Northwestern
PRITZKER SCHOOL OF LAW
Center for Racial and
Disability Justice

Northwestern Pritzker School of Law
Attn: Center for Racial and Disability Justice
375 East Chicago Avenue
Chicago, IL 60611-3069

12/18/2025

Kristi Noem,
Secretary, U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services (USCIS)
5900 Capital Gateway Drive, Camp Springs, MD 20746

RE: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

Dear Ms. Noem,

The Center for Racial and Disability Justice (CRDJ) at the Northwestern Pritzker School of Law is committed to advancing the rights, dignity, and collective liberation of disabled people, particularly those at the intersections of race, disability, class, gender, and migration. CRDJ works through research, policy analysis, community partnerships, and strategic advocacy to challenge the structural forces that marginalize disabled people and to build futures rooted in equity, belonging, and self-determination. Our work is grounded in empirical research and the practical insights of disabled people whose lives are directly shaped by federal programs and administrative decision-making.

We submit this comment in response to the Department of Homeland Security and U.S. Citizenship and Immigration Services' proposed rule, "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services" (Docket No. USCIS-2025-0205). This proposal would significantly expand the federal government's authority to collect, retain, and share biometric and genetic data from individuals connected to immigration processes, including U.S. citizens, children, sponsors, and family members.

This proposal represents a profound shift from limited identity verification toward a permanent, person-centric surveillance infrastructure, with serious implications for civil rights, disability access, racial equity, privacy, and due process. The rule fails to meaningfully acknowledge, or mitigate, the well-documented disparate impacts of biometric technologies [1, 2] on disabled people, people of color, children, and other marginalized populations. Absent robust safeguards, transparency, and accountability, the proposed rule risks entrenching racialized and ableist surveillance under the guise of administrative efficiency and fraud prevention.

The sections that follow detail CRDJ's primary objections to the proposed rule, organized around the following key areas of concern:

- Expansion of Biometric & Genetic Surveillance
- Failure to Address Racial Bias & Disparate Impact

- Disability Inaccessibility & the Risk of Criminalization
- Erosion of Privacy, Consent & Due Process

BACKGROUND

On November 3, 2025, the Department of Homeland Security (DHS), through U.S. Citizenship and Immigration Services (USCIS), issued a proposed rule titled "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services." The proposal would substantially revise existing regulations governing the collection, use, retention, and sharing of biometric information in immigration benefit adjudications, enforcement actions, and related administrative processes.

The proposed rule establishes an expansive regulatory definition of "biometrics," encompassing not only fingerprints, photographs, and signatures, but also palm prints, facial images, iris or ocular scans, voiceprints, and DNA. DHS characterizes this shift as part of a move toward a "person-centric" identity management system that relies more heavily on biometric identifiers than on biographic information. While framed as a technical modernization, this shift is significant because a person-centric biometric identity system transforms identity verification from a time-limited, case-specific process into an ongoing, body-based surveillance model that enables continuous monitoring and cross-agency tracking beyond the original purpose of data collection.

Under the proposal, USCIS would have broad discretion to require biometric submission from any individual associated with an immigration benefit or other request, including applicants, petitioners, sponsors, derivative beneficiaries, dependents, and individuals providing supporting evidence. Importantly, this authority would extend beyond noncitizens to include U.S. citizens, U.S. nationals, and lawful permanent residents when they are connected to immigration filings.

Age, DNA & Continuous Vetting

The proposed rule would remove existing age-based limitations on biometric collection, allowing DHS to require biometric data from children, including very young children, where deemed necessary. The rule would also expressly authorize DHS to request or require DNA evidence, including raw samples or partial DNA profiles, to establish biological relationships or biological sex in certain immigration contexts.

In addition, the proposal emphasizes continuous vetting, permitting ongoing identity verification and security checks beyond initial adjudication. Biometric data collected under the rule could be retained and shared across DHS components, including USCIS, Customs and Border Protection (CBP), and Immigration and Customs Enforcement (ICE), and with other government agencies, subject to applicable law. The proposal does not meaningfully limit data retention or provide detailed procedures for challenging errors or continued monitoring.

EXPANSION OF BIOMETRIC & GENETIC SURVEILLANCE

The proposed rule would substantially expand DHS's biometric and genetic surveillance authority, transforming immigration processing from a limited identity verification function into a broad, person-centric data collection regime. By adopting an expansive definition of "biometrics" and granting DHS wide discretion over when and from whom such data may be collected, the proposal enables surveillance practices far beyond what is necessary for adjudicating immigration benefits.

Under the rule, USCIS could require the collection of biometric identifiers (e.g., facial images, iris or ocular scans, voiceprints, and DNA) from any individual associated with an immigration filing, not only applicants and beneficiaries but also petitioners, sponsors, derivative family members, and others providing supporting information. This authority explicitly extends to U.S. citizens, U.S. nationals, and lawful permanent residents, significantly expanding DHS surveillance reach into the broader population.

The proposal also removes age-based limitations on biometric collection, allowing DHS to require biometric and genetic data from children, including very young children. Once collected, this information may be retained and shared across DHS components and with other government agencies, facilitating repeated vetting and long-term tracking across civil and enforcement contexts.

Of particular concern, the rule formally authorizes DNA collection as part of routine immigration processing. DNA is uniquely sensitive and immutable, revealing far more than identity alone. Incorporating genetic data into the biometric framework risks normalizing genetic surveillance as an administrative practice without clear necessity, proportionality, or limiting principles [3-10].

Collectively, these changes mark a fundamental shift toward ongoing biometric and genetic surveillance, raising serious concerns about the scale, permanence, and intrusiveness of data collection embedded in the immigration system.

FAILURE TO ADDRESS RACIAL BIAS & DISPARATE IMPACT

The proposed rule fails to meaningfully acknowledge or address the well-documented racial bias and disparate impacts associated with biometric technologies [1, 2, 11-18]. Despite extensive evidence that biometric systems, particularly facial recognition, iris scanning, and voice recognition, perform less accurately for people of color [19-22]. The proposal contains no standards for bias testing, accuracy thresholds, or mitigation measures.

This omission is especially troubling given the proposal's reliance on expanded biometric modalities as primary tools for identity verification, fraud detection, and continuous vetting. Errors in biometric systems are not evenly distributed. They disproportionately affect racially marginalized communities, increasing the risk of misidentification, heightened scrutiny, benefit delays, denials, or wrongful enforcement actions [15, 17, 18, 20, 23-25].

The rule also authorizes broad biometric data sharing across DHS components and with other government agencies, compounding the consequences of biased or erroneous biometric matches. In a system already marked by racialized enforcement and disproportionality, the expansion of biometric surveillance without safeguards risks amplifying existing inequities rather than addressing them [15, 16, 23, 26, 27].

Notably, the proposal does not include any analysis of disparate impact under civil rights laws, nor does it explain how DHS will ensure that expanded biometric collection complies with nondiscrimination obligations. By failing to confront the known racial biases embedded in biometric technologies, the rule adopts a false assumption of technological neutrality and disregards the predictable harms to communities already subject to heightened surveillance.

DISABILITY INACCESSIBILITY & THE RISK OF CRIMINALIZATION

The proposed rule fails to account for the access needs and legal rights of disabled individuals who may be subject to expanded biometric collection. Despite dramatically increasing reliance on biometric technologies, the proposal does not address how DHS will ensure meaningful access, reasonable accommodations, or alternative procedures for individuals with physical, sensory, cognitive, or psychiatric disabilities.

Many biometric systems presuppose normative bodies and behaviors [28], such as the ability to provide fingerprints, maintain eye contact for iris scanning, modulate speech for voice recognition, or follow rigid procedural instructions. Disabled individuals may be unable to meet these requirements [29]. The proposed rule offers no guidance on how disability-related barriers will be accommodated or how inability to comply will be distinguished from willful noncompliance or fraud [30].

This omission is particularly dangerous in light of extensive scholarship on the criminalization of disability, which demonstrates how disability-related differences are routinely misinterpreted by state actors as defiance, deception, or threat [31-35]. In enforcement-adjacent contexts—such as biometric collection linked to vetting, monitoring, or data sharing with law enforcement—disability can function as a risk factor rather than a protected status. This risk is heightened for disabled people of color, who already face disproportionate surveillance and punitive responses [29, 36-43].

By expanding biometric requirements without explicit disability safeguards, the proposed rule risks transforming disability-related nonconformity into grounds for heightened scrutiny, repeated biometric demands, or referral to enforcement systems. The absence of clear accommodation standards, training requirements, or protective protocols increases the likelihood that disabled individuals will be penalized for behaviors or bodily differences that are neither voluntary nor indicative of wrongdoing.

Notably, the proposal does not reference compliance with the Americans with Disabilities Act (ADA), Section 504 of the Rehabilitation Act of 1973, or related nondiscrimination obligations.

By failing to address how disability will be protected in an increasingly biometric-driven system, DHS risks entrenching ableist and punitive interpretations of difference within immigration processing and enforcement structures.

EROSION OF PRIVACY, CONSENT & DUE PROCESS

The proposed rule significantly erodes privacy, consent, and due process protections by authorizing expansive biometric and genetic data collection without meaningful limits, transparency, or procedural safeguards. By permitting DHS to require biometrics at multiple points in time and to retain and share that data across agencies, the proposal shifts immigration processing from a bounded administrative function into an open-ended monitoring system.

The rule provides limited clarity regarding when biometric submission may be required, how long data will be retained, or under what circumstances individuals may challenge the collection, accuracy, or continued use of their biometric information. Individuals subject to the rule are afforded little opportunity to provide informed consent, as biometric submission is effectively mandatory for accessing immigration benefits or participating in family-based processes. Refusal or inability to comply may carry significant adverse consequences, yet the proposal does not clearly articulate appeal rights or error-correction mechanisms.

The emphasis on continuous vetting further undermines due process by enabling ongoing surveillance without individualized suspicion or notice. Once biometric data is collected, individuals may be repeatedly screened, re-identified, or flagged based on opaque criteria, with little visibility into how decisions are made or how errors can be remedied. The proposal also facilitates extensive data sharing across DHS components and with other agencies, increasing the risk that biometric information collected for civil purposes will be repurposed for enforcement actions.

Taken together, these features concentrate substantial discretionary power in DHS while providing minimal procedural protections for affected individuals. Without clear limits on data use, retention, sharing, and redress, the proposed rule threatens fundamental principles of fairness, accountability, and proportionality that are essential to any system exercising coercive state power.

CONCLUSION

The proposed rule represents a profound expansion of federal surveillance authority that extends far beyond the administration of immigration benefits. As outlined above, the rule would normalize expansive biometric and genetic data collection, disregard well-documented racial bias and disparate impacts, fail to protect disabled individuals from exclusion and criminalization, and erode fundamental protections related to privacy, consent, and due process.

Taken together, these deficiencies are not technical oversights. They reflect a structural shift toward an immigration system that treats biometric surveillance as routine and difference as suspicion. By embedding broad discretion, continuous vetting, and inter-agency data sharing into core immigration processes—without meaningful safeguards—the proposal risks transforming everyday administrative interactions into mechanisms of lifelong monitoring and control.

The harms of this approach would not be evenly distributed. Communities that already experience heightened surveillance and punitive state responses would bear the greatest burden. For racialized and disabled individuals in particular, the convergence of biometric technologies, enforcement pathways, and the misinterpretation of difference as noncompliance creates a heightened risk of exclusion, escalation, and criminalization.

If finalized, this rule would set a dangerous precedent by expanding biometric and genetic surveillance without adequately accounting for civil rights, equal access, or the long-term consequences of data permanence and misuse. It would entrench surveillance as a condition of family unity, legal status, and participation in civic life, undermining trust in public institutions and weakening fundamental principles of fairness and accountability.

For these reasons, CRDJ urges DHS to withdraw the proposed rule. At a minimum, any future rulemaking must meaningfully address racial bias and disparate impact, ensure robust disability accommodations and safeguards against criminalization, establish clear limits on biometric and genetic data collection and use, and restore meaningful protections for privacy, consent, and due process [10]. Without these changes, the proposal risks causing lasting harm to individuals, families, and communities; further entrenching inequities the immigration system should be working to dismantle, not deepen.

If you have any questions, please feel free to contact Dr. Kate Caldwell at kcaldwell@law.northwestern.edu.

Sincerely,

Kate Caldwell, PhD
Director of Research & Policy

Jamelia Morgan
Founder & Faculty Director

Jordyn Jensen
Executive Director

Dimitri Nesbit
Civic Planning & Design Manager

Center for Racial and Disability Justice
Northwestern University Pritzker School of Law

REFERENCES

1. Barocas, S. and A.D. Selbst, *Big data's disparate impact.* Calif. L. Rev., 2016. **104**: p. 671.
2. Selbst, A.D., *Disparate impact in big data policing.* Ga. L. Rev., 2017. **52**: p. 109.
3. Clayton, E.W., et al., *The law of genetic privacy: applications, implications, and limitations.* Journal of Law and the Biosciences, 2019. **6**(1): p. 1-36.
4. Costello, R.Á., *Genetic data and the right to privacy: towards a relational theory of privacy?* Human Rights Law Review, 2022. **22**(1): p. ngab031.
5. Kindt, E.J., *Privacy and data protection issues of biometric applications.* A Comparative Legal Analysis, 2013. **12**.
6. Wan, Z., et al., *Sociotechnical safeguards for genomic data privacy.* Nature Reviews Genetics, 2022. **23**(7): p. 429-445.
7. Smith, M. and S. Miller, *Biometric identification, law and ethics*. 2021: Springer Nature.
8. Cech, M., *Genetic Privacy in the Big Biology Era: The Autonomous Human Subject.* Hastings LJ, 2018. **70**: p. 851.
9. Hallinan, D., M. Friedewald, and P. De Hert, *Genetic Data and the Data Protection Regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data?* Computer Law & Security Review, 2013. **29**(4): p. 317-329.
10. Kavanagh, M.M., et al., *Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations.* The Lancet HIV, 2019. **6**(1): p. e51-e59.
11. Michael, K., et al., *Biometrics and AI bias.* IEEE Transactions on Technology and Society, 2022. **3**(1): p. 2-8.
12. Valdivia, A., J.C. Serrajòrdia, and A. Swianiewicz, *There is an elephant in the room: Towards a critique on the use of fairness in biometrics.* AI and Ethics, 2023. **3**(4): p. 1407-1422.
13. Jones, G. and S. Wang, *Disparate Impact of Surveillance: The Precarious Condition of the Poor's Right to Privacy.* A Reexamination of Wisconsin v Yoder: An Untenable Holding in the Modern Era Disparate Impact of Surveillance: The Precarious Condition of the Poor's Right to Privacy: p. 28.
14. Sokhansanj, B.A., *Beyond protecting genetic privacy: understanding genetic discrimination through its disparate impact on racial minorities.* Colum. J. Race & L., 2012. **2**: p. 279.
15. Garvie, C., *The perpetual line-up: Unregulated police face recognition in America*. 2016: Georgetown Law, Center on Privacy & Technology.
16. Richardson, R., J.M. Schultz, and K. Crawford, *Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice.* NYUL Rev. Online, 2019. **94**: p. 15.
17. Benjamin, R., *Race After Technology: Abolitionist Tools for the New Jim Code*. 2019: Polity Press.
18. Ferguson, A.G., *The rise of big data policing: Surveillance, race, and the future of law enforcement*, in *The rise of big data policing*. 2017, New York University Press.

19. Buolamwini, J. and T. Gebru. *Gender shades: Intersectional accuracy disparities in commercial gender classification*. in *Conference on fairness, accountability and transparency*. 2018. PMLR.

20. Raji, I.D. and J. Buolamwini. *Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial ai products*. in *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*. 2019.

21. Cavazos, J.G., et al., *Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?* IEEE transactions on biometrics, behavior, and identity science, 2020. **3**(1): p. 101-111.

22. Koenecke, A., et al., *Racial disparities in automated speech recognition.* Proceedings of the national academy of sciences, 2020. **117**(14): p. 7684-7689.

23. Eubanks, V., *Automating inequality: How high-tech tools profile, police, and punish the poor*. 2018: Macmillan+ ORM.

24. Whittaker, M., et al., *AI now report 2018*. 2018: AI Now Institute at New York University New York.

25. Osoba, O.A., W. Welser IV, and W. Welser, *An intelligence in our image: The risks of bias and errors in artificial intelligence*. 2017: Rand Corporation.

26. Brayne, S., *Big data surveillance: The case of policing.* American sociological review, 2017. **82**(5): p. 977-1008.

27. Angwin, J., et al., *Machine bias*, in *Ethics of data and analytics*. 2022, Auerbach Publications. p. 254-264.

28. Zijlstra, S.Y., *Becoming Biometric*, in *International Development Studies*. 2021, Wageningen University & Research: Netherlands. p. 64.

29. Lee, T., *Biometrics and disability rights: legal compliance in biometric identification programs.* U. Ill. JL Tech. & Pol'y, 2016: p. 209.

30. Dorfman, D., *Fear of the disability con: Perceptions of fraud and special rights discourse.* Law & Society Review, 2019. **53**(4): p. 1051-1091.

31. Ben-Moshe, L., *Decarcerating disability: Deinstitutionalization and prison abolition*. 2020: U of Minnesota Press.

32. Perry, D. and L. Carter-Long, *The Ruderman white paper on media converage of law enforcement use of force and disability.* Boston, MA: Ruderman Foundation, 2016.

33. Morgan, J., *Disability, policing, and punishment: An intersectional approach.* Okla. L. Rev., 2022. **75**: p. 169.

34. Santoro, S. and J.N. Morgan, *DISABILITY CRIMINALIZATION: A PRIMER.* American Criminal Law Review, 2025. **62**(4): p. 1127-1150.

35. Ricciardelli, L.A., L. Nackerud, and A.E. Quinn, *The criminalization of immigration and intellectual disability in the United States: A mixed methods approach to exploring forced exclusion.* Critical Social Work, 2020. **21**(2): p. 18-40.

36. Mankoff, J., et al., *Areas of Strategic Visibility: Disability Bias in Biometrics.* arXiv preprint arXiv:2208.04712, 2022.

37. Saltes, N., *'Abnormal'bodies on the borders of inclusion: Biopolitics and the paradox of disability surveillance.* Surveillance & Society, 2013. **11**(1/2): p. 55-73.

38. Nair, P., *Surveilling Disability, Harming Integration.* Columbia Law Review, 2024. **124**(1): p. 197-271.

39. Haber, E., *Racial recognition.* CARDozo L. REv., 2021. **43**: p. 71.
40. Moy, L.M., *A Taxonomy of Police Technology's Racial Inequity Problems.* U. Ill. L. Rev., 2021: p. 139.
41. Broussard, M., *More than a glitch: Confronting race, gender, and ability bias in tech*. 2023: MIT Press.
42. Maddern, J. and E. Stewart, *Biometric geographies, mobility and disability: Biologies of culpability and the biologised spaces of (post) modernity*, in *Towards enabling geographies*. 2016, Routledge. p. 237-252.
43. Capers, I.B., *Race, policing, and technology.* NCL Rev., 2016. **95**: p. 1241.