

Digital Identity, Legal Precarity, and the New Architecture of Democratization and Citizenship

Mohd. Ruhul Amin

Aug 8, 2025

Abstract

This article presents digital identity as both an enabling infrastructure and a potential source of legal precarity within democratization and citizenship. It describes how digital credentials and biometric verification can improve portability, reduce duplication, and accelerate access to public services, humanitarian assistance, finance, and mobility. The article mentions that inaccurate records, failed biometric matches, inaccessible devices, vendor-controlled platforms, and opaque data-sharing arrangements may deny individuals essential rights without effective human intervention. Refugees, migrants, and undocumented populations face heightened risks because identity records may reveal sensitive information concerning family relationships, political history, ethnicity, location, or protection claims. The analysis emphasizes data minimization, purpose limitation, secure authentication, independent oversight, correction rights, selective disclosure, and non-digital alternatives. It concludes that digital identity contributes to democratic citizenship only when systems remain transparent, correctable, inclusive, reviewable, and capable of maintaining essential services while identity or status disputes are being resolved.



Digital identity is evolving as the digital key to accessing public services, finances, and mobility, and even humanitarian aid. That architecture provides an efficiency as well as a new kind of legal precarity, in August 2025. Without any kind of human decision-maker, access can be denied to the needed services as a result of a record error, failing to match biometric data, when the technology is inaccessible, or as a result of an opaque decision on data sharing. Modes of automated identity can make authority less transparent, and contestable administration is a core component of the process of democratisation and citizenship. Non-digital options, human review, correction and inclusion and privacy therefore must be taken into account early in the design phase with a rights-driven approach.

Digital identity can help to cut down on duplication, improve the speed and efficiency of verification, facilitate portability, and link refugees 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.

There is no such thing as too little data when it comes to refugees given that revealing information may lead to a leak of family connection, political background, enclave or national origin, or a refugee claim. UNHCR guidance is emphasising the importance of registration and identity management along with protection of personal data. The issue of consent becomes complex when assistance is reliant on registration because there can be significant material consequences if consent is refused. 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.

Definitions, reminders, security controls, audits and remedies are required with data-sharing agreements. 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.

Refugee status is a legal pathway and not a comprehensive picture of inclusion. But, even though someone is recognized, they may be hindered from obtaining housing, jobs, health care, education, banking, travel, and social protection opportunities. Documentation may still be challenging, agencies may be interpreting different rules and guidance may not exist with local service providers. A service-access approach encompasses the whole process of administration from eligibility through to receiving a service.

Practical citizenship is dependent on waiting times, travel costs, language support, the need for digital tools, 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.

A boundary in identity infrastructure between trusted and suspect populations can result in unequal citizenship. Statutory requirements for citizenship, permanent residence, visa possession, asylum seeking, and illegal immigrants vary with regards to requirements for proof or appeal and surveillance. Part of the difference is accounted for by formal legal classification but administrative and technical design can increase the difference. 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.

As of the end of 2023, UNHCR estimated that the number of forcibly displaced people amounted to 117.3 million, and this figure is likely to have surpassed 120 million by the end of April 2024. Scale puts great strain on asylum systems, host communities and humanitarian institutions. Numbers, however, blanket administrative diversities. A refugee registered in one locality, can, with a common card have access to services across health, education, employment and Municipality; another refugee registered in each locality.

Comparative analysis should therefore go hand in hand with a local implementation of national law. Achieving inclusion requires co-ordination, financial means, legal regulations and immunity from political scapegoating.

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. Loyalty tests are possible if you have an insecure job in the civil service. Election officials require materials and equipment, physical security, legal security, and credibility.

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. It also makes less likely for any one body to be captured and thus disable the entire system of accountability.

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 with the help of longitudinal evidence, matched comparisons, case tracing and interviews with affected communities. Data quality is also important as official recording might not count violations, civil society reporting might focus on the visible case and legal databases might exclude informal settlements or intimidation.

Fundamental rights are resilient when their protection is constant; it remains steady in times of insecurity, fear and quasi-political imbalance. The most difficult situations are those where involve unpopular groups, disputed speech, groups of migrants, prisoners, protesters and communities labeled as 'security risks'. Equal treatment in non-crisis times provides some meager data on the strength of the constitution. Resilience is reflected in upholding, in times of pressure, due process, individualized assessment, legal counsel, review and reasoned justification in institutions.

Distributional analysis will always play a role as a formally neutral rule can still have a concentrated geographic, disability, language, income, immigration or unequal access to digital systems impact. Thus a doctrinal review as well as an empirical investigation of the implementation of rights protection must be carried out.

Pointing to the fact, that the databases were interoperable, can help to simplify the access, but the connection between databases meets the scale of risk. The correction of one system should be legally propagated; an unverified alleged statement should not automatically get propagated across unrelated services. There is a need to have a data map that shows what fields need to be filled out, what they are for, who they are for, how long do they need to be stored and who is responsible for corrections. 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-protective when none of the boundaries of institutions have been overcome by convenience.

Basic needs should be sustained in the event of identity and status dispute through the use of 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 should be required on safeguards and the cost of checking them should be commensurate with the safeguard being checked. 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.

There is a need to give special attention to interoperability. Linkage between identity systems can be helpful to reduce duplication of registration, but having identity systems that are linked across numerous agencies increases the scope of potential misuse and

error. Sometimes credentials exist that give access based on purpose, and not giving access to a full personal record. Technical architecture needs to facilitate selective disclosure, correctness across interrelated system, and easy record of who accessed data and for what reason.

There needs to be some real force behind the human review. A staff member cannot undo an automated result, and will only provide symbolic assistance. Appeals require clear rules and deadlines, easy access to evidence, interpreters and a measure of services during the appeal process to meet essential needs. If not, there is a long security threat to those who would otherwise have resources to dispute a database.

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. Carrying irreversible consequences due to technical failure or opaque data sharing should not be the lot of refugee and migrants. Democratic citizenship is evaluated as much by what happens at regular points of contact, as by what is promised in the constitution.

When the new rights increase, and the consequent vulnerability does not lead to permanent surveillance, then identity infrastructure becomes legitimate. There is a need for continuity in essential services as identity issues are pending.