to identify individuals who are purportedly more likely to commit or be a victim of a crime" (person-based).[56] Both person-based and place-based predictive policing tools raise serious civil rights and civil liberties concerns,[57] which arise in part due to the data used to build those systems.

To build these systems, developers generally train algorithms using datasets that may include historical crime data amassed by police departments over the course of many years, sometimes decades.[58] Those data sets reflect existing disparities in police practices, such as over-policing of Black and Brown communities. Alarmingly, some police departments train predictive systems on information collected from unlawful practices, such as arrest records legally mandated to be sealed. Building

---

[55] Carpenter v. United States, 585 U.S. 296 (2018).
[56] Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[57] *See, e.g.*, Kristian Lum & William Isaac, *To Predict and Serve?*, Royal Stat. Soc. (2016), https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x; Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, Procs. of Machine Learning Rsch. (2018), https://proceedings.mlr.press/v81/ensign18a/ensign18a.pdf; Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. Rev. (2019), https://nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/.
[58] *See* Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

models off data that inherently contain bias results in biased tools creates a feedback loop that serves to further oppress Black and brown communities.

Several examples of flawed predictive systems stand out:

- **PATTERN:** The PATTERN risk assessment developed by the U.S. Department of Justice is used to inform programming and release decisions for individuals incarcerated in federal facilities. PATTERN scores can be calculated by adding up whole numbers based on roughly a dozen pieces of information about a person, and these scores may be calculated using paper-based forms or processes.[59] While a tool like PATTERN may appear to be simple, the tool was developed using statistical modeling techniques, including "machine learning boosted regression procedures,"[60] and it is used in ways that, like seemingly more complex AI systems, raise serious concerns about transparency, accuracy, and fairness.[61] These concerns arise from how PATTERN purported to measure likelihood of recidivism, which it based on data regarding likelihood of *rearrest*.[62] That distinction is critical. Overwhelming research has demonstrated that arrest is more reliably a measure of policing practices and priorities than actual crime, making arrest a racially-biased proxy for recidivism.[63] For example, when it comes to traffic stops — the most common form of interaction between police and the public — study after study has demonstrated that police engage in persistent racial discrimination when conducting stops, frisks, searches and arrests.[64]

---

[59] *See* Federal Bureau of Prisons, *PATTERN Risk Assessment,* https://www.bop.gov/inmates/fsa/pattern.jsp (last visited November 27, 2023).
[60] *See 2021 Review and Revalidation of the First Step Act Risk Assessment Tool*, National Institute of Justice at 16 (2021), https://nij.ojp.gov/library/publications/2021-review-and-revalidation-first-step-act-risk-assessment-tool.
[61] *See Formal Statement of the American Civil Liberties Union For a Stakeholder Engagement Session on First Step Act Implementation*, ACLU (Sept. 27, 2022), https://www.aclu.org/wp-content/uploads/document/ACLU_PATTERN_Public_Comment.pdf; Coalition Letter on the Use of PATTERN Risk Assessment in Prioritizing Release in Response to the COVID-19 Pandemic, ACLU (April 3, 2020), https://www.aclu.org/letter/coalition-letter-use-pattern-risk-assessmentprioritizing-release-response-covid-19-pandemic; ACLU, Comment Letter to Department of Justice on PATTERN First Step Act (Sept. 3, 2019), https://civilrights.org/resource/comment-letter-to-department-of-justice-on-pattern-first-step-act/.
[62] U.S. Department of Justice, 2021 Review and Revalidation of the First Step Act Risk Assessment Tool, available at https://nij.ojp.gov/library/publications/2021review-and-revalidation-first-step-act-risk-assessment-tool (December 2021).
[63] *See, e.g.,* American Civil Liberties Union, *A Tale of Two Countries: Racially Targeted Arrests in the Era of Marijuana Reform*, ACLU (2020), https://www.aclu.org/publications/tale-two-countries-racially-targeted-arrests-era-marijuana-reform; Lum & Isaac, *To Predict and Serve*, In Detail (2018), https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2016.00960.x.
[64] *See* Baumgartner et al., *Targeting young men of color for search and arrest during traffic stops: evidence from North Carolina*, Politics, Groups, and Identities (2016), https://fbaum.unc.edu/articles/PGI-2016-Targeting.pdf; Pierson et al., *A large-scale analysis of racial*

Moreover, a large percentage of arrests do not result in convictions.[65] Taken together, this evidence suggests multiple, fundamental issues with using rearrests as a proxy for recidivism.

- **Patternizr:** The New York City Police Department (NYPD) has been using millions of sealed arrest records in more than a dozen interconnected technologies including one predictive policing tool known as Patternizr.[66] Patternizr is a machine-learning model created by the NYPD that is trained on complaint and arrest reports that were generated between 2006 and 2015.[67] The corpus of data used to train Patternizr includes sealed records[68] and data from the height of the NYPD stop-and-frisk program, which targeted Black and Latino people and was ruled unconstitutional.[69] Hundreds of thousands of people stopped under that racially biased program were arrested,[70] often on specious allegations later dismissed, thus creating records that may well populate Patternizr. Querying Patternizr by submitting a new crime complaint will return additional, purportedly related complaints,[71] effectively suggesting specific individuals for detectives to investigate — meaning a person might find themselves suspected of a crime based solely on Patternizr's selection of their sealed arrest record in response to a detective's query. A class action filed by the Bronx Defenders challenging the NYPD's use of sealed arrest records — including in Patternizr — as a contravention of New York law is ongoing.[72]
- **Geolitica:** Geolitica (formerly known as PredPol) is a leading place-based predictive policing company that purports to help officers identify high-priority areas for patrol.[73] Those recommendations, however, reflect existing disparities in policing practices and create a feedback loop that will perpetuate them. As computer scientist Suresh Venkatasubramanian succinctly stated, "If you build predictive policing, you are essentially sending

---

disparities in police stops across the United States, Nature Human Behavior (2020); https://www.nature.com/articles/s41562-020-0858-1.

[65] For a discussion of the data from various jurisdictions about what percentage of arrests result in convictions, see Ames Grawert, *Brennan Center's Public Comment on the First Step Act's Risk and Needs Assessment Tool*, Brennan Center for Justice (2019); https://www.brennancenter.org/our-work/research-reports/brennan-centers-public-comment-first-step-acts-risk-and-needs-assessment.

[66] *See id*. *See also*, *R.C. v. City of New York*, No. 153739/2018, 2021 WL 4427369 (N.Y. Sup. Ct. Sept. 27, 2021) (granting preliminary injunction).

[67] Alex Chohals-Wood & E.S. Levine, *A Recommendation Engine to Aid in Identifying Crime Patterns* (Mar. 29, 2019), https://nparikh.org/assets/pdf/sipa6545/week10-police/policing/nypd-patternizr.pdf.

[68] *See* Complaint at 2, *R.C. v. City of New York*, 153739/2018 (N.Y. Sup. Ct. Apr. 4, 2018).

[69] *Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[70] *See id*. at 573.

[71] *Id*. at 6–8.

[72] *Id*.

[73] *Data-Driven Community Policing*, Geolitica (2023), https://geolitica.com/public-safety.

> police to certain neighborhoods based on what they told you — but that also means you're not sending police to other neighborhoods because the system didn't tell you to go there. . . If you assume that the data collection for your system is generated by police whom you sent to certain neighborhoods, then essentially your model is controlling the next round of data you get."[74]

Predictive policing tools are necessarily built on top of historical data—and the history of policing is a deeply racist one.[75] Historical crime data is not an objective history of all crime: it does not capture unreported crime, officer discretion in investigations and arrests, or the series of racist decisions that lead to a conviction in some cases and not others. Analyzing police behavior and crime data have revealed racial disparities in every stage of the criminal process.[76] To paint the picture, a Black person is more than twice as likely to be arrested than a white person, and five times more likely to be stopped without cause than a white person.[77] AI trained on that history will undoubtedly replicate it, exacerbating and automating discriminatory harms.

While many of the studies of the harms caused by AI in "predictive policing" have focused on harms related to race, the increasing use of machine learning and "black box" AI could very well mean that it becomes increasingly difficult to understand what factors the systems are relying on.[78] Consequently, there is no reason to believe that AI in predictive policing can be applied fairly and accurately, even in contexts unrelated to race. Models might rely on factors ranging from gun

---

[74] Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, Vice (Feb. 14, 2019), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed.

[75] *See* Connie Hassett-Walker, *The Racist Roots of American Policing: From Slave Patrols to Traffic Stops*, The Conversation (June 2, 2020), https://theconversation.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops-112816.

[76] Ezekiel Edwards, *Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime*, ACLU (Aug. 31, 2016), https://www.aclu.org/news/criminal-law-reform/predictive-policing-software-more-accurate ("Time and again, analysis of stops, frisks, searches, arrests, pretrial detentions, convictions, and sentencing reveal differential treatment of people of color. From racial bias in stops and frisks in New York, Boston, and Baltimore, to unwarranted disparities nationwide in arrests of Blacks and whites for marijuana possession (despite comparable usage rates), to disparities in the enforcement of minor offenses in Minneapolis, New Jersey, and Florida, as sure as the sun rises police will continue to enforce laws selectively against communities of color.").

[77] Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice.

[78] Dominic Weiss, *Inhuman Reason: Predictive Policing Algorithms and the Fourth Amendment*, ABA Criminal Justice Magazine (Jan. 30, 2025), https://www.americanbar.org/groups/criminal_justice/resources/magazine/2025-winter/predictive-policing-algorithms-fourth-amendment/.

ownership to marital status — or simply being the victim of a crime[79] — could similarly result in the wrongful targeting of police resources based on a machine's guess of who might commit a crime. At its core, predictive policing is inconsistent with due process.

b. Governmental Benefits and Administration

AI is actively being deployed in basic governmental operations. These AI systems affect everything from governmental benefits to child welfare programs and public housing:

- **Medicaid:** Idaho's Department of Health and Welfare was employing algorithmic systems to determine benefits for federally funded Medicaid programs.[80] Although the system cut some individuals' benefits by as much as 30 percent, officials were unable to explain why determinations were reached, and litigation by ACLU of Idaho revealed that the system was implemented without meaningful safeguards. The algorithmic system was implemented without notice, and the State of Idaho and its private vendor attempted to hide its functioning behind trade secrets claims.[81] The ACLU of Idaho eventually prevailed in court and learned that Idaho's system was "a set of formulas in a fairly basic Microsoft Excel spreadsheet," which computed each person's benefits in "hidden cells," leaving state officials unable to explain how or why it reached its benefits determinations.[82] Despite its outsized impact on individuals' rights, Idaho's algorithmic system lacked critical safeguards, based on underlying models that "Department staff had just brainstormed," but "never validated, standardized, or audited the instrument."[83]
- **Allegheny Family Screening Tool:** An ACLU and Human Rights Data Analysis Group audit of an algorithmic risk-scoring system used to inform child welfare decision-making in Allegheny County, Pennsylvania highlighted several ways in which the algorithm's design and deployment could enable algorithmic bias.[84] The risk-scoring system could potentially

---

[79] J. Justin Wilson, *Case Closed: Pasco Sheriff Admits "Predictive Policing" Program Violated Constitution*, Institute for Justice (Dec. 4, 2024), https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution.
[80] Testimony of Ritchie Eppink, Hearing AI in Government Before the S. Comm. On Homeland Security & Government Affairs (May 16, 2023), https://www.hsgac.senate.gov/hearings/artificial-intelligence-in-government.
[81] *Id.* at 3.
[82] *Id.*
[83] *Id.*
[84] Marissa Gerchick et al., *How Policy Hidden in an Algorithm is Threatening Families in This Pennsylvania County*, ACLU (Mar. 14, 2023), https://www.aclu.org/news/womens-rights/how-policy-hidden-in-an-algorithm-is-threatening-families-in-this-pennsylvania-county; Marissa Gerchick et al.,

disproportionately flag Black families and families with disabilities for investigation. The audit highlighted the system's use of existing government databases, including county child welfare, juvenile probation, and behavioral health records. Problematically, those databases reflect the lives of those who have more contact with government agencies and systems shaped by historical and ongoing discrimination — not necessarily those who pose greater "risk" to their children. Additionally, the outcome the tool predicts is the risk of child removal by the County, based on its historical practices. Because government databases, including those regarding child removal statistics, reflect systems shaped by historical and ongoing discrimination, using them to identify the characteristics of households more likely to have a child removed means selecting from a pool of factors that over-represents some groups of people and underrepresents others.

- **Tenant Screening:** "[C]rime-fighting grants" provided through the U.S. Department of Housing and Urban Development have been used by local housing authorities to deploy AI-powered surveillance.[85] For example, in "rural Scott County, Va., cameras equipped with facial recognition [technology] scan everyone who walks past them, looking for people barred from public housing."[86] Numerous other uses of facial recognition and similar technology in federally funded housing have been well documented.[87] Likewise, public housing authorities may rely on algorithmically driven tenant screening, including criminal background checks used as a prerequisite for public housing, often with discriminatory effects on over-policed populations.[88]

The Devil is in the Details: Interrogating Values Embedded in the Allegheny Family Screening Tool, ACLU (2023), https://www.aclu.org/the-devil-is-in-the-details-interrogating-values-embedded-in-the-allegheny-family-screening-tool. Allegheny County and its Department of Human Services receive federal funds. *DHS Funding*, Allegheny County (2023), https://www.alleghenycounty.us/Human-Services/About/Funding-Sources.aspx; *County Of Allegheny*, TAGGS (2023), https://taggs.hhs.gov/Detail/RecipDetail?arg_EntityId=swAAHUn5jiXXGX5RfqF%2Fmg%3D%3D.

[85] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, Washington Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing.

[86] *Id.*

[87] *Id.*; Dan Bateyko, *Taken for Granted: Where's the Oversight of AI and Federal Funding?*, CDT (Aug. 7, 2023), https://cdt.org/insights/taken-for-granted-wheres-the-oversight-of-ai-and-federal-funding.

[88] DeMetria McCain, Principal Deputy Assistant Secretary for Fair Housing and Equal Opportunity, U.S. Department of Housing and Urban Development, Memorandum on Implementation of the Office of General Counsel's Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions 2 (June 10, 2022), https://www.hud.gov/program_offices/fair_housing_equal_opp/fheo_guidance ("[H]ousing providers sometimes utilize third-party companies to independently screen and reject applicants using algorithms that may contain racial or other prohibited bias in their design."); *see* Comments of the

The potential risks posed by these systems to public trust, safety, privacy, civil rights, and civil liberties can be commensurate to the risks posed by exploitative or malicious uses of AI.

c. National Security

Over four years ago, the National Security Commission on Artificial Intelligence (NSCAI) issued a sweeping report that made clear U.S. intelligence agencies like the NSA, CIA, FBI, and others are pursuing "ubiquitous AI integration in each stage of the intelligence lifecycle."[89] Intelligence agencies are seeking to use AI to help select surveillance targets, identify people whose communications are intercepted, and analyze the vast amounts of data they collect.[90] Despite transparency commitments by ODNI and the agencies it oversees, the public knows little about how these AI applications are impacting people in the United States. For example, the National Security Agency has used AI "for a very long time" to support its intelligence-gathering activities, and today it is one of many spy agencies seeking to integrate AI across its activities.[91] AI may be used at the NSA for selecting targets for intelligence,[92] monitoring social media,[93] risk assessments, and watch listing.[94]

IV. The Revised Office of Management and Budget Memorandum Is an Important Milestone for Safe, Effective Governmental AI, But Key Shortcomings Should Be Addressed

Initial efforts to address the potential harms from federal uses of AI are underway. Under the Trump Administration, the Office of Management and Budget (OMB) revised crucial guidance for federal agencies' use of AI to ensure American leadership in both AI innovation and AI effectiveness, trustworthiness, and safety. This guidance, Memorandum M-25-21,[95] is built on principles of transparency and

---

ACLU, Tenant Screening Request for Information, Docket No. FTC-2023-0024 (May 30, 2023), https://www.aclu.org/wp-content/uploads/2023/07/2023.05.30-ACLU-Comment-to-FTC-CFPB-Tenant-Screening-RFI.pdf (describing private uses of algorithmic tenant screening).

[89] NSCAI Final Report at 110, https://perma.cc/FQ5H-ZGEH.

[90] *Id.* at 108–10, 143–45.

[91] *GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT*, NSA (Sep. 21, 2023), https://perma.cc/97GE-4ULZ.

[92] *See* NSCAI Final Report at 109, 112.

[93] Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, VICE (May 17, 2023), https://www.vice.com/en/article/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees/.

[94] DHS, *Artificial Use Case Inventory—Customs and Border Protection*: *Port of Entry Risk Assessments*, https://perma.cc/RCP2-VZWJ (last visited June 13, 2024); DHS, *2020–2021 Data Mining Report*, DHS at 26 (2022), https://perma.cc/9K6P-GUHG.

[95] Memorandum for the Heads of Executive Offices and Agencies, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," M-25-21 (Apr. 3, 2025),

American values, including protecting civil rights and civil liberties, established by Executive Orders and legislation during the first Trump Administration.

During his first term, President Trump directed that "[a]gencies must [] design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, civil liberties, and American values."[96] OMB expounded on those principles in an earlier memorandum to direct agencies to "consider in a transparent manner the impacts that AI applications may have on discrimination."[97] In the same memorandum, OMB recognized that "transparency and disclosure can increase public trust and confidence in AI applications" and that disclosures "should be written in a format that is easy for the public to understand and may include identifying when AI is in use."[98]

Ultimately, Congress enshrined these principles of public trust, transparency, civil rights, and civil liberties into law. The Advancing American AI Act mandates that each agency "prepare and maintain an inventory of the artificial intelligence use cases of the agency."[99] Similarly, the AI in Government Act of 2020 required OMB to provide guidance on identifying "best practices for identifying, assessing, and mitigating any discriminatory impact or bias on the basis of any classification protected under Federal nondiscrimination laws, or any unintended consequence of the use of artificial intelligence."[100]

a. Key Provisions of M-25-21 Will Help Ensure Federal AI Is Safe, Trustworthy, and Protective of Civil Rights and Civil Liberties

Memorandum M-25-21 is the latest iteration of efforts to foster public trust in federal uses of AI. Several key strengths of the Memorandum will help ensure that federal AI is safe, trustworthy, and protective of civil rights and civil liberties:

- **Public Use Case Inventories:** Transparency around federal uses of AI was foundational for AI policy during the first Trump administration. OMB's

---

https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf [hereinafter Memorandum M-25-21].

[96] Exec. Order No. 13960 of December 3, 2020, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 Fed. Reg. 78939 (Dec. 8, 2020); *see also.* Exec. Order No. 13859 of February 11, 2019, "Maintaining American Leadership in Artificial Intelligence," 84 Fed. Reg. 3967 (Feb. 14, 2019) (recognizing that federal uses of AI mut protect "economic and national security, civil liberties, privacy, and American values").

[97] Memorandum for the Heads of Executive Offices and Agencies, "Guidance for Regulation of Artificial Intelligence Applications," M-21-06, sec. 7 (Nov. 17, 2020) [hereinafter M-21-06].

[98] *Id.*, sec. 8.

[99] Advancing American AI Act, Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, sec. 7225, 136 Stat. 2395, 3672 (2022), https://www.congress.gov/bill/117th-congress/house-bill/7776/text.

[100] AI in Government Act of 2020, Pub. L. No. 116-260, div. U, tit. I, sec. 104(a)(3), 134 Stat. 1182, 2287 (2020), https://www.govinfo.gov/content/pkg/PLAW-116publ260/pdf/PLAW-116publ260.pdf.

2020 Memorandum on AI emphasized that "the continued adoption and acceptance of AI will depend significantly on public trust and validation," and consequently urged agencies to prioritize public participation and to provide information to the public on agencies' uses of AI.[101] Similarly, President Trump's 2020 Executive Order on artificial intelligence established the first framework for AI use-case inventories,[102] a requirement that was later incorporated into the Advancing American AI Act.[103] Memorandum M-25-21 preserves many key components of the public use case inventories by requiring agencies to publicly document each "use case" of AI,[104] including compliance with the Memorandum's risk management practices.[105]

- **Robust Risk Management Practices:** The core of Memorandum M-25-21 is a series of "risk management practices" to mitigate risks posed by certain "high-impact" uses of AI.[106] Crucially, these risk management practices include pre-deployment testing that reflects "expected real-world outcomes" and conducting AI impact assessments.[107] The impact assessments must address the quality and appropriateness of the AI system's data and capability, potential impacts on privacy, civil rights, and civil liberties, and the result of an independent review.[108] The AI must be monitored for adverse impacts throughout its life cycle, including functions that "may violate laws governing privacy, civil rights, or civil liberties."[109]
- **Broad Scope of "High-Impact" AI:** The Memorandum's core "risk management practices" apply to "high-impact" AI. "High-impact" AI is any AI that "serves as a principal basis for decisions or actions with legal, material, binding, or significant effect" on key areas of life: "civil rights, civil liberties, or privacy"; "access to education, housing, insurance, credit, employment, and other programs"; "access to critical government resources or services"; "human health and safety"; "critical infrastructure or public safety"; or "strategic assets or resources," including classified information.[110] Any AI that meets that definition must comply with the risk management practices

---

[101] M-21-06, secs. 1-2.
[102] Exec. Order No. 13960, sec. 5.
[103] Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, sec. 7225, 136 Stat. 2395, 3672 (2022), https://www.congress.gov/bill/117th-congress/house-bill/7776/text.
[104] Memorandum M-25-21, sec. 3(b)(v). As described below, the Department of Defense and the intelligence community are exempt from providing public AI use case inventories.
[105] *Id.* sec. 4(a)(i).
[106] Memorandum M-25-21, sec. 4(b).
[107] *Id.* sec. 4(b)(i).
[108] *Id.* sec. 4(b)(ii), (B), (C), (F).
[109] *Id.* sec. 4(b)(iii).
[110] Memorandum M-25-21, sec. 5.

unless an exception applies. In addition, several uses are *presumed* to be high-impact and subject to the risk management practices, including:[111]

- blocking, removing, hiding, or limiting the reach of protected speech;
- using risk assessments and facial recognition in law enforcement;
- adjudicating requests for critical federal services, processes, and benefits, including loans and access to public housing, continued
- eligibility benefits; and,
- determining the terms of employment.

- **AI Under Human Oversight:** The Memorandum appropriately recognizes that although AI may not independently make decisions or fully automate a task, it may nonetheless be "a principal basis" for consequential decisions or actions that carry risks to rights and safety. For example, the Memorandum recognizes that AI may be "high-impact" "whether there is or is not human oversight for the decision or action."[112] Similarly, the Memorandum emphasizes that "risks" arising from AI may occur whether "the AI merely informs the decision or action, partially automates it, or fully automates it."[113] This approach corresponds to how AI is actually used in practice, where AI often works in tandem with human decision-makers, rather than fully replacing them.

  For example, one law enforcement agency used an algorithmic systems to predict who was likely to predict future crimes,[114] including by drawing grades and abuse histories from the local school district's education records.[115] That algorithmic score was based not just on individuals' own criminal records, but merely being suspected of a crime, serving as a witness to a crime, or being a victim of a crime.[116] Officers then used the algorithmic output to identify individuals for harassment, seeking "to get them to move away or go to prison," including by getting more than a dozen individuals evicted from their homes.[117] Although humans made the ultimate decisions,

---

[111] *Id.* sec. 6.
[112] Memorandum M-25-21, sec. 4(a).
[113] Memorandum M-25-21, sec. 7.
[114] J. Justin Wilson, *Case Closed: Pasco Sheriff Admits "Predictive Policing" Program Violated Constitution*, Institute for Justice (Dec. 4, 2024), https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution.
[115] Neil Bedi & Kathleen McGrory, *Pasco's Sheriff Uses Grades and Abuse Histories to Label Schoolchildren Potential Criminals*, Tampa Bay Times (Nov. 19, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data.
[116] *Florida Parents Partner with IJ to Shut Down Dystopian "Predictive Policing" Program*, Institute for Justice (Mar. 10, 2021), https://ij.org/case/pasco-predictive-policing.
[117] Bedi & McGrory, *supra* note 115.

the algorithm's output was crucial to causing the harm, placing individuals in the crosshairs for governmental abuse.

Similarly, one predictive model used in colleges and universities evaluates individual students' likelihood of academic success and assigns them a corresponding "risk score." One investigation found the model's risk scores correlated with students' race, and in some cases, expressly incorporated it as a "high-impact predictor."[118] Academic advisors often review students' risk scores, and although the model did not independently make decisions about students, its scores might nonetheless "leave advisers with an immediate and potentially life-changing impression of students and their prospects within a given major."[119] Although AI did not make the final determination, its influence was significant, and the OMB Memorandum covers such scenarios.

b. Memorandum M-25-21 May Be Strengthened by Addressing Critical Shortcomings

Despite its strengths, the OMB Memorandum includes broad carveouts that threaten its efficacy in protecting the public's trust. As Congress and the Administration continue to improve governance of federal uses of AI, four key shortcomings should be addressed, either through legislation or working directly with OMB:

- **Bolstering Use Case Inventories:** The use case inventories may be further strengthened:
    - A previous iteration of the Memorandum required agencies to "*individually* inventory" each use case,[120] a requirement that was removed from Memorandum M-25-21. Individual documentation increases transparency, as it helps ensure that the public is aware of each AI system and avoids risks that crucial AI use cases would be obscured in aggregate reporting.
    - Further, the previous iteration of the Memorandum required that agencies not subject to the *individual* reporting requirement "still report and release aggregate metrics about such use cases that are otherwise within the scope of this memorandum, the number of such cases that impact rights and safety, and their compliance with" the

---

[118] Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, The Markup (Mar. 2, 2021), https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.
[119] *Id.*
[120] Memorandum for the Heads of Executive Offices and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," M-24-10, sec. 3(a)(iv) (Mar. 28, 2024) (emphasis added) [hereinafter M-24-10].

Memorandum's risk management practices.[121] Aggregate reporting achieved at least some balance between the purported need for confidentiality around military or intelligence AI uses and the need for transparency.

  - Finally, OMB has not yet publicly released its instrument for agencies to report use cases, but reporting suggests that the updated instrument will no longer gather crucial information. Omissions include whether notice is provided to individuals, whether there is human oversight or an option for opt-out, and if systems have disparate impact on protected classes.[122] Although neither version of the Memorandum required protections such as notice or opt-out in every instance,[123] collating the availability of those rights is crucial for both Congressional and public oversight.

- **Failure to Include State-Administered Federal Programs:** The Memorandum currently applies only to federal agencies—namely, any "executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch," with a few enumerated exceptions.[124] The scope of Memorandum at the federal level is appropriately broad, reflecting the broad use of AI across the federal government. However, the Memorandum excludes state and local programs receiving federal assistance; this will leave many particularly dangerous uses of AI unregulated, and OMB, the Administration, and Congress should take steps to expand the scope of the memorandum's applicability to federally funded programs. The exclusion of federally funded programs is particularly pernicious because federal funds may help support uses of AI with significant impacts on rights and safety, such as the Allegheny Family Screening Tool described above or AI technologies procured with Department of Justice grants.[125]

---

[121] M-24-10, sec. 3(a)(v).
[122] Madison Alder & Rebecca Heilweil, *Trump White House Issues Internal Federal Guidance on AI Reporting*, FedScoop (July 1, 2025), https://fedscoop.com/trump-white-house-issues-internal-federal-guidance-on-ai-reporting.
[123] M-24-10, sec. 5(c)(v)(B), (F) (opt-out required "where practicable and consistent with applicable law and governmentwide guidance"); M-25-21, sec. 4(b)(vi)-(vii) (requiring human review, appeal, and feedback mechanisms "where appropriate").
[124] *See* 44 U.S.C. § 3502(1).
[125] Brandon Block, *Federal Aid Is Supercharging Local WA Police Surveillance Tech*, Crosscut Cascade PBS (July 26, 2023), https://crosscut.com/investigations/2023/07/federal-aid-supercharging-local-wa-police-surveillance-tech; Chris Baumohl, *Two Years In, COVID-19 Relief Money Fueling Rise of Police Surveillance*, EPIC (Mar. 9, 2023), https://epic.org/two-years-in-covid-19-relief-money-fueling-rise-of-police-surveillance; Anastasia Valeeva, Wihua Li & Susie Cagle, *Rifles, Tasers and Jails: How Cities and States Spent Billions of COVID-19 Relief*, The Marshall Project (Sept. 7, 2022), https://www.themarshallproject.org/2022/09/07/how-federal-covid-relief-flows-to-the-criminal-justice-

- **Carveouts for National Security and Law Enforcement:** The Memorandum contains several carveouts for national security, defense, and law enforcement. The Advancing American AI Act codifies some of these exceptions for the intelligence community and the Department of Defense.[126] But the Memorandum itself establishes an *additional* exception for "national security systems,"[127] which can include systems involving intelligence activities, cryptologic activities, and "command and control of military forces," among other things.[128] As described above, these use cases can impose some of the most significant risks to civil rights and civil liberties, and their wholesale exemption from safeguards — even basic transparency — will exacerbate those harms.

  The Memorandum suggests that these agencies' uses of AI are "governed through other policy,"[129] but that is a significant overstatement. The policy sources it identifies are largely general statements of principles without meaningful accountability mechanisms or binding rules. For example, ODNI's *Principles for Artificial Intelligence Ethics for the Intelligence Community* describes six high-level guidelines — including a commitment to be "transparent and accountable," but the public to date has seen little evidence of either.[130] The Defense Department has released a toolkit "to help DoD personnel design, develop, deploy, and use AI systems responsibly," but using the toolkit is voluntary.[131]

---

system; Brian Naylor, *How Federal Dollars Fund Local Police*, NPR (June 9, 2020), https://www.npr.org/2020/06/09/872387351/how-federal-dollars-fund-local-police; Matthew Guariglia & Dave Maass, *How Police Fund Surveillance Is Part of the Problem*, EFF (Sept. 23, 2020), https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem.

[126] Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7225(d), 7228, https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf. "Intelligence community" is defined by 50 U.S.C. § 3003(4), and includes the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency, among others. The Advancing American AI Act exempts the intelligence community from the Memorandum's minimum risk management practices and both the intelligence community and the Department of Defense from the use case inventories. *Id.*

[127] Memorandum M-25-21, sec. 1(c).

[128] 44 U.S.C. § 3552(b)(6).

[129] Memorandum M-25-21, sec. 1(c) n.8.

[130] Office of the Director of National Intelligence, *Intelligence Community Principles of Artificials* (2020), https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2020/3634-principles-of-artificial-intelligence-ethics-for-the-intelligence-community-1692377385.

[131] Department of Defense, *CDAO Releases Responsible AI (RAI) Toolkit for Ensuring Alignment with RAI Best Practices* (Nov. 14, 2023), https://www.defense.gov/News/Releases/Release/Article/3588743/cdao-releases-responsible-ai-rai-toolkit-for-ensuring-alignment-with-rai-best-p/.

Similarly, President Trump directed the National Security Advisor to review recently issued National Security Memoranda (NSM) and make recommendations for rescissions[132] — which could include the NSM governing AI used as a component of national security systems.[133] Whether that NSM has been recommended for rescission is not publicly known. Overall, the intelligence and defense agencies lack specific rules and safeguards for their AI systems, as well as clear processes to implement and enforce those rules.

- **Potential Failure to Include More Rudimentary Algorithms:** The Memorandum incorporates one federal definition of "artificial intelligence," codified in the John S. McCain National Defense Authorization Act.[134] That definition limits "AI" to systems that "learn," use "human-like perception, cognition, [or] planning," "think or act like a human," "approximate a cognitive task," or "act rationally."[135] The scope of this definition is ambiguous — it may include more rudimentary algorithmic systems such as the PATTERN decision-making algorithm or Idaho's Medicaid benefits algorithm, or it may be limited to more advance technologies such as machine learning. Although more advanced technologies may present emerging challenges, existing, simpler algorithmic systems already in place are actively affecting civil rights and civil liberties.

In addition to addressing these shortcomings in the OMB Memorandum, this Committee and Congress will play important roles in ensuring that the Memorandum's directives — and the Congressional directives that underly it — are carried out by executive agencies. Neither the Memorandum nor its underlying statutory requirements have enforcement mechanisms, and Congress consequently has the ultimate responsibility through its oversight and budget authority to ensure that the Memorandum's protections are realized.

This Committee in particular has authority to conduct hearings and other oversight to ensure that the exceptions in the Memorandum are not simply a blank check for surveillance abuses. This includes ensuring that federal law enforcement is adhering to the Memorandum's safeguards and that national security and

---

[132] Exec. Order No. 14148 of January 20, 2025, sec. 3(c), 90 Fed. Reg. 8237 (Jan. 28, 2025).
[133] White House, Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence (Oct. 24, 2024), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security.
[134] Pub. L. No. 115-232, § 238(g) (2019), https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[135] *Id.*

intelligence agencies have sufficient policies and practices in place to protect civil rights and civil liberties.

V. Congress and this Committee Should Address the Civil Rights Impacts of Artificial Intelligence in Traditionally Protected Sectors

In addition to addressing criminal uses of AI, Congress should address the potentially discriminatory effects of AI, especially when used in traditionally protected sectors like housing, employment, credit, and more. For example, employers are using large language models to evaluate applicants' resumes,[136] which are instances of foundation models to evaluate job applicants, and those technologies can unfairly advantage male candidates or de-preference first-generation college graduates and racial minorities.[137] Other AI-driven hiring technology such as gamified personality tests can be inaccessible to and discriminate against applicants with disabilities.[138]

Similarly, credit scoring systems are algorithmic models that attempt to predict a borrower's risk and how well that person is likely to repay their debt obligations. These systems typically generate a numerical score used to help creditors in the financial services system determine the creditworthiness of a consumer. They are often used as part of a lender's decisions on underwriting and pricing. Algorithmic credit scoring disproportionately disadvantages Black, Latino, and Native American consumers who have historically had less access to traditional credit than white consumers.[139] As Federal Reserve Vice Chair of Supervision Michael Barr stated, "Artificial Intelligence…relies on the data that is out there in the world and the data…is flawed. Some of it is just wrong. Some of it is deeply biased…Information we have on the Internet is imperfect…if you train a Machine Learning device, if you

---

[136] Leon Yin et al., *OpenAI's GPT Is a Recruiter's Dream Tool. Tests Show There's Racial Bias*, Bloomberg (Mar. 7, 2024), https://www.bloomberg.com/graphics/2024-openai-gpt-hiring-racial-discrimination/.

[137] Avi Asher-Schapiro, *AI is Taking Over Job Hiring, But Can It Be Racist?*, Thomson Reuters (June 7, 2021), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC/; Jeffrey Dastin, *Insight - Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Thomson Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

[138] Lydia X.Z. Brown et al., *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?*, Center for Democracy & Technology (2020), https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.

[139] Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

train a Large Language Model on imperfect data, you're going to get imperfect results."[140]

Similar examples exist across traditionally protected sectors. Consequently, policymakers' efforts to combat harmful or exploitative AI should include mitigating discriminatory harms from AI, including requiring impact assessments, mitigation of harms, ongoing monitoring, and notice and appeal — many of the same requirements the Trump administration has implemented for federal uses of AI.

VI. Conclusion

Thank you for the opportunity to testify before this Subcommittee. As you consider how to meet the challenges of artificial intelligence, it is important that the Committee and Congress ensure that its response comports with civil rights and civil liberties, and that you exercise your oversight and legislative authority over other federal efforts such as the Administration's "information silos" Executive Order, as well as oppose any congressional AI "moratorium" preempting state laws, so as to not open the door to malicious uses of AI.

[140] *See* Federal Reserve Board of Governors Vice Chair Michael Barr, *Setting the Foundation for Effective Governance and Oversight: A Conversation with U.S. Regulators*, Responsible AI Symposium (Jan. 19, 2024), https://www.youtube.com/watch?v=HbM_zD0esDo.