UNIDOSUS
STRONGER COMMUNITIES. STRONGER AMERICA.

HEADQUARTERS
Raul Yzaguirre Building
1126 16th Street NW, Suite 600
Washington, DC 20036-4845

202.785.1670
202.776.1792
unidosus.org

January 19, 2024
Via email
office.of.legal.policy@usdoj.gov

Re: Written Comments on Law Enforcement Use of Facial Recognition Technology, Biometric Surveillance Technologies, Predictive Algorithms, and Data Storage and Access

On behalf of UnidosUS, we respectfully submit these comments in response to the Department of Justice, the Department of Homeland Security, and the Office of Science and Technology Policy's (OSTP's) request for public input on law enforcement use of facial recognition technology (FRT), biometric surveillance technologies, predictive algorithms, and data storage and access regarding such technologies.

UnidosUS is a nonprofit, nonpartisan organization that serves as the nation's largest Hispanic civil rights and advocacy organization. Since 1968, we have challenged the social, economic, and political barriers that affect Latinos through our unique combination of expert research, advocacy, programs, and an Affiliate Network of nearly 300 community-based organizations across the United States, including Puerto Rico.

Below, we make the following major points:

- While constitutional principles like due process, equal protection, and privacy underpin our laws in theory, outdated regulations fail to provide adequate accountability for rights- and privacy-infringing uses of data-driven surveillance systems. We cannot allow an infrastructure of invasive surveillance and unchecked data-sharing to undermine cherished constitutional freedoms.
- Latinos and other communities of color are vulnerable to rights- and privacy-impacting uses of technological forms of surveillance, which should be reconciled with democratic norms and practices.
- Agencies' lack of transparency has covered up the use of these technologies without proper testing, training, or implementation protocols.
    - A September 2023 GAO report found that law enforcement at the DHS and DOJ lacked basic protocols or training around the use of facial recognition technologies. In response, DHS Sec. Mayorkas published a memo articulating a policy commitment to constitutional principles that law enforcement and government agencies should revisit and update as a result of this report.
- The DOJ and the DHS have ample authority and opportunity to immediately correct the course around rights-impacting surveillance practices. Recommendations include:
- Institutionalizing impacted community involvement and feedback.
- Leveraging impact assessments for empirical evidence to inform metrics

- Closing accountability loopholes by declining use exemptions that undermine civil rights and liberties.
- Prioritizing data integrity and stewardship for rights-protecting systems.
- Creating incentives for rights-protecting technologies through responsible procurement.

Wherever they work and live, and whomever they are, everyone deserves access to basic democratic rights, including the right to privacy, the right to travel, the right to vote, and the right to due process of law. Yet Latinos and immigrants, like other historically marginalized communities, have endured legacy over surveillance by the U.S. government, resulting in disproportionate racial profiling, targeting, and tracking by law and immigration enforcement, including at the federal level.

Now, digital data-driven surveillance tools powered by algorithms and artificial intelligence (AI) systems, including FRT, biometric surveillance technologies, and predictive policing and sentencing algorithms, allow additional opportunities for the over surveillance of vulnerable communities. While these surveillance capabilities are frequently touted as serving public safety, their use can also be a source of systematic civil rights and liberties violations.

In other countries, we have seen that such technologies also offer chilling possibilities for oppressing freedoms by authoritarian regimes. These clear and imminent dangers demand oversight by the government to balance effective law enforcement with constitutional norms inherent to a free society and to prevent abuse in specific cases. While lower-income and communities of color are often the last to benefit from technological advances, they are also often the first to bear the brunt of intrusive and privacy-infringing uses of technologies. Such surveillance infrastructure can also create digital suspect classes, placing entire communities under heightened scrutiny and altering the amount and concentration of law enforcement resources at the community level, resulting in biased forms of over-policing unrelated to risk.

Law and immigration enforcement bodies, including at the federal and state levels, already have built and scaled intrusive surveillance systems by purchasing personal and consumer data inputs from utility companies, private contractors providing tools with facial and biometric recognition capacities, social media platforms, and third-party data brokers. This alarming data mining is in addition to data already contained in other government databases like DMV records. With nearly every federal agency independently collecting, processing, and hosting large amounts of personal data ranging from tax records, driver's licenses, voter registrations, social security numbers, DNA and biometric information, and passport information, nearly every person in the U.S. has personally identifiable information on file with a government agency.

For the 62.1 million Latinos living in this country, the risks of overreach and over policing are pervasive. In addition to the nearly 20 million immigrants who identify as Latino in this country and more than 10.6 million U.S. citizens of any racial or ethnic identification who live in mixed-status households, they also face unique risks to the infringement of basic rights from

oversurveillance. Under the authority of a hostile agency or administration, the consequences of now-routine forms of data collection on communities and individuals could go from egregious to disastrous—and, if left unchecked, offer tools for overreach that is unmistakably authoritarian. Notably, public reporting by the New York Times and others indicates plans are already in place for a future Trump Administration to conduct highly intrusive and unprecedented forms of immigration sweeps and internment.

The expansion of dragnet surveillance infrastructure disproportionately targets marginalized groups. Use of tools like FRT, biometric data surveillance, automated license plate readers, camera networks, geofencing, and predictive policing models systematically and disproportionately amass data on immigrants and communities of color due to historic over policing. This reality poses significant dangers for Latino and immigrant communities in the law and immigration enforcement contexts. Integrated surveillance systems provide an opportunity for government agencies and law enforcement bodies, including police and the Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP), to sidestep Congressional oversight and practice targeted, discriminatory, and intrusive surveillance targeting Latinos.

This is a critical moment for governments to check practices that can facilitate anti-democratic uses of power. The increasing ubiquity of data collection for a wide range of purposes by major actors in the commercial sector, alongside the increasing sophistication and capacities of AI models and algorithms, will continue to produce new tools for the government to further develop and fine-tune surveillance, predictive, policing, and profiling practices. The truncated rights of immigrants make these communities particularly vulnerable to threats posed by underregulated uses of AI.

An Unregulated Surveillance Tech Market Incentivizes the Neglect of Civil Rights and Liberties

Like everyone else, Latinos have shifted online to earn, learn, shop, participate in civic life, create community, and access jobs, financial products, and business opportunities. This online migration has created individual digital footprints and profiles that track, compile, and predict our behaviors, interests, habits, daily practices, and personal information related to everything from our health, social networks, personal identity, and daily transit and commute patterns.

Latinos represent a significant segment of the nation's consumers, entrepreneurs, business owners, workforce, students, residents, patients, and voters. Between 2020 and 2030, Latino workers will account for 78% of new workers. Companies track and monetize the personal information and behaviors of Latinos through commercial data surveillance, which means their data constitute a disproportionate share of the information, and therefore profits, generated by companies harvesting and selling this data to third parties. Organizations could use this data to create and train AI tools or to use them for ad-targeting and making decisions in arenas, from credit access to job opportunities.

Because of bias embedded within data models that perpetuates and exacerbates historical discrimination, Latinos are also at heightened risk of being harmed by government surveillance. Additional forms of discrimination and exclusion can afflict new algorithmic and machine-learning tools that make decisions based on inherently flawed datasets. For example, predictive policing tools have been shown to make predictions about a defendant's risk of re-offense that are inextricably confounded by racial bias.

Surveillance tech markets have been left largely unchecked and unregulated by the government, allowing private actors to steer the market in a race to the bottom by trading off democratic norms and constitutional protections for profit to increase the scale, sophistication, and marketability of AI tools. This further incentivizes invasive surveillance practices since an AI tool's viability is presumed to be directly tied to the size, reach, and granularity of datasets used to train and sustain it.

As the AI Executive Order and recent OMB memorandum make clear, using biased databases in arenas that are rights-impacted requires specific scrutiny and safeguards, including the choice not to use tools that are impossible to reconcile with core rights and principles.

Threats to civil rights and civil liberties can also occur when massive, privacy-infringing databases are sold to and used by policing and immigration law enforcement, which already must overcome complex histories of embedded bias and discrimination. For this reason, as we describe below, any "exceptions" for law enforcement or immigration enforcement purposes must not create a lack of accountability or transparency for such uses.

As our Founders knew when crafting our Fourth Amendment, balancing individual liberties and protections against government overreach with governance needs, biased and rights-infringing uses are more—not less—important in the hardest of use cases. Instead, we need rules and safeguards that reconcile effective law enforcement with privacy by design tools that preserve our careful and well-calibrated democratic norms.

A Lack of Oversight and Dragnet Deployment of Surveillance Systems by Government Enable Racialized Policing and Anti-Democratic Immigration Practices.

The Department of Justice (DOJ) and the Department of Homeland Security (DHS) were two of the earliest agencies to integrate facial and biometric recognition technology into their widespread video, image, and personal data surveillance network. The DHS began its own facial recognition "testing program" in 2013, with the agency's first known contract with a biometrics company originating as early as 2008, which was used to scan individual photos in the Rhode Island DMV database to identify targets for deportation. And yet, even most lawmakers were unaware of ICE's 2008 facial recognition program until July 2019, when The Washington Post published an expose detailing the program.

A lack of transparency and the absence of practice disclosures by agencies have provided cover for the use of these technologies to go unchecked and without proper testing, training, or implementation protocols. A September 2023 GAO report found that law enforcement at DHS and DOJ lacked basic protocols or training around the use of facial recognition technologies. In response, DHS Sec. Mayorkas published a memo articulating a policy commitment to constitutional principles that law enforcement and government agencies should revisit and update as a result of this report.

Examples of publicly known data-driven surveillance abuse by law and immigration enforcement bodies include the following:

- **Law enforcement misuse of spyware and cyber hacking tools.** Internal FBI documents obtained by The New York Times revealed in YEAR that the FBI had purchased and deployed Israeli-developed spyware, Pegasus, in certain criminal investigations. Pegasus is a spyware that can be installed on cell phones and other devices and is capable of receiving and reading text messages, tracking calls, collecting passwords, location tracking, accessing the device's microphone and camera, and harvesting information from installed mobile applications.
- **Predictive policing software automates racialized policing practices.** Predictive policing tools like PredPol and the abuse of data by police departments perpetuate systemic racism, as evidenced by wrongful arrests and over policing of minority neighborhoods informed by flawed facial recognition matches and racially biased crime forecasting algorithms.
- **ICE purchasing utility data to track immigrants and exploit the need for basic essential utilities**. A 2022 report developed by the Georgetown Law Center on Privacy and Technology highlights how the evolving practice of data-driven deportation has come at the cost of diminishing civil rights in the era of big data and AI-driven biometric surveillance capabilities. ICE has been found to exploit people's need for essential utilities such as water, gas, electricity, and internet to target and track individuals for deportation by contracting with private data brokers who sell utility customer data (name, address, phone data, driver's license data, and more) back to the agency. Specifically, this report outlines how ICE has used personal information belonging to over 218 million utility customers across the country to geolocate individuals—and that there are no federal and state laws protecting communities or individuals against these warrantless sweeps and searches of utility or other data.
- **ICE uses a constellation of databases to mission creep and disregard federally mandated enforcement priorities.** A 2019 report by the New York Times detailed how ICE's Homeland Security Investigations (HSI) division had been testing the use of automated social-media profiling to support the vetting of visa applicants and holders before and after entrance to the United States. HSI had historically been focused on transnational crime as opposed to civil immigration violations. But the report details

how ICE's access to "hundreds of disparate computer systems, from state and local governments, private data brokers, and social media networks" also leveraged software and sharing agreements meant for criminal and counterterrorism to track, target, and arrest low-priority targets–despite President Obama's Immigration Accountability Executive Action that colloquialized "Felons, not Families" to describe his deportation priorities. Under President Trump's Executive Order 13768, which rescinded President Obama's civil immigration enforcement policies and priorities, this agency's mission evolved into an all-out crash. Under this Order and the rapidly expanded data and facial recognition access of DHS, almost three times as many civil immigration arrests were made during the first 14 months of the Order compared to the previous 14 months under the Obama-era order.

- **DNA collection and surveillance practices criminalize race, ethnicity, and national origin.** A Trump Administration rule issued in 2020 directed DHS to collect DNA from anyone in immigration detention. This rule resulted in the addition of about 750,000 new samples annually from immigrant detainees to the FBI's Combined DNA Index System (CODIS) database, on top of the genetic information of 21 million people it already contained. Notably, Black and Latino men are already overrepresented in DNA databases. DNA collection and analysis practices enable differential tracking of migrant communities and establish default suspicion and criminalization of immigrant communities and communities of color. Without sufficient guardrails, these techniques can enable genetic profiling of entire communities purely based on race, ethnicity, or national origin, absent of probable cause or evidence of wrongdoing.
- **Federal entities have tried to gain access to protected voter data from states and DHS databases to perform voter purges.** In 2017, the now-disbanded Presidential Advisory Commission on Election Integrity created by President Trump to address debunked claims of voter fraud, requested voter information from all 50 states. Information requested included names, dates of birth, addresses, political party affiliation, last four digits of voter's social security number, and voter history. The Commission was also found to have requested information from two DHS databases on immigration detentions and citizenship applications to perform a similar analysis. This move doubled down on Trump's disproven claims that millions voted illegally during the 2016 election. The ease with which federal agencies could secure such granular, detailed data is a chief concern with the existing biometric surveillance capabilities of the DHS and the FBI.

These and other examples demonstrate a clear and urgent need for the DOJ, the DHS, and the OSTP to develop an oversight framework and issue guidance for law and immigration enforcement bodies that prohibit using such technologies in cases involving core matters of civil liberties.

Silence and a lack of transparency and accountability on the part of government agencies also risk alienating communities from cooperating with government and public safety efforts

because of mistrust and fear. Unjustified targeting of groups and individual privacy invasions further strain ties between law enforcement and Latinos and immigrants and further undermine community-oriented policing and public safety efforts. This targeting can also drive marginalized groups, including mixed-status households, further into the shadows, rather than encouraging engagement with government institutions.

The lack of guidance, transparency, and oversight from the DOJ and the DHS also feeds incentives to further expand data collection, as highlighted above. Without immediate action from the DOJ and the DHS that outlines clear and firm limitations, accountable oversight, and ensures public transparency on the use of surveillance tools and data sharing, there is little incentive to innovate in ways that preserve both privacy and law enforcement. Our nation can fix this situation, but it requires fundamental changes from these agencies.

The DOJ and the DHS Have Ample Authority – and Opportunity – to Immediately Course Correct Around Rights-Impacting Surveillance Practices

Policymakers have proposed principles and standards to govern AI systems (and related data-driven surveillance tools) including:

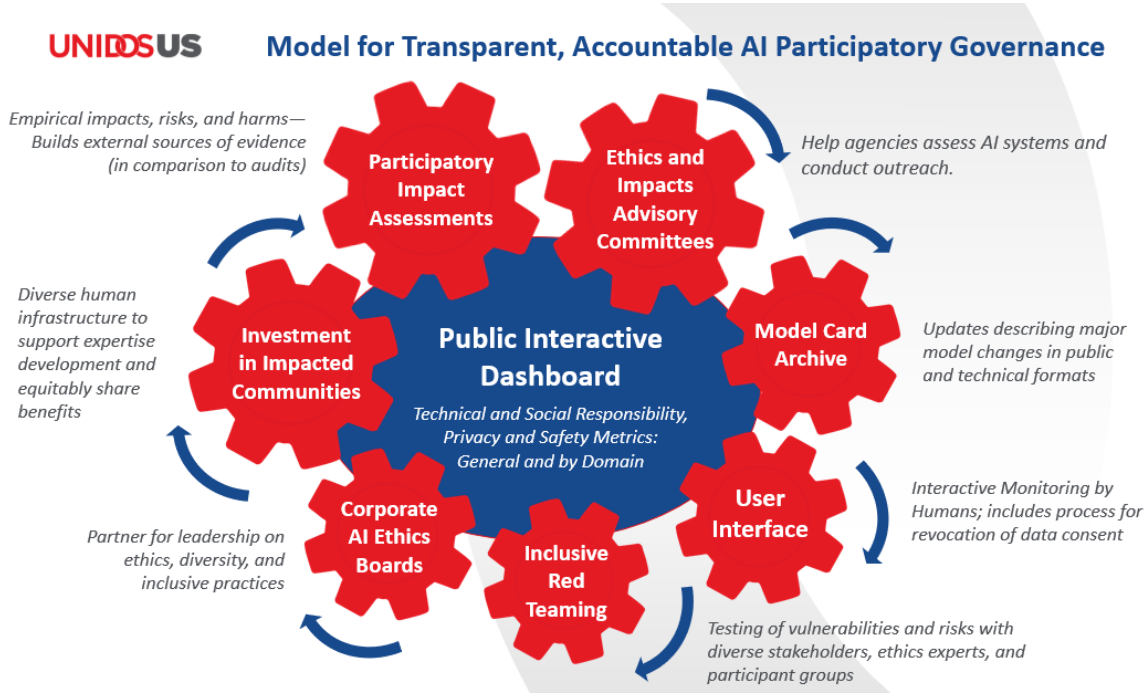
- The National Institute of Standards and Technology (NIST)
- The White House, Office of Science and Technology Policy (OSTP)
- The National AI Advisory Committee (NAAIC)
- The White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- The Office of Management and Budget (OMB) guidance on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.

When viewed alongside the directive at issue here related to Executive Order 14074 Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, it's clear that both the DOJ and the DHS have the authority and a critical opportunity to develop a responsible governance framework for data-driven and artificially intelligent surveillance systems.

As described in our Written Testimony on Governance of Artificial Intelligence and Comments on OMB Draft AI Memorandum, a responsible, accountable, and transparent approach to AI governance that includes privacy-enhancing techniques, use limitations, community-informed governance, rigorous oversight, and public transparency can safeguard against anti-democratic misuse of these technologies.

In particular, we call on the departments, including the DOJ and the DHS, to give impacted communities a voice in governance through practical mechanisms that provide a means of feedback for agencies about the uses and impacts of technologies in real time. We outline below a multifaceted and comprehensive governance model that includes inclusive red

teaming, impact assessments, and consumer complaint collection, alongside a public leaderboard for metrics and a requirement for community advisory committees for each agency, sub-agency, or department, as depicted below.



In addition, the Departments' Use Inventories and proposed risk management approaches could usefully be organized according to the "AI Risks and Trustworthiness" issues described by NIST, which highlight that AI systems should meet baselines for each of the following factors: 1) Valid and Reliable; 2) Safe; 3) Secure and Resilient; 4) Accountable and Transparent; 5) Explainable and Interpretable; 6) Privacy-Enhanced; and 7) Fair—with Harmful Bias Managed. The DOJ and the DHS should evaluate current uses in light of each of these values across their entire portfolio of AI uses, in consultation with NIST and other experts familiar with the evolving science for each of these measures, paying concentrated attention, as the OMB Memo indicates, to risks and safety- and rights-impacting uses. In mapping current uses of AI and algorithmic tools, agencies should also:

- Detail and explain the technological limitations of a tool given its use cases and relevant human factors.
- Identify the adequacy of any current evaluations of the training data, model design, impacts, and any mitigations for known and potential risks.
- Describe the extent of involvement or consultation with impacted communities (more on this below) on design, risks, impacts, or other aspects of the model or system.
- Explain the adequacy and conclusions of external audits and impact assessments that are underway or have been done.

- Fully characterize the socio-technical context at the agency related to human interactions with the technology, evidence on experiences of internal and external users, and other factors.

There are sound reasons for both departments to take a closer look at current uses and the lessons those offer before rushing to adopt new ones. Successful systems are more difficult to build and execute than they appear at first glance. For example, take the RMF's assignment to make systems, "Fair—with Bias Managed." Goals like achieving a "fair" model, which seems simple enough, can for sometimes be in tension with the accuracy of an AI model, as Brian Christian explains in his book, The Alignment Problem. In his book, Christian provides specific examples of researchers' efforts to grapple with algorithmic bias in parole decision-making.

Democracies learn in public and do not act until a deliberative process is completed that assesses harms and trade-offs, looks at technical capacities and implications for shared values, and lets various stakeholders weigh in. AI governance, to be democratic in nature, should anticipate potential harms and include mechanisms for accountability to the people they impact. Too often, the bias or flaws in models are understood too late—so we must get better at both predicting and preventing foreseeable harms through good design: Impacted groups are ideally positioned to tell technologists what they may not know.

Such challenges pose specific problems in the context of government programs. For example, facial recognition systems are notoriously bad at recognizing people from communities of color, as UnidosUS staff learned first-hand through our efforts to assist the federal government in enrolling taxpayers in Puerto Rico who had become newly eligible for federal Child Tax Credits. Because enrollees needed identity verification through digital systems that often failed to recognize their faces on standard Puerto Rican government ID cards, this frequently delayed or complicated their receipt of benefits.

Sometimes, failure modes are more obscure. Models have been caught, after the fact, gathering clues on factors related to race or gender in hiring decisions, for example, from word choice or specific activities listed on a resume, even when information on race and gender has been omitted, leading companies to discard the models as too inherently biased to be used.

Relatively simple automated decision-making models have also been shown to be deeply biased and to lack predictive value in areas such as mortgage lending, given the number of factors that function as proxies for race, even when protected class is omitted. Moreover, the black box nature of many models means that subtle forms of bias may remain undetected without specific steps, including interrogation of the model for bias, impact assessments, and other forms of actual empirical evaluation.

Too often, there is an emphasis on metrics that were created without civil rights scrutiny or the involvement of impacted communities. These fail to account for the socio-contextual dynamics and real-world animation of constitutional norms like equal protection or due process. Because

targeted communities cannot meaningfully redress surveillance harms from the outside, it is crucial to maintain the means for public accountability and community stewardship.

Among other reasons, this is why fairness or bias "audits," which many institutions generally measure against statistical outputs, can and do still result in inequitable, discriminatory real-world outcomes. What we define as "fair" or "equitable" must also include a qualitative assessment of how these systems affect vulnerable groups in practice. True equity requires their experiences, needs, and perspectives to shape governance frameworks and decisions around acceptable applications for these systems. Only by balancing technical audits with impacted communities' lived experiences, developed through inclusive impact assessments, can societal effects be understood and addressed.

Leveraging Impact Assessments for Empirical Evidence to Inform Metrics

In addition to inclusive red teaming, as the above list suggests, facilitating and supporting regular impact assessments focused on real-world effects can provide another vital feedback channel to strengthen AI governance. Crucially, these should be conceptualized as "third-party audits," and not as internal to government agencies.

Assessments also must be well-designed to produce tangible, specific, and usable results that inform standards. Formal evaluations conducted in partnership with public interest and other stakeholders can surface overlooked issues, generate empirical insights on how systems perform in actual usage, and center data on the impacts to, and experiences of, affected groups and individuals. Findings could directly inform iterative improvements to policies, model training, dashboard benchmarks, and other governance mechanisms.

Regular inclusive impact assessments would help provide external validation for oversight processes. Centering community voices and empirical insights within governance cycles fosters accountability. It demonstrates that a priority is placed on improving system impacts and real-world outcomes rather than on narrow or technical measures alone.

Further integration of AI systems into government could eliminate barriers or create new, and potentially even more problematic, issues. The DHS and the DOJ should first evaluate existing algorithmic systems against principles of fairness, accountability, and transparency. We should not replace current or flawed tools with AI—agencies should thoroughly evaluate current AI uses and publicly describe their context and limitations before expanding adoption. The task for the agencies should first be to thoroughly inventory uses, to create substantial new guardrails around *current* uses of AI tools in light of the NIST RMF, and to publicly identify the successes, caveats, criticisms from stakeholders, and shortcomings of these uses. Additional considerations related to this process include:

- Policy on current and new uses should be based on ethical guidelines linked to participatory design processes and expanded capacity, with multiple and overlapping opportunities for input.
- Impacted communities require formal structured roles and influence, not just 'check-the-box' perfunctory consultations.
- Structures for participation should include AI Ethics and Impacts Advisory Committees with defined roles and input opportunities alongside public dashboards and user complaint mechanisms to monitor AI system performance informed by community feedback.
- Continuous transparency mechanisms, such as a public dashboard, that publish indicators of capabilities, limitations, and real-world impacts would improve transparency and drive accountability and productive innovation while educating the public.
- Advisory Committees established at agencies can assess and catalog specific use-case AI risks, applications, mitigate harm, and assist with public outreach.
- Impact assessments of use cases and the development of an empirical body of evidence on the distributions of benefits and harms are needed to inform policy. Agencies should collect data on the experiences of affected populations to accurately describe how socio-technical systems operate in real-world conditions.
- Inclusive red teaming exercises that stress-test AI systems are essential to uncover pre-deployment risks, biases, and failure modes. Intentionally integrating marginalized expertise helps uncover gaps that technology teams may miss.

Exempting AI Uses at the Heart of Constitutional Governance Would Undermine Democratic Norms and Incentives to Develop Technologies That Are Rights- and Privacy-Enhancing

Perceived efficiencies from current and planned uses in criminal justice, immigration enforcement and related uses, and in public benefits will likely lead agencies to continue to gloss over deeply concerning data security, stewardship, privacy, and civil liberties concerns. As explained above, however, the use by governments of AI tools, even in cases involving core matters of civil liberties, extremely vulnerable populations, and privacy rights for immigrants and U.S. citizens, as well as legal due process and constitutional considerations, do not inspire confidence that the right guardrails are in place to dramatically expand uses of AI consistent with the democratic principles of fairness and other values.

Although the NIST RMF framework calls for AI to be "privacy-enhancing," the OMB's recent Memo fails to ensure that this will matter where it is needed most. Instead, the Memo's proposed waivers are likely to allow some of the most problematic and rights-infringing deployments of AI to continue to avoid even basic forms of public accountability. For example, as a law enforcement agency combining criminal and civil responsibilities, the DHS or its sub-

agencies may claim that law enforcement and national security exemptions apply or that an activity is "mission critical."

Such claims would be a terrible error. Hard cases cannot be the exception to our policies without undermining our fidelity to constitutional principles that rest at the core of our global leadership on personal freedoms and as a beacon of democracy. Instead, we need tools that allow fidelity to longstanding values and permit effective law enforcement.

Therefore, the OMB and the OSTP should develop a more tailored approach to these highly sensitive use cases. For their roles, the DHS and the DOJ should not seek to side-step the implications of their many safety- or rights-impacting uses. Crucially, such waivers erode any incentive to do the hard work of aligning the design of systems with rights—but the failure to use privacy-by-design principles should not be characterized as a function of the technology when it is, instead, a choice to sanction unaccountable, untransparent, and dangerous practices.

The OMB Memo further requires that "[w]hen law or governmentwide guidance precludes disclosure of the use of AI or an opportunity for an individual appeal, agencies must create appropriate mechanisms for human oversight of rights-impacting AI." The OMB and the OSTP should more specifically define what is an "appropriate" or inappropriate mechanism, as it poses the prospect of potential abuse and a lack of transparency in government decisions or processes.

Regardless, the DOJ and the DHS must immediately shut down and replace technologies and data that government entities can marshall for authoritarian ends in the future. Given the need to future-proof government from the specter of abuse, the OSTP and the White House should also lead a process of taking full account of current practices and fixing them in short order. At a minimum, the OSTP should create additional clarity regarding when agencies can seek waivers or exceptions from having to meet risk management requirements. The following is needed:

- When a waiver or exception is granted, there should be a mechanism to seek reconsideration of such a decision.
- The OMB Memo should be clear that waivers and exceptions sunset annually and should be reevaluated in light of these documented harms and risks.
- The Memo should require that agencies consider less rights-impacting alternatives before they are eligible for consideration for a waiver or exception.
- The Memo should require that agencies publicly report seeking waivers or exceptions, and they should report the grounds for this request and its resolution and timing.

In lieu of providing waivers, the U.S. should instead follow the lead of European governments in requiring individualized consent to the use of data without a court order. We should also require privacy by design principles that are compatible with effectiveness, such as strict data minimization, access controls, federated learning, and other privacy-enhancing techniques for

government AI uses. Collection by agencies of biometric data, including DNA, should also receive specific scrutiny given its power in the hands of future Administrations that may lack any semblance of democratic restraints.

Prioritizing Data Integrity and Stewardship for Rights-Protecting Systems

Large, encroaching surveillance systems that integrate millions of identifying data points create opportunities for invasive and violative privacy intrusions and individual or community-level targeting, including based on protected characteristics. Appropriate management and use of data improves both the performance of an AI system and its trustworthiness and safety. Privacy by design features such as branching and segmentation, federated data storage, and other safeguards enhance the security of government data storage while enabling and facilitating accountability for, and integrity of, government uses.

Without comprehensive federal data privacy legislation, the DOJ and the DHS both have an important opportunity to clarify through guidance and policymaking that traditional and updated forms of civil rights protections fully extend to the use of these data-driven systems. Given the scale and inherent high-risk impacts of the DOJ and the DHS data collection and surveillance systems, these agencies should prioritize developing and operationalizing data stewardship best practices. These agencies should develop these practices in partnership with technical experts, like NIST researchers and practitioners, for technical viability, and with input from civil rights and civil liberties advocates and impacted groups to orient technical standards towards constitutional norms and democratic principles. The creation of a community advisory committee, as we call for in our comments to the OMB, is a critical step.

Researchers identify a host of approaches that help to safeguard individual and group data privacy and security, including:

- In *Trustworthy AI: From Principles to Practice*, Bo Li, et al., outline a range of technical design approaches that enhance individual data privacy and security while also maximizing system robustness, security, transparency, fairness, and safety.
- In *"What We Can't Measure, We Can't Understand:" Challenges to Demographic Data Procurement in the Pursuit of Fairness*, McKane Andrus, et al., analyze the tension between data availability and making systems less discriminatory, including domain-specific applications. Recommendations include "clearer legal requirements around data protection and anti-discrimination, privacy-respecting algorithmic fairness strategies, and meaningful agency of data subjects."
- In *Eyes Off My Data: Exploring Differentially Private Federated Statistics to Support Algorithmic Bias Assessments Across Demographic Groups,* the Partnership on AI outlines techniques for prioritizing individual data privacy in the context of demographic data collection, processing, sharing, and management.

- The Bipartisan Policy Center's technical paper on *Privacy-Preserved Data Sharing for Evidence-Based Policy Decisions* highlights "emerging technical applications to deploy certain privacy-preserving approaches in targeted settings."

We urge careful review of these reports and others to discern implementable safeguards that should serve as basic design principles for government systems and models. Robust standards for privacy-protecting system design are foundational for building and maintaining secure, trustworthy data pipelines.

A privacy-centric data governance framework provides a floor to build and scale more trustworthy and rights-respecting interventions. Embedding these technical solutions from the outset can also safeguard against future exploitation, misuse, and abuse of these tools as Administrations change. The DOJ and the DHS have the authority to take near-term action to build such a framework and issue baseline protections, such as:

- Issuing guidance to restrict the use of facial recognition to post-incident criminal investigations rather than real-time surveillance absent a court order.
- Issuing guidance requiring probable cause warrants for access to DMV databases or other sensitive biometric data repositories storing substantial personal information.
- Limit the bulk sharing of data across agencies.
- Limiting the scope and retention periods for all biometric data.
- Creating an accessible civil rights impact review process for communities concerned about surveillance technology procurement or policies enabling structured public participation for oversight and reform.
- Appointing agency civil rights advisory bodies with diverse community representation able to review technologies and data-sharing proposals with binding veto authority based on privacy and liberties concerns.
- Halting facial or other biometric scans at border checkpoints absent individualized suspicion until a comprehensive and participatory equity assessment is completed.

Agencies Can Create Incentives for Rights-Protecting Technologies Through Responsible Procurement

We fully support the OMB Memo's provisions on procurement policies that underscore that AI contracts should align with national values and law, including "those addressing privacy, confidentiality, copyright, human and civil rights, and civil liberties." Since waivers for law enforcement or mission-critical functions could undermine progress in assuring that federal tax dollars are not spent on systems incompatible with this requirement, consistency across federal procurement policy provides another reason to substantially narrow or eliminate waivers.

Government procurement policies offer a powerful lever for incentivizing responsible practices in the private surveillance technology sector. Too often, vendors prioritize the ability to

showcase novel analytical capabilities to law enforcement without meaningfully accounting for potential civil liberties abuses or disproportionate impacts on vulnerable groups. Both government demand and private sector profit motives drive the market toward more invasive and ubiquitous surveillance systems—directly tying an AI tool's efficacy to ever-larger datasets gathered through public and private monitoring.

The DOJ and the DHS, like other agencies, can leverage their purchasing power to contract with providers committed to following accountability standards issued by the government. By incorporating key principles like data minimization, privacy by design, branching and segmentation, and mandatory community auditing into procurement standards, entire product lines and business models would need to shift to meet these civil liberties-conscious benchmarks in order to qualify for public contracts.

Over time, accountable procurement policies could make rights-respecting technologies the norm and drive the market in a race to the top, spurring innovation in privacy-preserving analytics and oversight tools as table stakes for government certification. Core design principles like articulating impacts on marginalized groups, enabling participatory assessments, and maintaining two-way accountability between vendors and the public could rebalance existing trade-offs between accountability and profit.

The DOJ and the DHS can jumpstart this transformation by using their purchasing power to uplift civil liberties as primary evaluation criteria alongside technical capabilities. Holistic security solutions benefiting entire communities can come only from providers equally committed to respecting individual rights. Forward-thinking procurement policies represent the first step toward restoring public trust in government surveillance and harnessing private innovation for the common good.

For questions or additional dialogue on these issues, please contact Laura MacCleery, Senior Director of Policy, at lmaccleery@unidosus.org, and Claudia Ruiz, Senior Civil Rights Analyst, at cruiz@unidosus.org.