

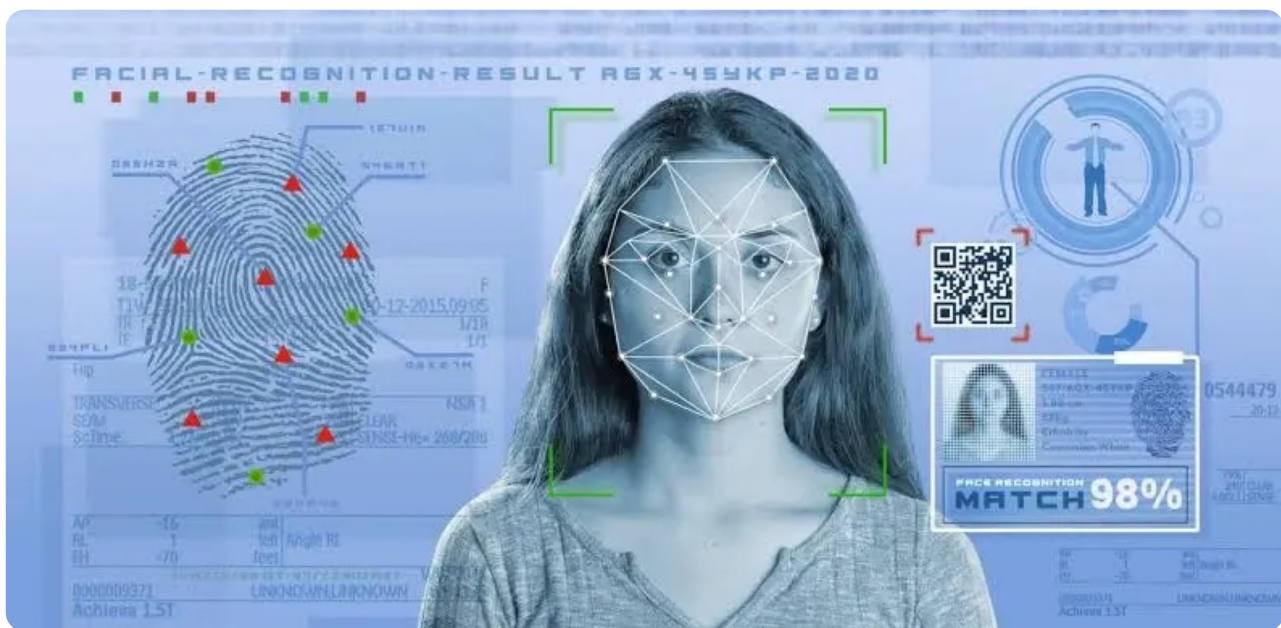
Biometric Borders and Unequal Citizenship: Democratization and Citizenship in the United States

Mohd. Ruhul Amin

Aug 23, 2025

Abstract

This article examines how biometric border systems can create unequal experiences of citizenship and migration control in the United States. It describes facial recognition, fingerprinting, iris scanning, and interconnected identity databases as technologies that may improve verification and reduce fraud while also expanding surveillance and distributing errors unevenly. The article mentions false matches, failed identification, secondary inspection, questioning, detention, and weak appeal procedures as consequences that may disproportionately affect migrants, asylum seekers, and individuals with limited documentation or legal support. It also discusses how identity infrastructure can divide populations into trusted and suspect categories, creating different burdens of proof, monitoring, and correction. Democratic legitimacy therefore depends on necessity, proportionality, transparent watchlist governance, contractor accountability, limited data retention, independent testing, and access to human review. The article concludes that border efficiency cannot justify irreversible harm caused by technical failure, discriminatory error patterns, or inaccessible procedures for correcting identity records.



Biometric borders transform the human body as a credential, into a search-key and into a risk signal. In August 2025, biometric verification systems such as facial recognition, fingerprints will become a significant part of travel and immigration in the United States. While quicker verification drives down delays and curbs fraud, automation also broadly sprays errors. Problems of unequal citizenship arise when one group experiences seamless processes, but others experience a series of rules, scrutiny, and weak notice and appeal mechanisms. Whether border technology is needed, proportionate, subject to review, and can be corrected are critical for the democratic legitimacy of such technology.

New technology, known as biometric borders, will offer a more rapid identification and enhanced fraud prevention facility using fingerprints, facial photography, scan of the iris or composite systems. There is no consistency in terms of accuracy for populations, environments, devices and accuracy of databases. Delay, questioning, detention and investigation may be given in the event of a false match, and what may be solved by a non-match can cause problems for entry or getting status. The scale of surveillance also shifts, as items are more easily identified in different locations, as well, through automation. Rights analysis needs to consider the need, purpose, dispersion of error, human oversight, management of watchlists, data retention, accountability of contractors, and redress opportunities prior to the incurable harm.

Distinguished citizenship may result from partitioning of identity infrastructure, separating so-called "trusted" from "suspect" groups. The different burdens of proof, appeal and surveillance of citizens, permanent residents, visa holders, asylum seekers and undocumented migrants. While this variation is partially attributable to formal legal

categories, a more administration-specific, and technically designed, difference would further the separation. If a person has an established document, fluency in language and legal help, he can correct an error but another person can't because of the database mismatch.

A perfect level of equality means more than identical technology, however. Procedures must: include accessible notice, interpreters, counselling, irrational consequences, independent review and alternatives for individuals who do not meet the biometric requirements.

Digital identity can help decrease duplication, expedite verification, facilitate portability and link up separated individuals to services. If access to the same infrastructure requires biometrics that are unreliable, devices that are inaccessible, erroneous records, or opaque data sharing, it can be even more complicated to access lawful assistance, which helps to further imply legal precarity. Exclusion, privacy, security, vendor lock-in and an inappropriate technology are identified as key risks in World Bank ID4D guidance. A rights-based approach requires data minimisation, purpose limitation, data correction, human oversight, secure authentication, independent oversight and an alternative to the digital approach. Never make a technical error into a deprivation of food, movement, legal status or medical care as a result of convenience.

Data on refugees is highly sensitive, as disclosure of this information, for example, may reveal family ties, political involvement, whereabouts, ethnic origin or claims for protection. UNHCR guidance puts an emphasis on registration and identity management, with the protection of personal data. When the assistance requires registration, consent can become complicated – refusal of it will have significant material repercussions. Thus, in the political sphere, it is important that governance is founded on legitimate benefit and need and not an imagined free market of exchange.

Data sharing agreements should have a set of recipients, a data retention time limit, security measures, audit trails, and sanctions. Future changes in politics have to be taken into account as risk assessment – a database, which is safe under one administration, may become dangerous under another.

The so-called "refugee or migrant" status is a legal avenue but not an exhaustive description of inclusion. Even with recognition, there may remain obstacles to access to housing, employment, health services, education, financial services, mobility and social services. Documents remain hard to verify, agencies employ different rules, and local service providers are stymied. Service-access approach involves the entire process to

eligibility and receipt.

Practical citizenship is influenced by waiting time, travel cost, language support as well as appeal, discrimination and data sharing. Ordinary institutions' repeated and affirming recognition of status and prompt, remedying response to instances of failure becomes a credible measure of legal inclusion.

The process of institutional constraints is through independence, capacity, transparency and coordination. If a court is not truly independent and lacks an adequate leave of the way to access court remedies, it isn't very independent. Even the professional civil service would be susceptible to loyalty tests if it has no secure offices. Election officials must be equipped, secure, lawful and trusted.

In order to enjoy media freedom, journalists need information and protection from retributive investigation. Constraints take hold when multiple institutions are able to identify, detect, delay and mitigate abuse. Redundancy is also a way to lessen the risk of capture causing breakdown of the entire system of accountability.

Proportionality offers a structured approach to appraising rights restriction which is under pressure. There has to be a clear purpose and the measure must serve that purpose, there has to be a serious consideration of a less restrictive alternative, the final burden must be commensurate with the expected benefit. Weakness of the method through the absence of evidence and the official assertion being considered proof. A strong review considers scope, length, exemptions, quality of the data and the distribution and changing circumstances. Proportionality also necessitates periodic re-evaluation as an action that might be necessary in a crisis may turn out to be unnecessary in an after crisis scenario where facts, capacity or alternatives may shift.

There are four levels of measurement – commitment, capacity, behaviour, outcome. The combination of Treaty ratification and capacity revealed by budgets and staffing documents commitment. Administrative decisions and enforcement patterns reflect behaviour and safety, access, equality and remedy reflect outcomes. When all four are used together it will not be as if you were playing a game of false optimism.

For a country, there are two ways of doing better when there is abuse; document, or do better with some other economic change. Mechanisms are identified in the light of longitudinal evidence, matched comparison, case tracing and interview with the affected communities. Data quality is also important, as official reporting may miss violations, civil society data may focus on visible violations, and legal databases may fail to capture

cases of intimidation and informal settlement.

While connection between databases turns risk to another level, interoperability makes access simpler. A change of one system should be propagated in a legal manner and unverified allegations should not automatically proliferate across unrelated systems. Every aspect of governance requires a data map that specifies what fields are for, their intended usage, who will receive the data, how long the data will be held and whom it can be remedied. Mission expansion or unauthorized use can be identified from access logs, and independent audits.

Technical specifications should facilitate selective disclosure: no more information should be provided to the service provider than is necessary for him to make a certain decision. Integration is rights-protecting and, as a result, does not neglect or cross institutional boundaries.

Basic needs should be safeguarded during challenging situations of identity or status changes in service continuity. Emergency health access, supervised manual verification, and temporary credentials and provisional enrollment are ways to avoid an administrative problem resulting in homelessness, untreated illness, and interruptions in schooling. Fraud controls are required for safeguards, but verification expenses should be in line with the service which it protects. Agencies should document the results of the dispute and what the ongoing system problems are. Continuity rules uphold dignity and enhance the quality of data as corrections are made via a formal review process rather than re-denying it at different service counters.

Though constitutional protection is different for different locations, status, and legal doctrine at the American border, constitutional legitimacy demands clear governance. Information should be provided to travelers regarding the collection, retention, sharing and available alternatives for biometric. Watchlist and matching systems need to be audited to check for a fair distribution of errors and mission expansion. Independent testing should not just be considered proprietary – in vendor contracts.

Frictionless movement alone can not be the cornerstone of a democratic border. Some "extra" policing may be perfectly legitimate, but there should be penalties—and monitoring. There is documented criteria for secondary inspection, device search, data retention and referral to follow. Once the technical suspicion of citizenship is hard to deny, citizens' citizenship becomes a one with a practical inequality in spite of their formal legal citizenship.

For the inclusion to happen, the whole administrative chain from legal recognition to accessible access of services is required. However, digital identity and biometrics can help in that journey, provided that systems remain inclusive, secure, correctable and human verifiable. Technical failure and opaque data sharing must not result in an irreversible consequence for the refugee or migrant. Democratic citizenship is evaluated as much by what happens at regular points of contact, as by what is promised in the constitution.

Infrastructure for identity is legitimate the more it grows the rights without the vulnerability becoming permanent surveillance. There is a need for continuity in essential services as identity issues are pending. Data minimization helps mitigate the risks of data cyber security and the possible political misuse in the future.