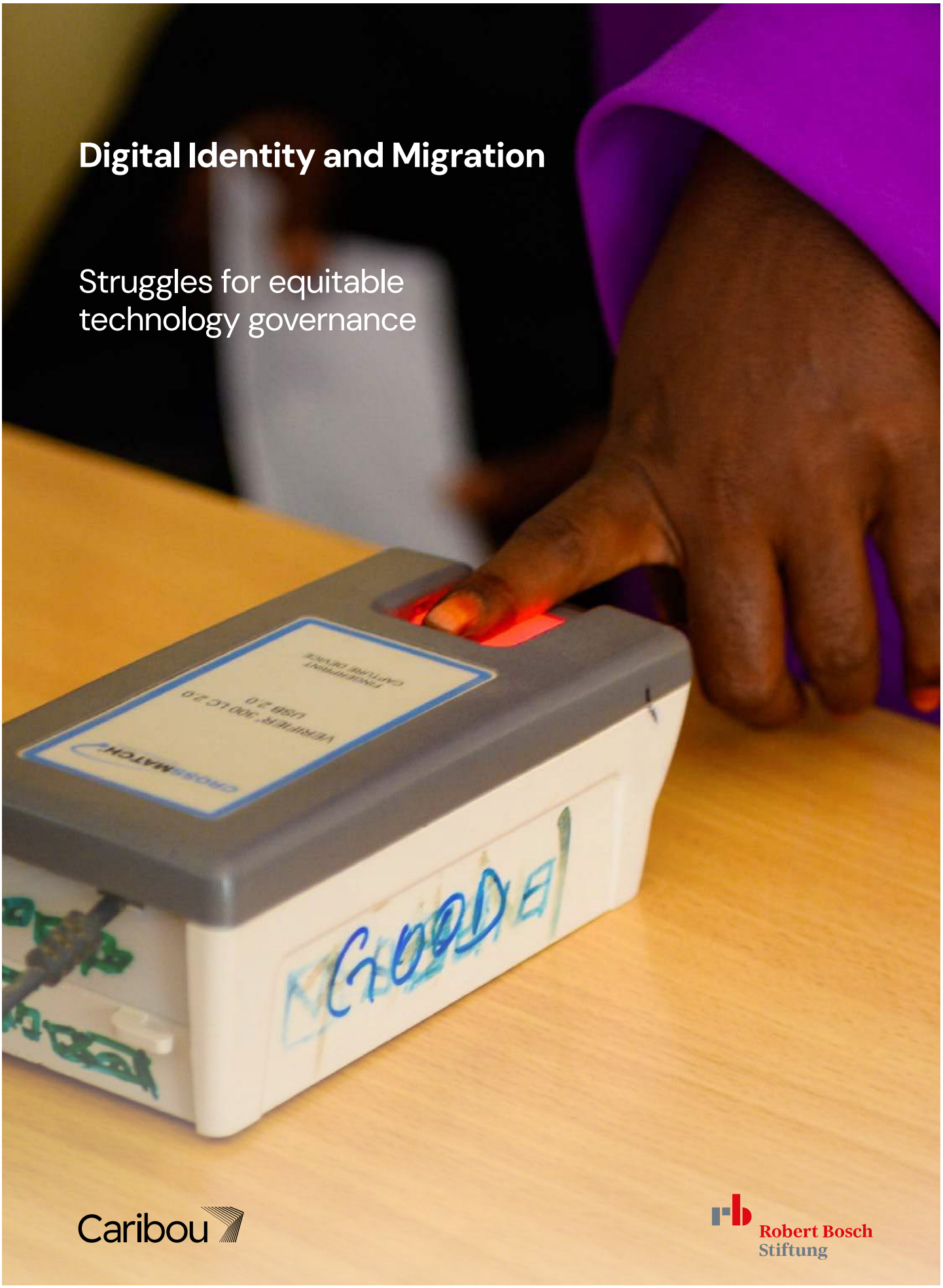
Digital Identity and Migration

Struggles for equitable technology governance



Caribou

Robert Bosch Stiftung

Authors

This report was written by Margie Cheesman. It synthesizes the original empirical work of the Identity in the Age of Migration project team: Aaron Martin, Emrys Schoemaker, Keren Weitzberg, Yussuf Bashir, Asha Jaffar, Saada Loo, Thea Kirsch, Marianne Samaha, Ana Werkstetter Caravaca, Sophie Benanni-Taylor, Isadora Dullaert.

Recommended citation

Cheesman, Margie. *Digital Identity and Migration: Struggles for Equitable Technology Governance.* Caribou Publishing, 2026. https://caribou.global/publications/digital-identity-and-migration-struggles-for-equitable-technology-governance

DOI: 10.64329/QZRR3416

Published February 2026

Caribou delivers fund management, learning partnerships, and research, advisory, and evaluation services, supporting organizations worldwide to build more inclusive and ethical digital economies.

www.caribou.global

This report was produced by Caribou in partnership with the Robert Bosch Stiftung GmbH. The views presented in this paper are those of the authors and do not necessarily represent the views of the Robert Bosch Stiftung GmbH.

Robert Bosch Stiftung

Accessibility

This PDF has been designed using Adobe's PDF accessibility evaluation tool, a checklist of considerations to support compliance with the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, among the most comprehensive and widely-used accessibility standards for digital content.

Cover image: Klein Ongaki, with funding from Privacy International

Contents

Introduction

Digital identity has emerged as a booming industry, and as a critical battleground in global struggles for equitable technology governance. Despite progressive rhetoric around new and decentralized models of identity management, prevailing systems remain highly centralized and concentrated in the hands of governments and private companies. The European Commission has adopted legislation that mandates member governments to develop digital identity wallets, emphasizing user empowerment and data protection. But without adequate safeguards these efforts risk reproducing existing exclusions under new technological guises.

It is now well known that migration management contexts serve as crucial testing grounds where many identity technologies are first deployed and refined. Learning from the experiences of the most vulnerable can help decision-makers understand and anticipate risks that affect everyone. From traditional landing cards to sophisticated biometric checks at borders, identity systems embody a fundamental duality: they include and exclude, supporting both recognition and surveillance.[1] They can offer pathways to care and targeted welfare provision while simultaneously enabling hostile environment policies of mobility control and population monitoring.

1 Weitzberg et al., "Between Surveillance and Recognition: Rethinking Digital Identity in Aid."

Governments are increasingly rolling out new identification initiatives: from the imminent EU Digital Identity Wallet to various mandatory schemes recently proposed in the UK such as the BritCard. As states harden border control measures for political gain, examining how diverse identity systems operate within their specific social and institutional contexts is critically important if governance actors are to understand their impacts on rights, inclusion, and democratic governance—including, but not only, for migrants.

The experiences of migrants, refugees, and asylum seekers reveal fault lines in digital identity systems that ultimately affect all marginalized groups. These systems are often designed to enable efficient, secure forms of political recognition and access to services. At the same time, migrants—who navigate multiple jurisdictions, carry diverse documentation histories, and face heightened surveillance risks—expose the limitations and exclusions entailed in the design and use of digital identity systems. These fault lines highlight broader patterns of digital exclusion that can also affect the elderly, disabled persons, ethnic minorities, and economically disadvantaged populations. Understanding these challenges requires recognizing that digital identity systems are never merely technical solutions that can be evaluated as simply good or bad but rather are inherently political and social infrastructures that embed particular values, assumptions, and power relations, making them never neutral in their effects on different populations.

Caribou's research project Identity in the Age of Migration (November 2023–September 2025) examined the social implications of digital identity systems, the power structures shaping their adoption, and how migrants' experiences could inform more equitable approaches to identification. The research team adopted a multi-sited comparative methodology, with an interest in understanding:

- Global North and Global South dynamics
- The significance of different political and bureaucratic environments and legal statuses of refugees, asylum seekers and other categories of migrants
- Key institutional settings—from intergovernmental to state to humanitarian—and their crossovers

This multi-sited research involved in-depth fieldwork with migrants, asylum seekers, and refugees in Kenya and Germany, participatory workshops and interviews with identity governance stakeholders, including state, EU, and UN agencies, and comprehensive literature reviews. Funded by the Robert Bosch Stiftung through its Global Issues strategic partnership on migration, this work contributes to international cooperation on migration policy, governance, and practice, aiming to support humane, far-sighted, and sustainable approaches to identity management in the digital age.

The project addressed three key research questions:

1 **What are the implications of identity innovation in migration contexts?**
This involved examining the technological choices shaping the outcomes of cutting-edge identity innovations. This report focuses on insights from three notable case studies: the EUDI Wallet, the UK BritCard, and the Red Cross DIGID initiative. These cases exemplify how one paradigmatic new model of identity innovation—the digital wallet—has emerged, with varying implications for migrants and migration management.

2 **How do institutional power dynamics shape the implementation and outcomes of digital identity systems?**
The project examined the governance and decision-making processes that strongly influence the outcomes of digital identity projects. This report zooms in on humanitarian aid, where the institutional landscape is rapidly changing amid unprecedented funding cuts and calls for structural reform. This research involved examining who controls humanitarian identity systems, how decisions are made, and which interests are prioritized.

3 **How can migrant experiences inform the design of more inclusive and equitable identity systems for all?**
The research team investigated the lived experiences of migrants navigating digital identity systems in two contrasting national settings: Kenya and Germany. Our research documented how design choices and power structures translate into concrete barriers to accessing rights, services, and opportunities for marginalized groups. We present migrant-informed principles for more equitable systems, demonstrating how attention to migrants' experiences can benefit broader populations facing socioeconomic exclusion in the digital age.

The implications of identity innovation in migration contexts

Evaluating digital wallets

Among new models of identity management, one key paradigm has recently emerged: the digital wallet.[2] Digital wallets represent a significant technological shift in how identity credentials are stored, managed, and shared across borders. These systems promise significant improvements on traditional, centralized surveillance schemes: enhanced security, user control, and interoperability.

Our research engaged with key stakeholders, including the Open Wallet Foundation and MOSIP. We followed notable digital wallet projects, examining proposed and existing solutions across regional, state-led, and humanitarian sector governance contexts. These projects included the European Commission's EUDI Wallet, the UK BritCard, and the Red Cross DIGID initiative. We investigated the diverse and promising features of the digital wallet model and the critical concerns it presents in relation to implementation and access.

2 Cheesman, *Digital Wallets and Migration Policy: A Critical Intersection*.

CASE STUDY 1

The EU Digital Identity Wallet

The European Union's Digital Identity (EUDI) Wallet initiative represents an ambitious intergovernmental digital infrastructure project with significant implications on worldwide standards for digital identification. Through a smartphone app, European citizens, residents, and businesses will be able to store digital equivalents of official documents (e.g., university degrees, health information, transport tickets, driving licenses) and access public and private services across the EU.

Member States will make wallets available to every citizen, resident, and business by the end of 2026, with a target for the wallet to be available to 80% of EU citizens by 2030. Four large-scale pilot projects launched in April 2023, involving over 350 entities from 26 Member States, Norway, Iceland, and Ukraine, and scheduled to continue through 2025. Adoption will vary significantly across Member States, dependent on digital maturity, politics, and trust in each EU country.

The EUDI Wallet exemplifies the potential benefits associated with decentralized wallet models:

- Enhanced user privacy through selective disclosure (users can choose which identity details to share for specific purposes)
- Unlinkability protections to prevent tracking of user behavior across services
- Reduced dependency on US big tech authentication systems, supporting EU digital sovereignty
- Standardized identity verification across public and private services within the EU

However, these benefits target EU citizens, legal residents, and businesses; the proposed scheme excludes many migrants by design.[3]

3 Dullaert, *The European Digital Identity Wallet: Why It Matters and to Whom*.

The promise of digital wallets

Digital wallets are electronic systems that store both information and value, enabling users to manage identity credentials, personal data, currency, and tokens, primarily through mobile devices but also via cloud hosting.[4] The technology encompasses various approaches, from decentralized, user-controlled systems to government-owned and -managed digital infrastructures, each with distinct implications for user autonomy, data protection, and rights. Digital wallets offer potential solutions to fragmented identity systems and financial exclusion that migrants, asylum seekers, and refugees often face. They propose to provide a secure, persistent method of storing identity credentials across borders.

Potential benefits of digital wallets include:

- Reduced dependency on paper-based documents, which can be lost, damaged, or retained by third parties
- Self-managed identity verification without institutional intermediaries
- Integration of wider key services (such as financial services) with identity management
- Enhanced privacy through selective disclosure features
- The harmonization of fragmented data systems across institutions

4 Cloud-hosted digital wallets store sensitive data and cryptographic keys on remote servers rather than locally on the user's device. While device-based wallets keep all data locally on smartphones or dedicated hardware, cloud-hosted versions sacrifice user control and privacy in exchange for the ability to access funds and data from any internet-connected device through provider-managed servers. Examples of cloud-hosted solutions include cryptocurrency exchange wallets, mobile payment apps, and browser-based services.

CASE STUDY 2

The UK BritCard

In contrast to the EUDI Wallet's citizen-focused model, the BritCard represents a migration-control-first approach to digital identity recently proposed in the UK and currently under consideration by Downing Street. Championed by Labour Together, the proposal envisions a mandatory, universal digital identity credential specifically designed to prevent illegal migration through digitized bureaucratic checks.[5] The BritCard would be built upon existing GOV.UK infrastructure, rebranding the current government identity wallet as the "BritCard app" with an estimated development cost of £400 million and annual administration costs of £10 million.

This digital wallet explicitly targets migration control, with supporters believing it will "streamline right-to-rent and right-to-work checks, reduce welfare fraud, and send a clear message that the UK is not 'soft touch' on illegal migration."[6] The proposal claims this solution will prevent future Windrush-style exclusions by creating "a canonical, up-to-date view of the set of people with the right to be in the country."[7]

5 Cheesman et al., "The Britcard: Progressive or Concerning?"
6 Labour Together, *BritCard: A Progressive Digital Identity for Britain*, 10.
7 Labour Together, *BritCard: A Progressive Digital Identity for Britain*, 18.

Divergent approaches, critical implications

Our research revealed how the digital wallet is not a unified model of innovation. Instead, digital identity wallets can serve fundamentally different political projects with diverse implications for migrant communities' access to rights, services, and socioeconomic inclusion.

1 **Technical exclusion mechanisms**
The proposed BritCard uses migration concerns as an entry point for a system that would ultimately affect all UK residents. It is an enforcement-oriented rather than rights-based digital solution, explicitly targeting those deemed "irregular." By contrast, EUDI claims universal empowerment for EU citizens and residents, but creates broader systematic exclusion of all non-EU migrants regardless of legal status through its technical requirements; an EU e-ID and advanced smartphone access are prerequisites. In our research, one migrant participant suggested, "it's not for people like me."[8] Meanwhile, DIGID is specifically designed for excluded populations (refugees and other humanitarian recipients) and the wallet provides inclusive access through printed QR codes for non-smartphone users. However, DIGID represents an isolated workaround: a short-term humanitarian initiative unintegrated with wider services and systems in Kenya.

2 **Data protection, surveillance, and profit concerns**
Digital wallet schemes hold surveillance risks if implemented without strong standards and safeguards. EUDI represents a progressive approach to digital identity, framed around GDPR compliance, privacy-by-design principles, and selective disclosure for users. At the same time, security vulnerabilities on low-quality devices risk increasing hacking, and there are currently no comprehensive frameworks for cross-border enforcement and data transfer protections. Civil society groups warn about EUDI's potential to augment government tracking capabilities when put in practice by Member States.[9] The No Phone Home campaign against the ISO/IEC 18013-5 standard demonstrates how digital identity standards remain contested: privacy advocates are currently challenging server retrieval capabilities that enable tracking, emphasizing that selecting privacy-preserving standards is as critical as choosing between centralized and wallet-based architectures. The BritCard's unclear data governance frameworks, combined with its explicit immigration enforcement objectives, raise significant concerns about how migrant data will be collected, stored, and potentially shared across government departments, as well as concerns around scope creep. In both these schemes, commercial involvement may create financial incentives for expanded migrant surveillance.

8 Kirsch et al., *"It's Not For People Like Me": Centering Migrants' Perspectives in the EUDI Wallet Debate in Germany*.
9 Dullaert, *The European Digital Identity Wallet: Why It Matters and to Whom*.

3 **Technological solutionism**

In different ways, these case studies illustrate how technological interventions can inadvertently distract from deeper political challenges. Rather than confronting hostile environment policies that create migrant precarity, the BritCard digitizes those policies. While EUDI was not designed as a migration solution, its implementation occurs within existing legal frameworks that maintain barriers preventing migrants from obtaining foundational identity documents in EU Member States. DIGID advances a new workaround for humanitarian recipients lacking recognized IDs. In humanitarian actors' struggles to tackle the underlying causes of refugees' exclusion from mainstream systems, DIGID remains a standalone project offering a functional rather than foundational solution. These examples highlight a broader pattern where technological tools, regardless of their original intent, cannot substitute for the political reforms needed to address fundamentally political challenges surrounding the socioeconomic exclusion and marginalization of migrants and refugees.

4 **Reinforced divides**

The digital wallet model often represents a progressive approach to user control, effectiveness, and security. Yet, like any identification technology, digital wallets risk deepening and engendering two-tier systems if implemented without socially inclusive principles. EUDI threatens to reinforce the divide between EU nationals and third-country nationals through technical design choices that privilege existing citizenship status. As the wallet integrates across EU services, excluded migrants will face compounding barriers to employment, housing, healthcare, and education.[10] The BritCard explicitly weaponizes digital identity for hostile environment policy enforcement. Universal mandatory participation means migrants cannot avoid surveillance systems even for basic transactions. DIGID represents a well-intentioned but bounded approach, where refugees remain blocked from accessing mainstream employment, banking, or education systems essential for integration.

10 Weitzberg et al., under review.

CASE STUDY 3

Dignified Identity in Cash Assistance

The IFRC (International Federation of Red Cross and Red Crescent) and fintech firm Gravity launched Dignified Identity in Cash Assistance (DIGID) in 2019 as a blockchain-based digital wallet that stores user credentials, providing QR codes for those without smartphones as a way to increase inclusion for those without device access. Kenya Red Cross initially piloted the system in Nairobi and Dadaab to enable people lacking official IDs to access humanitarian cash assistance through Kenya's mobile money infrastructure.

The program later expanded into a medical wallet piloted in Turkana County and the Kalobeyei refugee camp, enabling mobile populations to securely store and access their health data across different medical facilities for better diagnoses and treatment. However, DIGID remained confined to the humanitarian ecosystem and never scaled beyond its pilots. This was due to insufficient buy-in from major humanitarian organizations, lack of government regulatory frameworks, unsustainable donor funding cycles, Safaricom's market dominance, limited smartphone access, and siloed data infrastructures between competing humanitarian organizations.[11]

These case studies reveal how the wallet model in fact represents diverse approaches to digital identity management, encompassing fundamentally different philosophies about how the power to manage personal information should be distributed among institutions and individuals. The proliferation of digital wallet projects requires careful evaluation to understand how advancements in user empowerment, control, and privacy play out and intermingle with long-term challenges around socioeconomic inclusion, integration, and rights protection—which migrants and other marginalized groups disproportionately face. These wallet projects each enact exclusions, risks, and inequities differently, reflecting specific power dynamics in how they are funded, governed, and implemented.

Ultimately, all digital identity systems inherently straddle the boundaries between inclusion and exclusion, and between surveillance and recognition.[12] Understanding these limitations leads us to examine the institutional forces that drive such exclusionary choices—forces that operate not only in state systems but also in the humanitarian sector where digital identity innovations are frequently tested and refined.

11 Weitzberg et al., *Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya*.

12 Weitzberg et al., "Between Surveillance and Recognition: Rethinking Digital Identity in Aid."

Power dynamics shaping the outcomes of digital identity systems

The case of humanitarian aid

The promises and pitfalls of state digital identity systems are often reproduced or amplified within humanitarian contexts, where digital identity technologies are frequently piloted before broader adoption. This section zooms in on our stakeholder workshops and interviews with humanitarian practitioners, which will culminate in an anthology title *A History of the Future: Digital Identity and Aid* (forthcoming in 2026).

Our analysis focuses on this rapidly shifting sector where funding structures, institutional hierarchies, and political constraints create conditions where organizations struggle to balance organizational and donor interests over beneficiary needs. These dynamics have become particularly pronounced amid the severe and widespread funding cuts fundamentally reshaping the humanitarian landscape since Donald Trump's reelection to the US presidency in 2025. While reduced traditional funding streams create potential openings for more beneficiary-centered and localized approaches to identity management and aid delivery more broadly, the same financial pressures are simultaneously driving increased privatization of core humanitarian functions, threatening organizational independence and humanitarian integrity.

Fragmented, unsustainable digital systems

In the 2016 Grand Bargain agreement, the humanitarian sector committed to strengthen the humanitarian-development nexus, transitioning from short-term aid to longer-term, locally led responses that give host states, organizations, and communities a greater role in managing relief and services. Despite growing emphasis on this transition, the critical role of digital technologies, systems, and data in this process has been largely overlooked.[13] Siloed humanitarian information systems currently create duplication, inefficiencies, and inconsistent service delivery.[14] Rather than continuing to build one-off digital systems, there is growing recognition among some humanitarian organizations that robust digital public infrastructure would help bridge humanitarian and development responses and national identity systems, even as there are significant concerns about the risks of data sharing across systems, institutions, and legal contexts.[15] A concerted approach will require humanitarian organizations to reach consensus on data sharing standards and align around verification requirements.[16]

The potential of this longer-term approach is evident in Kenya, where refugee-led organizations are pushing for communication between refugee data and national identity systems, thereby pursuing digital inclusion (and socioeconomic inclusion) in ways that sidestep the politically fraught questions of legal recognition and naturalization. This raises important questions about whether digital access might offer a new route for claims-making—one that becomes particularly significant in an era of humanitarian aid cuts, when increasing numbers of refugees are forced to live outside under-serviced camps.

Government control and political constraints

Political constraints significantly impact data management practices in humanitarian aid, particularly regarding beneficiary identification and assistance coordination. These constraints are particularly evident in contexts where refugee governance efforts initiated by international donors rather than host governments become, as researcher Maissaa Almustafa argues,

13 Schoemaker and Martin, "Digital Transformation and the Humanitarian-Development Transition."
14 Cheesman and Schoemaker, "The Reset Imperative: Digital Identity in Humanitarian Response.'"
15 Schoemaker and Martin, "Digital Transformation and the Humanitarian-Development Transition."
16 Cheesman and Schoemaker, "The Reset Imperative: Digital Identity in Humanitarian Response.'"

"connected to frameworks of governance that mainly aim to contain refugees in their own regions and to deter them from accessing the territories of the Global North."[17] Kenya's case shows how states can use digital identity systems strategically, with biometric identification enabling systematic surveillance of Somalis and obstructing their recognition as Kenyan citizens. As Keren Weitzberg, Saada Loo, and Asha Jaffar note, "a decade ago, amid heightened securitization following a string of al-Shabaab attacks, the Kenyan government weaponized identification systems against the refugee population by suspending refugee registration and enforcing SIM-card registration policies."[18]

Donor influence and technological solutionism

Donor funding sources strongly shape humanitarian organizations' decision-making, responsibilities, and data-sharing practices around identity management. As one humanitarian practitioner told us during interviews, "*funding shapes the logic of projects,*" with donor interests often directly influencing the adoption of specific data systems and technologies. This dynamic is illustrated by a European government donor's approach to funding early biometric systems, where "*the government funded a biometric system on two conditions: a local company would get the contract, and it would be compatible with the European Dublin Convention system.*" The adoption of biometric refugee registration, and "function creep" of biometric checks into broader humanitarian services, are driven by institutional priorities, including but not limited to securitization and efficiency. Donor-driven structures contribute to "pilotitis" in the humanitarian sector—a focus on funding time-limited tests that leads to fragmented and unsustainable solutions with insufficient collective learning from pilot programs. The challenge is compounded by technological solutionism, where faith in technology as a silver bullet to governance challenges trumps evidence suggesting more nuanced approaches are needed. The tension between organizational survival and mission integrity is captured in one practitioner's reflection on the incentive for humanitarian organizations to "conjure" innovative pilots: "*We organisations don't control the rules of the game regarding resources and funding. If we didn't do some 'conjuring' for leadership to talk about, we wouldn't be able to do other good stuff that's less flashy, like our refugee-led work. We are not only our conjured projects, but senior leadership wants them.*"[19]

17 Weitzberg et al., *Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya.*

18 Weitzberg et al., *Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya.*

19 Cheesman, "Conjuring Innovation: Tech Pilots as Products."

Centralization vs. decentralization

Digital identity systems face inherent tensions between moves towards decentralization against established norms of centralized authority in aid. Decentralization is often promoted as offering greater user control, enhanced privacy protection, and reduced single points of failure; advocates argue it can empower individuals by giving them direct ownership of their digital credentials while reducing dependency on large institutions and systems that may be inaccessible, untrustworthy, or potential single-points-of-failure. The EUDI promises European citizens (and legal residents) control over personal data across borders. Similarly, "self-sovereign identity" (SSI) initiatives aim to enable refugees to maintain their digital identities even when displaced across multiple jurisdictions. However, systems promoted as decentralized sometimes maintain centralized authority structures.[20] Pilot projects involving the decentralized database technology blockchain serve as indicative examples here. For one interviewee in our humanitarian practitioner research, "*even if blockchain is used, it can still be governed as a highly centralized system with one organization as the centre of gravity.*" The practical implications of centralization become evident in cross-border coordination challenges. UN beneficiary database systems exemplify this tension: "*Our biometric database is nationally siloed by design: field offices see only their country's data, while headquarters can view everything.*" While often the result of commitments to protection and legal compliance, these structures create information asymmetries that can undermine coordinated aid delivery whilst concentrating decision-making power at organizational headquarters.

Privatization and organizational independence

Aid funding cuts are driving increased privatization of humanitarian services, with significant implications for organizational integrity and independence. The complexity of managing multiple partnership arrangements is captured in one organization's experience: "*We operate with four partnership templates that sometimes run simultaneously: procurement of goods or services, receiving donor funds, informal arrangements without agreements, and agreements where no money exchanges hands. The problem is these areas don't talk to each other.*" The value of maintaining independence through diversified funding sources was emphasized by interviewees:

20 Cheesman, "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity."

"*No-strings-attached resources from private donations are incredibly valuable because we maintain our decision-making power. We can choose to say no. But that will become harder as we're scraping for resources, especially in the current political context where private sector power is growing.*" The trend towards privatization of core humanitarian functions presents new challenges, including in norms around aid delivery.[21] In our humanitarian sector research, one observer noted, "*the most significant trend I foresee is the privatization of refugee registration.*" This shift, visible during crises such as the Rohingya situation in Bangladesh, raises fundamental questions about data protection and privacy, security, and adherence to humanitarian principles when core functions are outsourced to private entities.

Beneficiary and local actor marginalization

The localization agenda, emerging from the 2016 Grand Bargain commitments to channel more funding directly to local and national actors, aimed to fundamentally redistribute power within the humanitarian system. Motivations to localize digital identity systems include data sovereignty (communities controlling their own information), capacity building (developing local technical expertise), and sustainability (ensuring systems persist beyond international presence). However, the concentration of power within established humanitarian institutions continues to create barriers for beneficiaries and smaller local organizations to meaningfully participate in the design and governance of identity systems. This dynamic is exemplified by issues around data centralization, where one practitioner we interviewed noted that "local NGOs are concerned about losing control and access to their data when it is centralised in a UN-run database, as the UN has diplomatic immunities and privileges, making them unaccountable."

Some organizations have been attempting to shift these power dynamics. Projects like DIGID in Kenya are motivated by the goal of "self sovereignty" for refugees and local actors, providing workarounds to exclusion, and allowing people to manage attestations and deletions of identity information themselves—even if this approach is difficult to realize given uneven access to smartphones, connectivity, and digital literacy. Localization efforts increasingly face existential threats as the current humanitarian funding crisis may force donors to prioritize familiar, centralized channels that promise efficiency and accountability over the longer-term investments required for genuine localization, potentially undermining nearly a decade of progress towards more equitable humanitarian governance.

21 Madon and Schoemaker, "Digital Identity as a Platform for Improving Refugee Management."

Implications

The power dynamics shaping digital identity systems in humanitarian contexts reveal a web of competing interests that often subvert the stated objectives of humanitarian aid. From donor-driven technological choices to the weaponization of identification systems by states, these dynamics demonstrate that technical solutions cannot be divorced from their political and economic contexts. Addressing these challenges requires systemic changes including:

1. Establishing clear guidelines for funding agreements that align donor interests with humanitarian principles, agnostic to technological solutions
2. Implementing protection-first approaches to digital identification, applying standards and policies that prioritize data protection, minimization, encryption, and user control
3. Improving coordination by aligning around levels of assurance for identity verification
4. Developing participatory approaches to technology adoption that meaningfully involve beneficiaries and local actors, including development and social protection agencies
5. Creating robust regulatory frameworks and accountable data sharing monitors for private sector partnerships

Rather than perpetuating fragmented, short-term solutions—as seen in digital identity pilots—humanitarian organizations need to move towards an infrastructure-led approach: "*optimising the railway network, rather than buying expensive trains.*"[22] This work would create sustainable foundations for the humanitarian-development transition, centering community ownership and leadership.

Institutional and political interests currently dominate the design and implementation of digital identity systems. Without adequate consideration of the priorities and needs of migrants and refugees, these institutional dynamics—from humanitarian pilot projects to state policy implementation—too often manifest in inequitable lived experiences for marginalized groups navigating digital identity systems across different contexts. The power structures identified in humanitarian settings directly shape the systems that migrants encounter in host countries, while state digital identity policies influence how humanitarian actors can support displaced populations. This interconnection becomes visible when we examine how migrants experience these systems in practice.

22 Schoemaker and Martin, "Digital Transformation and the Humanitarian-Development Transition."

How migrant experiences can inform more inclusive and equitable identification systems

Insights from Kenya and Germany

The fault lines revealed through migrants', refugees', and asylum seekers' experiences with digital identity systems expose vulnerabilities that extend far beyond migration contexts. While these groups face heightened exclusion due to their differential legal status and mobility rights, many of the barriers they encounter—such as inflexible documentation requirements, system complexity, inadequate privacy protections, and exclusionary governance structures—reflect broader patterns of digital exclusion that affect elderly populations, disabled persons, ethnic minorities, and economically disadvantaged groups.

Centering migrants' experiences reveals principles for more just and inclusive digital identity systems that benefit all vulnerable populations. Our research compared the experiences of migrants in Global North and Global South contexts—Germany and Kenya—to understand how different technological infrastructures, regulatory frameworks, and implementation approaches shape identification practices across diverse socioeconomic and institutional environments.

Systemic exclusion and policy implementation gaps

Digital identity systems worldwide demonstrate the tensions between security, efficiency, and inclusion. The evidence we gathered from Germany and Kenya reveals that the tangle of analog bureaucratic and digital identification practices supports the recognition of mobile populations but can also exacerbate existing inequalities and even create new forms of exclusion. For example, Kenya's new Social Health Authority requires online registration for health coverage, but refugee IDs are not integrated into the system, causing delays and exclusions.[23] Due to the government decision to enforce SIM card registration laws, many refugees in Kenya have lost access to phone services and M-PESA (mobile money) accounts. Both refugees and asylum seekers in Kenya struggle to obtain government-issued identification, further blocking their access to essential services. Refugees are mostly shut out of Kenya's digital public infrastructure. This systematic exclusion transcends national boundaries, affecting how migrants, refugees, displaced persons, and other mobile populations access services, exercise rights, and participate in economic and social life.

There is a persistent gap between legislative intentions, many of which are promising, and their concrete implementation. Well-intentioned policies—such as moves towards greater socioeconomic inclusion for refugees within Kenya's 2021 Refugees Act—can fail when administrative systems lack the flexibility or political will to accommodate diverse documentation histories, complex legal statuses, and varied cultural backgrounds. In Germany, our research shows that legal reforms to facilitate skilled migration successfully aimed to decrease the workload of public authorities by extending visa validity periods. However, this decision effectively excludes migrants from accessing e-government and other digital services during that period.[24] This aligns with broader patterns across German municipalities and federal states, where immigration authorities consistently report excessive workloads and delays, with federal regulations and reforms often perceived as adding to rather than reducing administrative burden for processing permits and other key tasks. Identity systems are not merely technical solutions but social and political infrastructures that can both enable and block participation in society. Legal, administrative, and bureaucratic inequities create systemic barriers that affect people's ability to navigate systems and access essential services.

These challenges manifest differently across contexts but share common patterns. In both Germany and Kenya, migrants encounter arbitrary decision-making, inconsistent application of rules, and complex procedural

23 Weitzberg et al., *Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya*.

24 Kirsch et al., *"It's Not For People Like Me": Centering Migrants' Perspectives in the EUDI Wallet Debate in Germany*.

requirements that assume stable residency and standard documentation pathways. ID requirements differ between sectors and agencies, creating unpredictable and uneven experiences for users. The digitalization of identification systems sometimes reduces bureaucratic challenges associated with human intermediaries; some migrants suggested this reduced the risk of in-person bias or discrimination. At the same time, many research participants also noted increased arbitrariness and reduced support—challenges that significantly impact migrants' well-being, erode their time and energy, and hamper their ability to access basic rights.

While we conducted fieldwork in radically different national contexts, both reveal a pressing need for systemic reforms to eliminate inconsistencies in identity management and reduce the bureaucratic burden on migrants, asylum seekers, and refugees. Digitalization holds potential to address inequities and exclusions faced by vulnerable groups by, for example, reducing in-person discrimination and improving information transparency. Fulfilling this potential should be a primary objective rather than a positive side effect of identification policy.

Documentation and access barriers

Migrants globally face similar documentation challenges that cascade into broader exclusion from services, rights, and opportunities in host countries. German authorities' document verification process for asylum seekers, particularly for passports to confirm identity and origin, can be time-consuming and error prone. As one respondent explained, "*I provided everything which could prove that I am from Syria, and yet, the first ID document I received when I filed my application for asylum stated that my nationality was 'unclear.'*" Overcoming errors and gaps with foundational documentation can become an insurmountable cycle of exclusion. For some refugees in Germany, their passports were retained by other EU countries that ordered their deportation, leading to spiraling consequences.

In Kenya, even citizens can face discriminatory procedures to prove their "Kenyanness" for ID cards, an experience that deeply impacts Kenya-Somali nationals.[25] Verification processes often assume linear migration pathways and intact, accessible document chains that may not reflect the realities of displacement, persecution, or migration. When initial identity documents are incomplete, damaged, lost, or issued by unrecognized authorities, individuals can become trapped in bureaucratic limbo.

25 Weitzberg, "Keeping People out of Camps: Biometric Technologies, Contested Sovereignty, and Border Practices within Humanitarian Spaces."

The connection between identity documentation and financial inclusion represents a significant challenge across contexts. One respondent in Germany explained their experience: "*My problem was that I couldn't apply for my residence permit without having insurance. And I couldn't have insurance without a bank account*." In Kenya, the requirement for a KRA (tax) PIN for various services underscored the barriers in accessing financial and official identity-related services due to the lack of necessary documents. Financial exclusion is a common struggle among migrants, asylum seekers and refugees in different regions. Banking systems, credit services, insurance providers, and digital payment platforms typically require forms of identity verification that mobile populations may struggle to meet. This creates cycles of exclusion where lack of documentation prevents access to services, which in turn makes it harder to establish the identity credentials needed for broader integration. These barriers are not merely administrative inconveniences but fundamental obstacles to economic participation and social inclusion. Rigid documentation requirements can inadvertently create parallel systems—including risky fake ID markets which expose people to exploitation and extortion—as marginalized populations are blocked from mainstream services and basic opportunities.[26]

Accessibility and privacy challenges

Digital identity systems are often designed with mobility and diversity as afterthoughts rather than core considerations, yet mobility and diversity are relevant for everyone. Accessibility challenges significantly impact migrants. In our research, user experience issues are remarkably consistent across different national contexts: complex and siloed bureaucratic systems, interfaces that assume high digital literacy, language barriers that prevent meaningful access, and requirements that reflect the needs of settled populations rather than mobile ones.

When migrants *can* access identity verification, document renewal, or status updates remotely, this eliminates significant practical barriers: the cost and time of traveling to administrative centers, the challenge of navigating unfamiliar locations, and the difficulty of taking time off or arranging childcare for in-person appointments. For populations who may be geographically dispersed, lack reliable transportation, or face mobility restrictions, virtual access can be transformative. However, the benefits of digitalization are currently captured primarily by those who already have advantages: stable housing, income and employment,

26 Cheesman and Hackl, "The Identity Issue: Digital Risks of Proxy IDs in Kenya's Online Economy."

reliable internet access, established digital literacy, and familiarity with the dominant language and cultural norms. Digital ID schemes often have poor accessibility features, with cultural and linguistic diversity rarely embedded in system design from the outset—failing to accommodate multiple languages and ethnic naming conventions, for example. Addressing such problems is not merely about translation but about creating systems that recognize and respect diverse, culturally relevant approaches to identity recognition and documentation.

Privacy and data protection concerns take on heightened importance for mobile populations who may have fled surveillance or persecution. Many digital identity systems fail to balance legitimate security needs with fundamental rights to privacy and data protection. Risks are particularly acute for vulnerable populations such as migrants, asylum seekers, refugees, undocumented individuals, victims of domestic violence, LGBTQ+ persons escaping hostile jurisdictions, political dissidents, and Indigenous communities. These groups may face persecution, involuntary repatriation, arbitrary detention, family separation, denial of citizenship, or violence if their personal data is compromised or misused. Digital identity systems often employ invasive biometric collection without consent, enable location tracking and cross-border data sharing, and suffer from inadequate retention policies and vulnerability to breaches. Beyond physical threats, they may facilitate surveillance overreach, algorithmic discrimination in service provision, denial of due process, restriction of movement, and violations of non-refoulement principles.

Many of these concerns surfaced in our research. Despite legal privacy frameworks, migrants face disproportionate surveillance and data collection by authorities. For example, German jurisprudence has evolved to introduce the concept of "informational self-determination"; nevertheless, the German Federal Office for Migration and Refugees has used automated "phone scraping" to extract data from asylum seekers' mobile phones—including location metadata, contact information, and text messages—to verify their identity and country of origin when they could not provide valid documentation. In Kenya, biometric data collection has been used to systematically monitor refugees, raising issues of exclusion from national ID systems.

Historical contexts vary, but the principle remains universal: migrants very often have heightened vulnerability to data misuse and require stronger protections. To guard against mass privacy invasions and function creep, strong technical standards are paramount. Policy alone cannot protect against certain risks once they are an inbuilt technical feature, as argued by the No Phone Home campaign.

Participatory design?

Due to poor system design and ingrained discrimination, tens of thousands of Kenyan citizens were denied national identity cards because they were biometrically registered in refugee databases, leading to long-standing mass exclusion from rights and services, and years of civil society campaigning.[27] Clearly, those who will be most affected by identity systems should have genuine input into their design and operation. Migrants, refugees, and asylum seekers were—unsurprisingly—seldom engaged in system design, which is vital for identity management processes that accurately reflect their specific barriers, needs, and circumstances.

The need to include migrants in the design and development of digital identity systems emerged as priority in our fieldwork and among policy advocates. For example, when registering refugees for the Fayda digital identity scheme in Ethiopia, UNHCR and Ethiopia's Refugees and Returnees Service took steps to decriminalize the issue of double registration by establishing a joint committee to resolve people's legal status, thus preempting the problems that had plagued Kenya. This is a rare example of a more participatory and inclusive approach, which learned from the challenges of a neighboring country.

Despite these rare examples of participatory design, user experience and perception data consistently reveal disconnects between system capabilities and actual needs. Policymakers should prioritize understanding the lived experiences of mobile populations and create mechanisms for ongoing feedback and system adaptation. This requires aligning technical standards and policies with due consideration of how systems function in practice for diverse users. Transparency about system requirements, benefits, and limitations is crucial for building trust and ensuring informed participation. Marginalized user groups need clear information about how digital identity systems work, what data is collected, how it is used, and what rights they have regarding their personal information.

27 Weitzberg, "Keeping People out of Camps: Biometric Technologies, Contested Sovereignty, and Border Practices within Humanitarian Spaces."

Recommendations

Equitable design means understanding how identity systems can work for the most marginalized users first, ensuring that the benefits of digitalization extend to those who need them most rather than primarily serving those who already have the most privileges and entitlements. Grounded in migrants' everyday experiences, our research produced insights that are broadly applicable to policymakers designing and maintaining digital identity systems.

1 **Service integration and inclusion**
Digital identity systems are tools that realize higher-level policy goals. Migrants' needs can be supported through wider policies that enable marginalized groups to access essential services including banking, healthcare, education, and employment. Alongside this, create sustainable pathways for socioeconomic integration that allow individuals to progressively build identity credentials over the long term. Prevent exclusion from digital public infrastructure based on immigration status or documentation gaps.

2 **Risk-proportionate standards**
Implement tiered levels of assurance that align identity verification requirements with the actual risk and sensitivity of the service the person is accessing. Ensure that maximum security standards are not unnecessarily applied to all situations where they would exclude vulnerable populations without commensurate benefit. For example, biometric checks are unwarranted for low-risk contexts and services.

3 **Privacy by design**
Implement robust No Phone Home standards and data protection policies that recognize how marginalized groups face heightened vulnerability to tracking, privacy invasions, and other abuses. Design systems that collect only necessary information and provide transparent governance of data use. Ensure individuals have meaningful control over their personal data and provide clear redress mechanisms.

4 **Basic digital access**
Improving marginalized populations' access to digital connectivity (Wi-Fi hubs, low-cost devices, charging stations) can offer a pragmatic mechanism for extending basic services and economic opportunities without requiring contentious political decisions on legal recognition or naturalization for migrants. Meanwhile, retain analogue mechanisms for key processes: socioeconomic inclusion should not be premised on access to digital technology, which is not universal.

5 **Inclusive access methods**
Design verification processes that accommodate diverse documentation histories and non-linear migration pathways. Create alternative pathways for identity verification that do not rely solely on traditional documents, such as trusted community members vouching for low-risk services. Establish clear, consistent criteria that prevent arbitrary decision-making whilst sensitive to diverse individual circumstances.

6 **Accessible design principles**
Create user interfaces that are accessible across different levels of digital literacy, language proficiency, and cultural backgrounds. Ensure systems work effectively in low-resource environments and for users with intermittent connectivity. Design for interoperability to prevent system fragmentation that can exclude mobile users. Users should be able to track their account, status, and appointments rather than through arranging in-person queuing slots, visiting multiple online platforms, and repeatedly submitting documents.

7 **Participatory governance mechanisms**
Establish formal channels for diverse users' input into system design and operation. Create feedback mechanisms that allow for ongoing system improvement based on user experience. Ensure marginalized groups, including non-citizens, are represented in governance structures and decision-making processes.

8 **Capacity building and support**
Provide digital literacy support and system navigation assistance. Train staff to work effectively with diverse populations and prevent discriminatory treatment. Create community-based support networks that can assist with system access and technical help.

9 **Accountability and oversight**
Implement monitoring systems to identify and address function creep and discriminatory practices in system operation, making them available to civil society. Establish clear complaint mechanisms and ensure effective remedies for system failures. Regular audit processes should assess whether systems are achieving inclusion goals and policies in practice.

Conclusion

This report examined the implications of digital identity systems for migrants and vulnerable communities through three interconnected lenses: emerging digital wallet technologies, power dynamics in humanitarian contexts, and migrant experiences in Kenya and Germany. Our findings reveal that, while digital identity innovations promise greater inclusion and user control, without addressing the needs of the most marginalized and under-resourced communities, their technical design, governance, and implementation often reproduce or augment existing exclusions.

Existing and proposed digital identity wallets—from EUDI, BritCard, and DIGID—demonstrate how the same technological paradigm can serve fundamentally different political projects, from international citizenship empowerment to national migration control to closed-loop humanitarian assistance. Viewed as sociotechnical systems rather than neutral solutions, digital identity systems can replicate existing blockages for some, even while they enable efficiency, empowerment, and improvement for others.

Similarly, our analysis of humanitarian contexts shows how funding structures, institutional hierarchies, and political constraints mean donor and organizational interests are often prioritized over beneficiary needs, mitigating the benefits of humanitarian digital identification and data systems. Even where digital identification systems help migrants in Kenya and Germany access recognition and services, their implementation also illuminates broader patterns of digital exclusion that extend beyond migration contexts. The barriers migrants encounter—complex interfaces, inflexible documentation requirements, inadequate privacy protections—affect everyone. Their experiences provide essential insights for creating more inclusive approaches to digital identity, and digitalization in general.

The path forward requires moving beyond technological solutionism and towards systemic reforms that address the political causes of exclusion. This is a call for humanistic political reform both within and beyond digital identity systems themselves, encouraging alternative approaches to the unjust assumptions and practices of hostile environment policies.

Digital identity management will always straddle surveillance and recognition. If the harms of identity-based exclusion are to be reduced in the digital age, ID systems must, at a minimum, adopt privacy-by-design frameworks for all data subjects including non-citizens, flexible documentation standards to expand identity recognition, accessible interfaces, service integration pathways, audit and participatory governance mechanisms.

Further research on digital sovereignty is needed across individual, organizational, state, and international levels—examining how personal data rights and autonomy intersect with corporate accountability, regulatory frameworks, and cross-border cooperation to address questions of agency and control in digital identity systems. These systems are not neutral technologies but political tools that can either enable or prevent full participation in society. The design choices made today will determine whether identification bridges or deepens inequalities.

References

Cheesman, Margie. "Conjuring Innovation: Tech Pilots as Products." *Caribou* (blog), August 28, 2024. https://caribou.global/publications/conjuring-innovation-tech-pilots-as-products/.

Cheesman, Margie. *Digital Wallets and Migration Policy: A Critical Intersection*. Migration Strategy Group on International Cooperation and Development, 2022. https://www.bosch-stiftung.de/en/publication/digital-wallets-and-migration-policy-critical-intersection.

Cheesman, Margie. "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity." *Geopolitics* 27, no. 1 (2020): 134–59. https://doi.org/10.1080/14650045.2020.1823836.

Cheesman, Margie, and Andreas Hackl. "The Identity Issue: Digital Risks of Proxy IDs in Kenya's Online Economy." *UNHCR Innovation* (blog), April 13, 2023. https://medium.com/unhcr-innovation-service/the-identity-issue-digital-risks-of-proxy-ids-in-kenyas-digital-economy-52eec129ebea.

Cheesman, Margie, Aaron Martin, and Keren Weitzberg. "The Britcard: Progressive or Concerning?" *LSE British Politics* (blog), July 16, 2025. https://blogs.lse.ac.uk/politicsandpolicy/the-britcard-progressive-or-concerning/.

Cheesman, Margie, and Emrys Schoemaker. "The Reset Imperative: Digital Identity in Humanitarian Response.'" *Caribou* (blog), July 11, 2025. https://caribou.global/publications/the-reset-imperative-digital-identity-in-humanitarian-response/.

Dullaert, Isadora. *The European Digital Identity Wallet: Why It Matters and to Whom*. Caribou Publishing, 2024. https://doi.org/https://doi.org/10.64329/WLMZ7879.

Kirsch, Thea, Marianne Samaha, and Ana Werkstetter Caravaca. *"It's Not for People Like Me": Centering Migrants' Perspectives int eh EUDI Wallet Debate in Germany*. Caribou Publishing, 2026. https://doi.org/10.64329/CXBS6022-1.

Labour Together. *BritCard: A Progressive Digital Identity for Britain*. 2025. https://www.labourtogether.uk/all-reports/britcard.

Madon, Shirin, and Emrys Schoemaker. "Digital Identity as a Platform for Improving Refugee Management." *Information Systems Journal* 31, no. 6 (2021): 929–53. https://doi.org/10.1111/isj.12353.

Schoemaker, Emrys, and Aaron Martin. "Digital Transformation and the Humanitarian-Development Transition: The Role of Digital Public Infrastructure and Data Protection." In *Data Protection in Humanitarian Action: Responding to Crises in a Data-Driven World*, edited by Ana Beduschi, Massimo Marelli, and Aaron Martin, 110–28. Routledge, 2025. http://doi.org/10.4324/9781003650164-9.

Weitzberg, Keren. "Keeping People out of Camps: Biometric Technologies, Contested Sovereignty, and Border Practices within Humanitarian Spaces." *Journal of Ethnic and Migration Studies* 51, no. 14 (2025): 3590–609. https://doi.org/10.1080/1369183X.2025.2513155.

Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. "Between Surveillance and Recognition: Rethinking Digital Identity in Aid." *Big Data & Society* 8, no. 1 (2021). https://doi.org/10.1177/20539517211006744.

Weitzberg, Keren, Margie Cheesman, H. Stoll, Aaron Martin, and Isadora Dullaert. "Digital Identity Infrastructure as Civil Stratification: A Comparative Analysis of the European Digital Identity Wallet and the European Asylum Dactyloscopy Database." Manuscript under review.

Weitzberg, Keren, Saada Loo, and Asha Jaffar. *Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya*. Caribou Publishing, 2025. https://doi.org/10.64329/LVBI5031.

Caribou

Robert Bosch Stiftung

February 2026