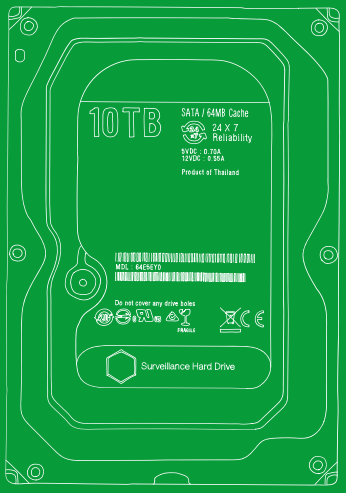
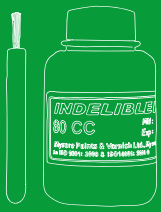
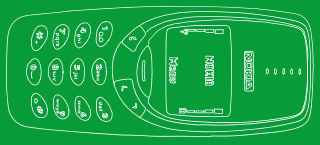
# Aid and ID:

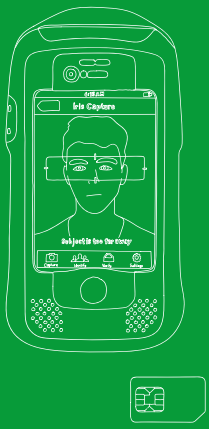



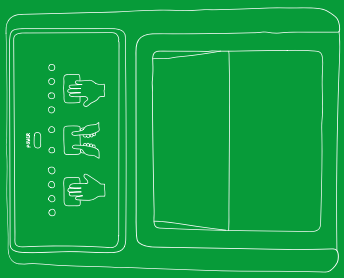



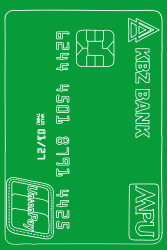


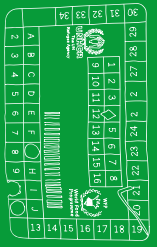


# Making People Matter



Edited by
Margie
Cheesman

# Aid and ID: Making People Matter

Edited by Margie Cheesman


Published by Hafan Books, Swansea, 2026

www.hafanbooks.org

Hafan Books is a solidarity project of the registered charity Swansea Asylum Seekers Support

www.sass.wales

All proceeds go to the charity



This work was developed by the Digital Sovereignty Observatory, a project supported by the Robert Bosch Foundation

ISBN: 9781738404995


Robert Bosch
Stiftung

# Contents

# Acknowledgments

Special thanks to all our humanitarian contributors, the Robert Bosch Foundation team, Tom Cheesman, Edwin Mingard, and my long-standing collaborators Aaron Martin, Keren Weitzberg, and Emrys Schoemaker, whose insight and support have been invaluable to this work in countless ways.



# Index of illustrations

# Glossary

## AML

AML (Anti–Money Laundering) is the framework of laws and controls that use identity verification, transaction monitoring, sanctions screening and reporting duties to detect and prevent money laundering, terrorism financing and other financial crimes.

## Biometrics

Biometric identification systems use unique physical characteristics (fingerprints, iris patterns, voice or facial recognition) to verify identity. These systems collect and store biological data that cannot be changed if compromised.

## Blockchain

A distributed database shared among computer network nodes, best known as the technology behind cryptocurrencies. Blockchains store data in blocks linked together, creating a chain that is secure, transparent, and difficult to modify.

## Data canisters

Secure digital 'containers' that store personal data and let individuals or organisations control who can see or use it.

## Digital identity

A digital representation of a person, made up of data and attributes that allow them to be recognised and interact within digital systems.

## Federated data management

A data governance and integration approach in which multiple independent organisations maintain control over their own data systems while enabling secure, standardised sharing and interoperability across a network.



## Functional identity

A temporary or purpose-specific form of identification created to enable access to services.

## Foundational identity

An official, government-recognised form of identification that establishes a person's legal identity.

## Interoperability

The ability of different systems and organisations to exchange and use information consistently and securely.

## KYC

KYC (Know Your Customer) is the process of verifying the identity of both individuals and organisations before authorising access to services. For individuals, this involves confirming personal details and identity documents, while for organisations it includes verifying legal registration, for example.

## Levels of assurance

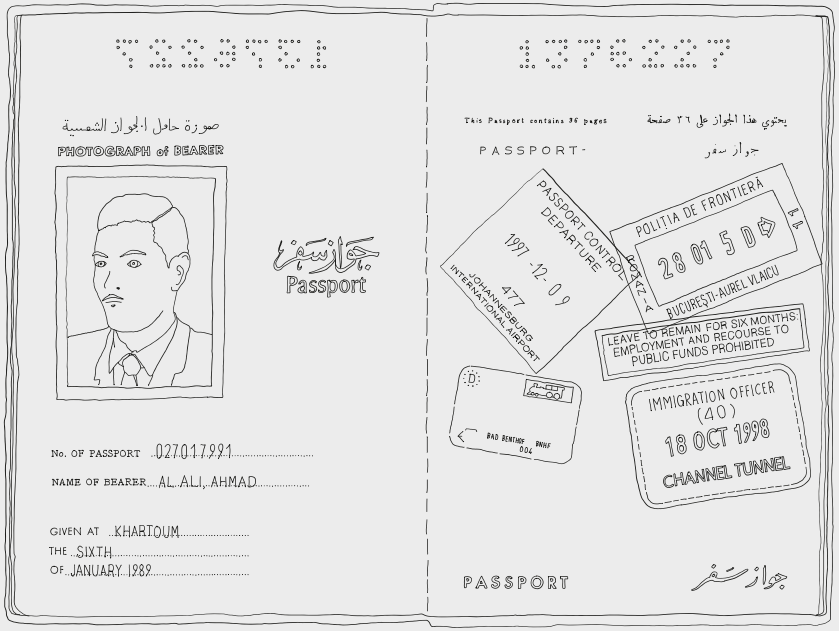
Measures of how trustworthy an identity verification or authentication process is. Low assurance may be sufficient for emergency relief, whereas higher assurance may be required for activities such as border management or sensitive protection services.

## Self-sovereign identity

Identity management solutions prioritising users' ownership and management of personal information over centralised institutions. They tend to incorporate the distributed database technology blockchain.

## Verifiable credentials

Digital identity documents (like diplomas or licenses) that use cryptography to prove they are authentic without the need to contact whoever issued them. They are held and controlled by the individual, who can choose when and what to share.




*Foreword by Margie Cheesman*

# Making People Matter: Identity Management and Humanitarian Governance

*Dr Margie Cheesman is an Assistant Professor in Digital Economy at King's College London and co-lead at the Digital Sovereignty Observatory. She is an anthropologist specialising in the social and political dimensions of technology in humanitarian contexts.*

At the time of writing, international aid is on a 'terminal trajectory'.[1] Severe funding cuts are forcing humanitarian organisations to dramatically scale back programmes, release staff, and make urgent decisions about which forms of assistance will have to disappear. These cuts reflect a broader shift in the political economy of aid: donor retrenchment, geopolitical realignments, rising domestic spending pressures in donor countries, and the redirection of resources toward security and border control agendas. Funding pressures are rightly pushing attention to the more visible elements of crisis response: urgent distributions, cash transfers, shelter provision, health services. Yet beneath all of these activities sits an ecosystem of technologies that are both essential and routinely overlooked: identity management.

Identity management systems underpin everything from who appears on assistance lists to how protection cases are followed, how coordination is achieved across different humanitarian agencies, and how individuals practically access life-saving services. Identity systems are not just another

1 Owen, G. (2025). 'The Managed Decline of the Western Humanitarian Sector'. Journal of Humanitarian Affairs, 6(2), page 67.

logistical tool: they fundamentally organise relationships between crisis-affected communities and aid providers and are thereby the linchpin of humanitarian action.

This anthology asks: what futures of humanitarian identity management are being imagined, contested, or foreclosed in this turning point for the sector? And what can be learned from the biographies of practitioners who have been building and maintaining these systems over time? We invited humanitarians to reflect not simply on tools or technologies of identification, but on the fraught conceptual, political, and ethical questions that identity management has raised in their work.[2]

*

The documentation of identity is central to how states and institutions govern populations. Identification systems have long been used as instruments of classification, bordering, and population management: from the League of Nations' Nansen passport, which provided displaced and stateless people with legal recognition and mobility, to revolutionary France's efforts to issue papers enabling controlled mobility, taxation, and conscription, and later the function of identity cards in Nazi Germany and the Rwandan genocide.[3] In humanitarian settings, multiple actors—states, international agencies, and private firms—co-produce identity management systems in conditions of displacement, crisis, and uncertainty. In these contexts, identity systems do not simply record and confirm 'who people are'; they shape how they are recognised, what they are entitled to, and how they can move. Access to identification—whether through passports, national ID cards, or digitally enabled systems—is closely tied to legal recognition, welfare provision, and protection from exploitation, detention, or deportation.[4]

Identity has never been a stable or singular concept. In the digital age, it stretches across legal, institutional, and technological domains and cross-cutting struggles for sovereignty among individuals, organisations, and states. Within humanitarian contexts, identity may refer simultaneously to foundational identification issued by governments, functional identities created by aid agencies or service providers, and the digital traces individuals generate through everyday transactions and communications. These systems now extend beyond basic demographic data to incorporate biometric, credit, and behavioural information.

The accounts of humanitarians collected here confirm that identity systems make people. Rather than simply reflecting pre-existing identities, these systems actively produce them. They render individuals legible to institutions through categories that shape eligibility to services, exposure to risk, and access to support.[5] An identity system may enact a person as a biometric subject anchored to an iris scan, a household eligible for food assistance, a rights-holder with claims over personal data, or a potential duplicate requiring verification. Each configuration carries implicit, value-laden assumptions about human needs, vulnerability, and trust, as well as stakeholder priorities—from institutional efficiency, risk, and compliance to beneficiary dignity and empowerment. Identity systems make people matter. Their dialectical tendencies simultaneously confer political recognition and essential care to groups like refugees while exposing them to forms of surveillance and economic and mobility control.[6] They are usually framed through the language of inclusion, yet

2 Please note all views expressed are those of the individual contributors and should not be taken as representing the official positions of their organisations.

3 Caplan, J., & Torpey, J. (2001). Documenting Individual Identity: The Development of State Practices in the Modern World. Princeton: Princeton University Press.

4 Manby, B. (2021). The Sustainable Development Goals and 'legal identity for all': 'First, do no harm.' World Development, 139. https://doi.org/10.1016/j.worlddev.2020.105343.

5 Cheesman, M. (2020). 'Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity'. Geopolitics, 27(1), page 3.

6 Weitzberg, K., Cheesman, M., Martin, A., & Schoemaker, E. (2021). 'Between surveillance and recognition: Rethinking digital identity in aid'. Big Data and Society, 8(1).

identity systems can also entrench exclusion where people's nationality or legal status remains contested, and broader legal protections and due process safeguards are absent.[7]

Identification cannot be understood in isolation from the broader governance systems within which they operate. Humanitarian aid involves the organised provision of assistance and protection in crisis, but it also functions as a system of governance—shaping how needs are defined, which populations are prioritised, and how support is delivered.[8] In this sense, the aid industry operates simultaneously as a moral project of care and a political practice of ordering and managing populations. Identity systems sit at the centre of this tension as the key infrastructures through which humanitarian governance is enacted in practice.

Identification challenges crystallise in humanitarian contexts, where populations struggle to 'prove who they are' when personal documents are missing, lost or not formally recognised. Meanwhile, multiple actors—state, humanitarian, private-sector—operate simultaneously with different mandates, sovereignty imperatives, data protection frameworks, and legal obligations.[9] Under these fraught conditions, the politics of identification becomes visible: what identity data is collected, by whom, for what purposes, and with what consequences for people whose futures remain precarious.

Centring humanitarians' career-long experiences and reflections, this anthology provides an historical lens on these questions. The practitioners interviewed here have worked across decades, regions, and organisational cultures—from international agencies like UNHCR, World Food Programme, and the World Bank, to local organisations and initiatives; from Gaza to Myanmar to Pakistan. Their stories trace the evolution from ink-stamped queues of crisis-affected people resembling 'sheep herding' practices, to the rise of biometric checks, digital registration platforms, large-scale international data systems, cash-based assistance, mobile wallets, and, more recently, initiatives involving privacy-preserving or user-controlled technologies and self-registration pathways. These technological shifts were never purely technical: they followed geopolitical events, donor incentives, internal organisational cultures, post-9/11 securitisation agendas, persecution risks, host-state negotiations over sovereignty and control, and localisation efforts. Each technological development has enacted people in different ways: as bodies to be counted, as data points to be verified, as potential fraudsters to be authenticated, as tech users entitled to control their own digital credentials, as rights holders to be integrated into national systems.

Practitioners in this anthology highlight the structural pressures that continue to shape humanitarian identity systems. Organisations operate in short funding cycles and rapidly shifting emergencies, yet identity infrastructures require long-term investment, maintenance, and ongoing political negotiation. Sweeping aid budget cuts now intensify these challenges. Against a backdrop of institutional delegitimisation, humanitarian organisations are encountering escalating imperatives to reduce siloes, improve operational efficiency, and mitigate fraud.[10] Efforts to streamline identity management will play an essential role in improving inter-agency coordination, reducing duplication, and saving on costs.[11] Yet unresolved questions remain about who will finance 'interoperable' identity infrastructures, how they can be collectively governed, how shared 'levels of assurance' may be agreed, and whether stronger integration with state systems will open pathways to longer-term inclusion in social

7 Manby, B. (2025). 'Statelessness and Digital Identity'. Caribou. DOI: 10.64329/VCFZ8386.

8 Fassin, D. (2007). 'Humanitarianism as a Politics of Life'. Public Culture, 19(3), 499–520.

9 Martin, A. (2025). Why sovereignty matters for humanitarian data. Big Data and Society, 12(3).

10 Loy, I. and W. Worley (2026). 'What's shaping aid policy in 2026?' The New Humanitarian. Accessed at: https://www.thenewhumanitarian.org/analysis/2026/01/07/whats-shaping-aid-policy-2026.

11 Cheesman, M. and E. Schoemaker (2025). 'The Reset Imperative: Digital Identity in Humanitarian Response'. Caribou. Accessed at: https://caribou.global/publications/the-reset-imperative-digital-identity-in-humanitarian-response/.

protection, financial services, legal recognition, and mobility rights—or instead reinforce closed-loop aid architectures characterised by surveillance, dependency, and precarity.

Practitioners warn against optimising identity infrastructures for institutional oversight and efficiency gains more than the dignity and autonomy of their subjects. Faster may not be fairer or safer; it is necessary to anticipate the full range of human, non-financial costs associated with new and automated identity interventions. Digital identity systems can introduce hidden burdens and restrictions on those at the frontline, along with new commercial intermediaries and safeguarding concerns.[12] Unfair and exclusionary outcomes of identity systems are not passively accepted by their subjects, as shown by the Right to Food Campaign countering the Aadhaar system in India and Rohingya protests against biometric refugee cards in Bangladesh.[13] Some see a renewed opportunity to rethink the proportionality of identity checks, reduce data collection, simplify processes, and invest in tools that support collaboration rather than competition for data, resources, and recognition among humanitarian agencies. Choices made now will reverberate long after budgets stabilise.

Alongside debates about technological choices, the political landscape is evolving. States are developing ambitious digital public infrastructures and demanding greater control over refugee and migrant identification.[14] Even where national identification frameworks remain unevenly developed

12 Cheesman, M., and C. Aradau (2025). 'Technosocial Reproduction and Humanitarian Reason'. E-Flux. Accessed at: https://www.e-flux.com/architecture/humanitarianism/6782979/technosocial-reproduction-and-humanitarian-reason.

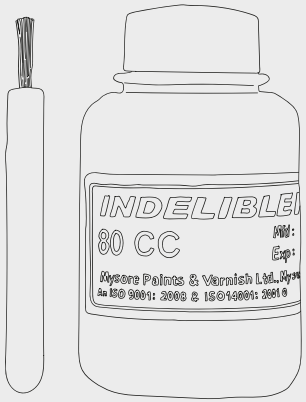
13 Maseiro, S. (2025). Unfair ID. SAGE, p. 118; Madianou, M. (2019). 'Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises'. Social Media and Society, 5(3), p. 9.

14 Schoemaker, E. and A. Martin (2025). 'Digital Transformation and the Humanitarian-Development Transition: The Role of Digital Public Infrastructure and Data Protection' in Data Protection in Humanitarian Action. London: Routledge. pp. 109-128.



or dependent on international support, governments are asserting authority over populations and negotiating access to humanitarian data, producing uneasy alliances between state and humanitarian sovereignty. Private-sector actors now offer verification services that reshape, and sometimes narrow, humanitarian agencies' options, authority, and decision making in operations.[15] Localisation initiatives challenge the dominance of top-down, centralised, international identity infrastructures, raising questions about whether rethinking digital identity systems can help redistribute power to frontline actors rather than consolidate it in the Global North. There are growing demands for systems that protect individuals' rights over their personal data, dignity, and autonomy, including greater control over how identity information is shared and reused ('self-sovereignty'). Decentralised approaches—from 'verifiable credentials' to encrypted 'data canisters'—make beneficiaries and frontline organisations the custodians of sensitive personal information, although they may depend on political and technological conditions that are unevenly distributed. Identity management thus becomes a terrain where the future of humanitarian governance itself is negotiated. Beyond merely technical design choices, these are commitments about whose interests the aid sector's core operational infrastructures ultimately serve. What emerges across the anthology is a shared concern: identity systems will continue to shape the conditions under which people in crisis contexts are seen, heard, and supported, but they must be designed to prioritise care for the lives they affect.

15 Henriksen, S. E. (2023). 'Finding the "Sweet Spot": The Politics of Alignment in Cross-Sector Partnerships for Refugees'. Business and Society 63(1), 145-184; Martin, A. (2023). 'Aidwashing Surveillance: Critiquing the corporate exploitation of humanitarian crises'. Surveillance and Society, 21(1).




*Karl Steinacker*

# From Ink Marks to Iris Scans: 30 Years of Refugee Registration

*Karl worked for several UN agencies between 1988 and 2018. Responsible for refugee registration at the United Nations High Commissioner for Refugees (UNHCR), he oversaw the development of digital identity strategy and the introduction of biometrics. He now works as a freelance expert and teacher in Berlin, Germany.*

I joined the humanitarian world 30 years ago. One of my early assignments was the refugee crisis following the Rwandan genocide.[16] As a programme officer in Tanzania, I was responsible for ensuring the protection of half a million refugees. We had serious problems identifying who was who. We initially outsourced identification to refugee leaders who would provide lists for aid distribution, but these leaders were sometimes the same people who had committed genocide. The conflict of interest made that approach impossible. When we started registering identities with available technology, the process resembled sheep herding: building enclosures, processing people one by one, branding them with ink. That wasn't dignified at all. Manual data processing took months, by which time the information was often irrelevant. The whole system was fundamentally designed to detect fraud, especially 'recyclers'—refugees who would leave the camp,

16 The Rwandan genocide in 1994 was a systematic mass killing that occurred over approximately 100 days, primarily targeting the Tutsi minority population and resulting in approximately 800,000 deaths. The conflict created massive refugee movements as over 2 million people fled to neighbouring countries like Congo, Tanzania, and Burundi.

return to the border, and register again to receive additional benefits. The problem was: mistrust in affected populations was the basis of the operation.

In the 90s, UNHCR began incorporating new technology, but mainly for data entry. By 1998, I was in Geneva working on a new identity registration system. During the Kosovo war,[17] Microsoft came along and offered a portable solution—still not biometric, mind you. Identity registration was originally part of the food section. Until 1992-93, UNHCR handled food sourcing, transportation, and distribution before transferring this role to the World Food Programme (WFP), creating pressure to improve our registration systems as we provided beneficiary lists to WFP. It's important to understand that UNHCR doesn't have a mandate to register people: it's the backup plan when states cannot provide identity documentation. Anyway, a significant shift occurred as registration moved from operations to the protection department. Registration became framed in legal terms by protection lawyers, while the practical implementation remained operational. This created a disconnect between policy and practice because the lawyers would draft policies, but they weren't the ones implementing registration in the field.

In the early 2000s, we developed the registration database PROGRES (Project for Registration and Management of Refugees) and shifted from registering entire families as a unit to registering each person individually. The Dutch government funded a biometric system on two conditions: a Dutch company would get the contract, and it would be compatible with the European Dublin Convention system.[18] So, registration comes with political interests. After the September 11 attacks, refugee registration became increasingly securitised, with greater emphasis on identifying potential security threats among refugee populations. For Afghan repatriation from Pakistan,[19] we implemented an anonymous iris scan system. Biometric data wasn't linked to wider identity information, protecting refugees from potential Taliban retribution. While this system reduced fraud among the 2 million scans registered, it created situations where the machine decides. If someone was flagged as previously registered, there was no override, even with false matches. We saw a tension between privacy protection (not linking biometric data to identities) and our broader protection goals, which involved being able to override automated decisions in exceptional cases. For remaining Afghan refugees in Pakistan, we subcontracted NADRA, Pakistan's National Database and Registration Authority, when our systems couldn't handle the volume. This essentially meant asking the Pakistani police to register refugees, but they did it efficiently. This outsourcing pattern repeated during the Syrian crisis in Jordan with IrisGuard, the biometrics company providing large-scale identity verification of refugees.[20] It is not enough to anonymise biometric data. Inadequate plans have been put in place regarding the long-term security of identity data—when can it be revoked or deleted, for example?[21]

As head of registration from 2004-2008, I oversaw PROGRES development and biometrics piloting. We shifted toward a global biometrics-based system. Then, I left for assignment in the field, and Accenture built for UNHCR

17 The Kosovo War (1998-1999) was an ethnic conflict between Serbian forces and ethnic Albanian civilians in Kosovo, marked by systematic ethnic cleansing policies implemented by Yugoslav/Serbian forces under Slobodan Milošević. Approximately 444,000 refugees escaped to Albania, 245,000 to Macedonia, and tens of thousands more to Montenegro and other nearby nations.

18 The Dublin Convention is EU regulation determining which member state is responsible for examining asylum applications.

19 Following the US invasion of Afghanistan in 2001, there was significant pressure to repatriate Afghan refugees from Pakistan, where many had lived for decades.

20 The Syrian crisis beginning in 2011 forced millions to flee to neighbouring countries, with Jordan hosting hundreds of thousands of refugees requiring registration. IrisGuard is a Jordanian-British company specialising in iris recognition technology. The company is also contracted by the Jordanian government to provide biometric machines used to police the country's national borders.

21 See Karl's article with Katja Lindskov Jacobsen (2021), 'Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered' https://www.prio.org/comments/742.

the Biometric Identity Management System (BIMS)—a platform later inspiring India's Aadhaar identity system.[22] BIMS was then integrated into Microsoft Dynamics, which is a customer relationship management software platform. Returning to UNHCR's global identity management service in Copenhagen in 2016, I saw the limitations of our previous approaches. Microsoft Dynamics proved too heavy for field conditions. We developed an emergency registration system based on logistics technology with QR codes and QR readers, successfully deployed during the Venezuela crisis.[23] Back then, I began questioning what I called 'biometric overkill'—using sophisticated identity checks for everything from delivering soap to resettling refugees in the United States, without due consideration of proportionality.[24] Data protection also emerged as a big concern around that time, with consultants determining whether UNHCR was compliant with GDPR (General Data Protection Regulation) or eIDAS (European electronic Identification Authentication and trust Services).

Post-9/11, governments became less willing to outsource refugee registration. Countries like Kenya and Pakistan wanted greater control over refugee identification. A key challenge emerged: our documents had limited value if not recognised by authorities. UNHCR invested significantly in registration for refugee protection purposes, yet it often primarily served to provide data to the World Food Programme (WFP). This disconnect led me to explore

22 Aadhaar is the world's largest biometric ID system, based on a 12-digit unique identification number issued by the Indian government to residents using their biometric and demographic data.

23 The Venezuela crisis led to one of Latin America's largest displacement situations, with millions fleeing economic collapse and political instability since 2014.

24 This concern echoes what Forte terms "biopolitical creep"—the gradual normalisation and expansion of surveillance technologies in humanitarian settings, despite concerns around the proportionality and necessity of biometric systems in aid delivery. See: Forte, M. (2025). 'Bodies, Biopolitics and Biometrics: Refugee/Asylum Seeker Management in the Digital Humanitarian Age.' LSE International Development Review, 4(4), 1–9.



alignment with mainstream data policies, though there was limited organisational appetite for this approach. I initiated a decentralised identity wallet project addressing data interoperability issues, but the project didn't continue after my departure as priorities shifted. In humanitarian organisations, the challenge is prioritising technology investments when they compete with immediate needs like schools or water supply. Identity registration, while foundational, does not always receive the recognition it deserves. It's not exactly the most exciting part of humanitarian work, but it's absolutely essential. Institutional context shapes willingness to innovate. WFP has transformed from food logistics to cash logistics partly from organisational survival pressures, making them more innovative than UNHCR, which is fundamentally an organisation of lawyers. Don't underestimate how conservative lawyers can be!

Looking ahead, I believe refugee registration will need to remain contextual rather than universal. A case in point is the situation in Ukraine since 2023. Ukraine regards its Diia application[25] as an embodiment of national sovereignty and severely restricts the use of identity systems brought to the country by the UNHCR, the WFP and other aid providers. UNHCR has learned there are drawbacks to centralising too much data. UNHCR's biometric database, BIMS, is nationally siloed by design. Field offices see only their country's data, while headquarters can view everything. This has created situations where headquarters identified cross-border issues but lacked a strategy for approaching governments without undermining their authority. We could

25 Ukraine's Diia (Дія, meaning Action) is a national digital government platform and mobile app that allows citizens to access official documents and public services online, effectively functioning as a digital ID and e-governance system.

see things happening like double registration of children across borders,[26] but we couldn't tell governments without making them look ignorant.

The most significant institutional trend I foresee is the privatisation of refugee registration. When Rohingya refugees entered Bangladesh in 2017,[27] the government received numerous offers from companies to handle registration. This connects to the shift towards cash-based assistance instead of in-kind goods. Financial institutions like Mastercard are investing in humanitarian projects because they can manage large-scale cash programmes but lack the identification component. I expect private companies will increasingly contract directly with governments for refugee registration. What governments really want is exclusive ownership of refugee data—something UNHCR has been reluctant to concede. This trend will likely accelerate, though it may be limited in very poor countries unless there's a sponsor with strategic interests. Refugee registration is moving toward a more privatised, government-controlled model than the humanitarian-led approach of the past three decades.[28]

By the end of 2025, the world underwent significant geopolitical shifts. While humanitarian agencies are facing unprecedented funding cuts, a digital-industrial and services complex focused on population, border and migration control has emerged in the United States. This observation is also true for the European Union, albeit to a lesser extent. The intertwined relationship between US law and migration enforcement agencies, and the high-tech sector that supplies them, creates vested interests that influence public policy. As with the defence industry, the driving factor behind the relationship between governmental agencies and digital corporations is mutual benefit: one side obtains technologies, and the other is paid to supply them.

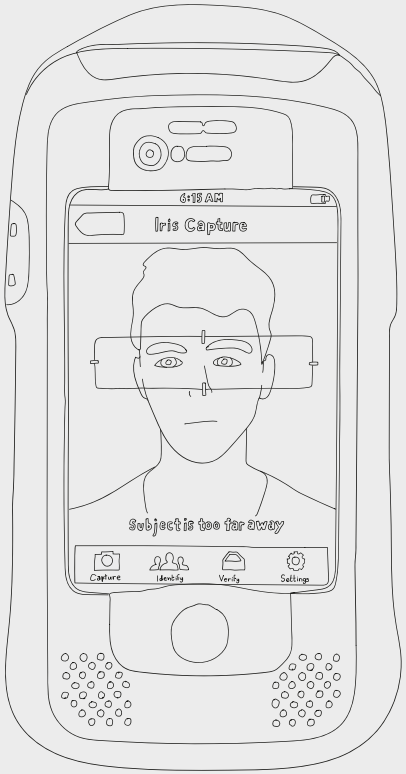
This development may initially be limited to the United States, but in the medium to long term, similar structures are likely to emerge elsewhere, too. Although a first attempt to establish new aid structures during the Gaza war may have failed,[29] it is likely that political and economic players will continue to experiment. Governments will want to control population movements and humanitarian aid while the digital-industrial and services complex will make profits from the provision of the necessary technologies. In view of the above, humanitarian agencies may be forced to make stark choices: They must either become executors of policies and technologies that serve the global interests of the digital-industrial and services complex or turn into non-operational observers of politically determined aid policies.

26 See Keren Weitzberg's research on double registration in Kenya, where citizens are 'trapped' in humanitarian biometric databases, meaning they struggle to access citizenship rights: Weitzberg, K. (2025) 'Keeping people out of camps: biometric technologies, contested sovereignty, and border practices within humanitarian spaces' Journal of Ethic and Migration Studies 51(14).

27 In 2017, over 700,000 Rohingya fled persecution in Myanmar to Bangladesh, creating one of the world's largest refugee settlements.

28 The conversation with Karl up to this point was held in October 2024. The preceding conversation was conducted in November 2025.

29 The operations of the 'Gaza Humanitarian Foundation' from February to November 2025 included biometrics and other digital technologies. See: Skyline International for Human Rights (2025) 'The Price of a Meal: Forced Biometric Surveillance and Military Control of Humanitarian Aid in Gaza'. Accessed at: https://t1p.de/cfvh7.




*Volker Schimmel*

# The Inclusion Dividend: From Control Systems to Trust Ecosystems for Refugees

*Volker is the Head of Global Data Service at the UNHCR. He is currently based in Copenhagen, Denmark.*

My path into humanitarian data didn't start with technology. I studied conflict and displacement at the LSE in the late 1990s and early 2000s, during the pivotal Iraq War era. I then worked with UNHCR in Rwanda's Great Lakes region on repatriation and external relations. I am a lifelong but self-taught tech enthusiast who always considered digital tools as part of problem-solving. In Rwanda, there was no data unit or digital infrastructure in place, so I learned MapInfo and began producing digital maps for internal and external communications. As a non-lawyer among many legal colleagues at UNHCR, data visualisation gave me a new language to bridge important conversations.

Disaster management coordination roles pulled me deeper into databases and information management systems. Working in Burundi, I taught myself Lotus Domino, Access, and SQL. Then, my UNRWA (United Nations Relief and Works Agency for Palestine Refugees in the Near East) position became one of the most significant of my career: a six-year urban planning project redesigning Palestinian refugee camps—one just 600 by 200 metres yet home to 10,000 people, with two schools, two mosques, and a health centre. We decongested the camp, replaced single-storey shelters with multi-storey buildings, and created public spaces. This community-driven planning touched the core of Palestinian identity, where any improvement risks resembling naturalisation and undermining the right of return. It was delicate work, involving everything from supply chains and

government liaison to managing technical staff, architects, engineers, and data. I learned early, long before formal data policies, that every operation has a data systems dimension. Starting in the 2000s—mid-Web 2.0, when open source was exploding, but before we had anything like SharePoint—I introduced tools like Dropbox for data sharing, replacing the practice of shipping around bulky external hard drives.

When the Syrian civil war began in 2011, I led UNHCR's field office in Jordan over four years, responsible for 500,000 people, refugee registration, cash programmes, and more. Identification challenges in Jordan reflected broader, longstanding patterns we are still dealing with today. First, establishing identity. When people cross borders without documents they can share or we can trust, establishing identity with any confidence is extremely difficult. Second, issuing credentials and preventing fraud. Once identity is set, how do we reliably recognise people across hundreds of thousands of interactions with only a few hundred humanitarian staff? We need cards, biometrics, and other ways of helping staff quickly and accurately confirm identity and authorise access to entitlements. Third, enabling partners. With its refugee protection mandate, UNHCR's privileged role in identity management carries a responsibility to support other humanitarian actors. That has meant overcoming institutional reluctance to share data and moving toward collaborative models. The fourth challenge is government transition. Ultimately, identity management should rest with the state, not UNHCR. The challenge is ensuring meaningful transition to government ownership and leadership. There are different models and pathways to inclusion for refugees, but inclusion is paramount.

Historically, establishing and registering identities has been a costly and burdensome process for both beneficiaries and agencies. Humanitarians expend significant time managing appointments, and refugees take children out of school or leave work for mundane registration tasks and journeys to centres. One of the biggest priorities I'm pushing is The Digital Gateway: UNHCR's digitalisation of registration. Nobody physically goes to bank branches anymore; why should refugees be obliged to visit registration centres? We need a mix of new channels between website apps, call centres, kiosks that make the process accessible and frictionless.

In Jordan, we introduced biometrics. Fraud had quickly become a recurring challenge in UNHCR's cash programmes; everything from misrepresentation to selling identities to selling entitlements. We saw a futures market in ATM cards, with people buying stacks of cards from refugees, who had commitments for three to six months of cash assistance but needed money immediately. This was driving diversion at peak of 20%. Such a high level of diversion jeopardised our work, made the overall level of risk untenable and had to be addressed. That's where the biometric layer comes in, introducing in 2012 an iris-scan at the ATM to confirm that the person presenting the credential is its legitimate holder. Biometrics have become crucial for preventing misrepresentation and identity theft. We're continuously examining and improving the consent and data-protection implications, but in my view the costs of not having a secure binding are far higher.

Identity registration still brings challenges which we need to focus on; but let us also build beyond it. We need to lower the bar so that our systems are fully contingent on individuals volunteering information rather than UNHCR making data decisions on their behalf. There might still be cases of legitimate basis beyond consent in lifesaving or mandate-specific data decisions, but overall, we need to move towards a model centred on beneficiaries' individual agency. Another of my priorities is therefore the verifiable credentials approach. This means we secure identity and biographic data, encrypt it with our private key, and issue it to individuals as a credential. Individuals hold and control the credential themselves and present it to any organisation that uses our public key to verify their authenticity. The underlying technology, public-private key encryption, is decades old; our breakthrough lies in lowering the adoption barrier by providing not only the public key but a simple verification app and in the future possibly software development kits. Crucially, this model

doesn't require a 'phone home'[30] to UNHCR: you don't have to have a live link back to UNHCR to fetch an identity. You don't have to call a central server to confirm that somebody is who they claim to be. Verification happens instantly, even offline. It's low-tech, robust, and easy to replace, which matters enormously in our operating environments.

Individuals should be able to share only the specific information required for a given interaction rather than exposing all data each time their identity is verified, which can happen with credentials like QR codes, and certainly with verifiable credentials. In Erbil, Iraq, we piloted iris biometrics for cash delivery using point-of-sale devices designed to let people choose what data to share. In the end, the solution was effective and proved important during the COVID pandemic. At the same time, we encountered common implementation issues that remain a challenge to address. Operators were sometimes impatient or poorly trained, and users had limited digital literacy. That's what worries me most: not biometrics themselves, but the gap between good intentions, system designs, and user capacities. We make assumptions about how intuitive a system is. When these gaps emerge, the stakes of identity, entitlements, and protection are high in humanitarian settings. Operator behaviour in vendor delivery situations is another overlooked risk. Enormous power sits with those distributing food or cash, and with shoestring staff and thin oversight at scale, misuse can undermine even the best technical safeguards. Relying on the in-person interaction between the individual and the verifier, selecting what information the individual wants to disclose, comes with significant risks of abuse and coercion.

30 'Phone home' means that the digital identification system communicates with the original issuer or a proxy to verify the validity of the credential. This configuration allows tracking: it provides the issuer (here, UNHCR) with a record of every time a beneficiary uses their digital ID to prove their identity. See the No Phone Home Campaign: Young, K. (2025) 'Nearly 100 Experts Are Saying "No Phone Home"' https://identitywoman.net/no-phone-home-what-it-means-and-why-it-is-important/.



We're working closely with MOSIP[31] on selective disclosure of identity information in refugee settings. However, the standard assumption is that one person has one stable phone number and one device over time. Those conditions simply do not match UNHCR's operational reality, where many beneficiaries lack smartphones, SIM cards change frequently, and devices are shared. In regions with high smartphone penetration such as the Middle East, Asia Pacific, parts of Europe, we can move faster. But across much of sub-Saharan Africa, parts of Western Asia, reaching widespread self-managed digital identity will remain difficult for at least the next five to ten years. I often consider Estonia's e-government journey, a national priority that still took 20 years to build and refine—a reminder that the hardest parts like digital literacy, data governance, and edge cases are usually resourced last, yet ultimately determine whether any of this works.

The past 15–20 years have been about moving from isolated, monolithic identity systems to a shared trust ecosystem with clear standards for exchanging data. For years, the humanitarian sector has worked in silos. Some organisations have played fast and loose with data, while big agencies like UNHCR hoarded crucial data. Data sharing wasn't the norm, even though other organisations may have needed it. With the advent of the cluster system[32] 20 years ago, and the explosion of NGOs, different engagement was necessary. When I started as Head of Data Service nearly five years ago, I pushed for a trusted systems approach, especially in protracted operations where multiple organisations serve the same people. My predecessors' vision linked trust with blockchain, while I see the future in international standards

31 The Modular Open Source Identity Platform (MOSIP) is a digital public infrastructure used by various global governments to run national ID systems.

32 Attributed to Jan Egeland, UN Emergency Response Coordinator, in 2005, 'clusterisation' was a systemic reform by which humanitarian organisations were grouped into specific sectors such as health, water and shelter, with designated 'cluster lead agencies' responsible for coordination within that sector.

derived from ISO and ICAO[33] rather than technology specific. My pitch was always: data sharing must happen because partners deliver life-saving services to people whose protection is our responsibility. We all have to play by similar, predictable rules, which correspond with risk. The most difficult part is data protection agreements, which require an iterative process of agreeing on language, scope, and terms. The conversation usually starts with 'Give us your data,' which immediately raises questions: What data? For what purpose? What elements are actually necessary? That's where the real work lies: carefully defining scope, purpose, reciprocity, and data subject rights. After that, the rest should just be flipping switches to let data flow back and forth.

One truth I've learned is that nothing is as permanent as an interim solution. There has been a chronic duplication problem in the sector. Organisations would land in the field and spend millions of dollars—or the shoestring budget they had—building their own parallel systems, then the identity ecosystem would fragment further. We're working to change that. We have developed PING, the PRIMES Interoperability Gateway, as a standard protocol for data sharing and identity authentication. This aims to create trust and contractual reassurance that mutual rules are observed. Once a data-sharing agreement is in place, interoperability should take only days, at the most a couple of weeks, to start, not months or years. The system must work for the full spectrum of partners, from those with no technology to large agencies and governments with complex IT systems. In February 2025, together with WFP we presented a Tanzania proof of concept based on these principles and technologies to our respective senior leadership, showing what a seamless, fast, secure, data-protection-forward model can look like. It received strong support—not just because of the funding crisis, but that helped. By late next year or mid-2027, we expect to have global roll-out and a blueprint ready for any new operation.

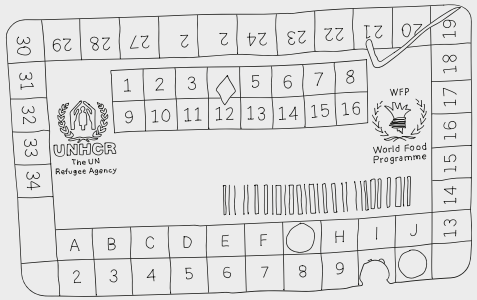
Taking the medium and long-term view, none of this should be UNHCR's, WFP's, or anybody's responsibility other than the state. Our goal is a world where every country has the capability and the interest to include refugees in their national systems. But inclusion can serve very different purposes: Are individuals being included to surveill and expel them, or to give them recognised identities that unlock services like SIM cards, work permits, and social protection? This 'inclusion dividend' is the central question with governments.[34] Ultimately, humanitarian organisations operate at the invitation—and sometimes the impatience—of governments, which can pressure us, expel staff, or shut down cooperation. This is part of the operational reality and not unique to identity management, but it matters. Governments often worry that refugee data could be repatriated to countries of origin—either because of good bilateral relations or a political shift that triggers pressure to 'send people back'. That risk shapes many conversations about data sharing.

Governments' institutional capacity is also a major challenge. This is improving, but 10–20 years ago even large operations—whether in Iraq or across sub-Saharan Africa—often relied on a single database built by one overworked staffer on an underfunded ministry's laptop. Questions of IT security, access management, infrastructure, and data lifecycle simply didn't arise because the systems were too fragile. Some contexts still look like this today: for example, Burkina Faso's IDP (Internally Displaced People) registration system, where we are working with the government to help modernise. The good news is that many governments are developing clearer digital strategies, national clouds, and stronger data protection laws, which is an entry point for the right way of including refugees.

33 ISO is an international body that develops technical standards used worldwide, including standards for identity documents, smart cards, and biometrics. ICAO is a UN agency that sets global specifications for passports and other travel documents so they can be securely read and verified across borders.

34 See Schoemaker, E., Martin, A., & Weitzberg, K. (2023). 'Digital Identity and Inclusion: Tracing Technological Transitions'. Georgetown Journal of International Affairs 24(1), 36-45.

Interoperability with governments can take two forms. First, a country can integrate refugees directly into its national ID system, issuing them legally valid, recognised identity documents while noting their status. Ethiopia followed this model, using UNHCR's data to feed into its issuance process. Second, a government may choose to register refugees entirely on its own. This is acceptable if the outcome, recognised identity, is achieved. But it carries risks: we lose the ability to apply integrity checks or compare records, even though misrepresentation (especially nationals trying to register as refugees) is a persistent challenge. Without feedback loops, UNHCR may hold incomplete or incorrect data, and governments may duplicate investments unnecessarily. More importantly, this can undermine the integrity of identity data that underpins international protection. These approaches are not yet 'verifiable credentials'. They treat UNHCR as a trusted registry used by a limited set of partners. But once inclusion expands to a much larger ecosystem, verifiable credentials become relevant. Verifiable credentials build on interoperability by enabling trusted data exchange without requiring UNHCR to sit in the middle. They preserve the trust foundation while effectively disintermediating UNHCR, which is a key step for scaling identity inclusion for refugees across many actors.




*Ryan Beech*

# Doing More with Less Data: Building Proportional Identity Systems

*Ryan is Head of Identity Management Operations at the United Nations World Food Programme (WFP). He is currently based in Munich, Germany.*

I lived in a village in El Salvador with the Peace Corps for two and a half years in my early twenties, but I had no plans for myself thereafter and I had never heard of WFP. During my master's in international relations, a professor recommended an internship with WFP in Jordan just as the Syrian crisis was kicking off in 2012. I moved to Amman and joined what was initially a small, understaffed country operation that had been doing technical support to the government for school feeding. Suddenly, it became a major crisis response with half a million Syrians crossing the border. It took time to establish the new emergency operations in the country office and my first role as a humanitarian was focused on writing situation reports, with English writing being my only directly transferable skill, along with a willingness to live and work from Mafraq where the new Zaatari refugee camp was located. This is where I gained relevant experience in humanitarian operations.

By the time I left Jordan in 2017, I was heading up the cash and voucher operations. The office had made major evolutions in assistance—we started with hot meals catering to refugees, then moved to paper vouchers, digital vouchers, then biometric iris scan payments, and eventually blockchain. I led a small technical team responsible for managing household data and worked with the financial service provider to deliver the monthly cash assistance to half a million people. I later moved into an HQ role advising country offices and working

on our corporate standards, systems, and capabilities, all under the banner of cash-based transfers (CBT). At that time, there wasn't a separate identity management portfolio, but when that emerged as a priority, CBT experts clearly had the right experience. The identity aspect was core to our programme quality and assurance: how to prioritise assistance with vulnerability targeting, produce lists of who you will reach, ensure those lists are connected to a payment modality, all while safely managing data, detecting duplicates, leakage and fraud, et cetera.

In 2020, I led the development of the Cash Assurance Framework for WFP, which outlines the priority controls for operational assurance and programme quality. I made it my mission to enhance the resources available to our peers in the field, and I wanted them to have more support in terms of guidance, systems and services than I had when I was starting out. We therefore also developed cost-recoverable business services focused on assurance to help the field operations digitise core business processes such as identity registration, verification, entitlement card management, reconciliation and anomaly detection. I'd like to think that this work made a significant impact in the level of assurance in WFP's CBT operations, much of which we are now also applying to food delivery.

The recent funding cuts are worrying. WFP country offices are having to let go of staff and significantly reduce the amount of assistance to people in need. Our team will have to say goodbye to real technical experts who support critical innovations like self-registration, anomaly detection, photo deduplication—a cost-effective alternative to fingerprint biometrics. Self-registration for example has changed the game in terms of speed, convenience and assurance in our operations. In Gaza, residents regularly update their household information including phone numbers and location details without having to visit a registration site, which allows us to update distribution lists and prevent duplicate food delivery even without internet access. In Sudan, WFP registered 7 million people in 10 days in inaccessible parts of Darfur, allowing WFP to send money remotely to families in need where we couldn't send trucks. Unfortunately, with these cuts, we will lose some of our core technical staff who ideated and maintain these vital new solutions, despite the millions of dollars in efficiencies these activities bring.

For identity management in general, it's important to acknowledge that a one-size-fits-all approach doesn't work. Context is crucial yet poorly understood. Rigid and unresponsive systems can result in field staff relying on Excel and other workarounds which are less secure and less efficient. We've had more success applying modular flexible solutions that are designed with a clear understanding of the business purpose and that can be configured for each country operation. Contexts can vary in terms of the approach to identifying people, availability of internet, or role of WFP and partners. When we can make use of available data or IDs or collapse key business processes into fewer steps then we can increase the efficiency of operations and the convenience to the people we assist.

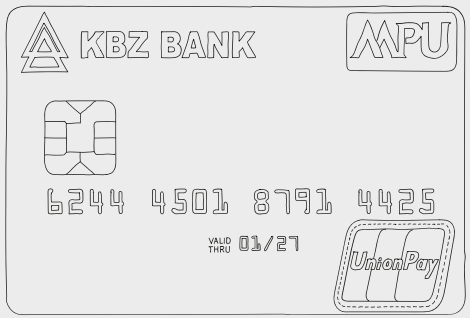
As humanitarians working on systems and data, I think we need to be thoughtful and measured in our response. We should always strive to have a very clear understanding of what we are trying to solve and why, and from that be able to identify what we need to do it. We should try to do more with less when it comes to asking for people's personal data, especially biometrics and especially from children. Operational controls should be proportionate to the assistance and services we are providing and with a broad analysis of risk. For example, children that are receiving assistance today will be alive decades from now, do we know what the world will look like then in terms of technology and the authorities in power? How certain are we that data we collect today won't be used to persecute people in the future? We need to be very careful.

I'm not a huge fan of the idea to set up big mega systems that everyone can dip into for data they want. I haven't seen it work in practice and large data pools can increase privacy risks. Social protection research on government registries shows that programme-specific databases can be

more effective, up to date and secure.[35] Humanitarian work is hard, and we are constantly under pressure and faced with constraints including not enough time, resources or staff. Therefore, I think we need to be humble in terms of our ability to keep sensitive data safe. Even if we control for cyber security risks, which is harder than ever these days, there is always the risk that staff fall victim to phishing scams and handover their log-in passwords. The safest approach is to not collect data we don't need and to delete data when we no longer need it.

Given the resource constraints across the humanitarian sector, I think now is the time to leverage existing tools and comparative skills across agencies. We all have less capacity, and so we need to work together to make best use of what we have. Getting caught up in competition over whose system to use is unhelpful in my opinion. In WFP we often use partners' tools and data, and it can work fine. We also partner with the private sector to deliver assistance digitally, and this will likely increase. I think what is important is to ensure capacity for humanitarian roles, such as understanding population needs and their preferences for receiving assistance and participating in programmes, listening to their feedback and adjusting operational designs to ensure aid reaches the people we aim to support. These are roles that are innately humanitarian and need to be done well by UN agencies, NGOs and government, even while some aspects of aid delivery are absorbed into private sectors. Our clientele has different needs and aspirations compared to those who companies may focus on.

35 See Barca, V. & Chirchir, R. (2014). 'Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries'. London: Overseas Development Institute. Accessed at: https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf.




*Tina George Karippacheril and Juul Pinxten*

# Efficiency for Whom? The Hidden Costs of Digital Social Protection

*Tina and Juul are colleagues at the World Bank. Tina is Lead Social Protection Specialist for Nigeria based in Abuja, coordinating a $7.6 billion portfolio of programs on Health, Education, Social Protection, and Gender. Juul in an Economist based in Washington DC whose work supports social protection reform in Yemen, Egypt and Djibouti.*

Juul: I met Tina shortly after I joined the World Bank in Indonesia back in 2014. At the time, about 10-15% of Indonesians were receiving cash transfers under different social assistance programmes, and it was all delivered by the postal system. A few years later, I had heard a story that the Queen of the Netherlands, who was Ambassador for Financial Inclusion back then, had made a visit to the President, asking him straight off the bat, 'How many people here are banked?' Long story short, he ended up thinking 'Why don't more Indonesians have a bank account and how can I change that quickly, before the Queen comes back to visit again?' That was the turning point. Within a very short time, all social assistance payments were to be made through the banking system. This pushed forward ATM cards and formal identification processes that banks required, which so many people were missing.

Tina: I love the story about Queen Máxima, it's one I like to tell too, and there's a second part to it. On one of our field visits back in 2016 we then went to an island called Buru. One of the women there was a beneficiary of a cash transfer programme. She was among the 10 million poor households who got one of the new ATM cards. But she also had to walk for a full day to get to the nearest ATM and withdraw the

actual cash. With the previous postal system, though it had very high distribution costs, the cash assistance came directly to the village. The critical point is, there are always frictions between administrative efficiencies through digitalisation at the back end, and the lived realities of those on the front-end, especially in rural and remote areas. There are private costs that need to be accounted for from the get-go, hence the importance of a human-centred approach when we are designing digital transformation that works optimally for people and administrators.

Juul: From our meeting rooms we might argue that new technology is more efficient or identify ways of saving money that will then be used to improve the overall benefits or coverage of a development programme. But this should not come at the cost of the beneficiary. In the end, efficiency may not be gained in all the senses you want it to be. Since the withdrawal of USAID and other major cuts to foreign aid, this narrative of value for money has taken even more prominence than before. I wish it had happened earlier because now there's very little money to gain value out of. I do think that digital systems building will suffer from the aid cuts, even though the value of this infrastructure approach is more recognised than it was 15 years ago.

Tina: The decline of foreign aid represents a watershed moment in West Africa and everywhere. For context, the World Bank's goal is a world free of poverty, and shared prosperity. France was the first country to borrow from the Bank post-World War II and then 'graduated', becoming one of the largest shareholders and donors to IDA (International Development Assistance), the Bank's concessional fund for the poorest countries. South Korea is another great example, as a recipient of IDA in 1961, then transitioning to being a major donor to the Bank, providing financing and knowledge to help other developing countries. The Bank's role is not just providing financing but know-how and technical assistance for governments to become self-reliant, stable economies. We might be in the kitchen with them, but our partnership follows the country's economic and development agenda. With recent aid cuts, countries are taking a greater role in domestic resource mobilisation. Governments will be working more closely with the private sector to deliver services to people, raising domestic resources to do it, using their budgets more effectively.

There's an ongoing debate around whether governments should be the ones implementing digital ID systems or not—whether identification should follow a decentralised 'self-sovereign' model where individuals control their own digital credentials or a centralised government-wide model. My view on this is: There is no 'one-size fits all'. Every country will pursue its own context-specific approach. A promising example I have worked closely with is Togo's e-ID programme, overseen by the Ministry for Digital Economy and managed by Agence Nationale d'Identification (ANID), and it's one to watch. It's a beautiful laid-out architecture, W3C[36] compliant verifiable credentials and delivered free of cost to people, especially for the poor who cannot afford expensive cards. What makes it noteworthy is they have developed targeted communications, for example to young people to understand and pick up their e-IDs, bringing in hip-hop artists and musicians to encourage adoption. Their hard work is inspiring, creative, and positive. In time, take-up of digital identification and payment systems in Togo can fundamentally improve health, education, water, energy, or social assistance service delivery, and financial inclusion of the poor in underserved and rural areas.

36 A W3C-compliant digital ID follows global standards from the World Wide Web Consortium (W3C) for how digital identities and credentials are created, shared, and verified. Using Decentralised Identifiers (DIDs) and Verifiable Credentials (see definition above) to secure identity data while enabling interoperability, meaning digital IDs issued by one system can theoretically be trusted and used across different platforms, countries, and wallets.


*Amalraj Nallainathan*

# Beyond Legal Status: Designing Identity Systems for Complex Needs

*Amalraj has worked with the International Organisation for Migration (IOM) for over 18 years. His Programme implementation and information management roles have taken him to South Sudan, Nigeria, Sri Lanka, Bangladesh, and beyond.*

When I deployed to South Sudan in 2013, we were tasked with registering internally displaced people sheltering in a Protection of Civilians (PoC) area. These families were fleeing for their lives, trapped by violence and unable to engage in any livelihood activities. Registration was their only gateway to food assistance and basic survival supplies. In this desperate situation, huge crowds flocked to get registered, and the pen-and-paper process we used was chaotic and burdensome for everyone—beneficiaries and staff included. In such a remote location, we relied on wristbands or indelible ink marks on skin to prevent duplicate registrations. These methods were fundamentally untenable; ink faded, bands broke, and crowd control became dangerous. We knew it was our duty to provide assistance in a more dignified way.

In 2015, we introduced biometric registration. This technology quickly became a practical solution to address the widespread lack of national identity documentation, allowing us to manage the aid delivery process with far greater efficiency and effectiveness. Consequently, we implemented biometrics to address similar challenges in Somalia, Nigeria, and Chad. In contexts like Somalia, uncoordinated registration processes by multiple agencies created a high risk for fraud, aid diversion, and significant wastage of resources. Unlike the PoC registration in South Sudan, this operating

environment is far more complex and demanding. Here, the objective is not only to streamline operations and prevent inclusion or exclusion errors, but to mitigate aid diversion in insecure, remote areas with limited infrastructure. Achieving this requires robust data exchange among partners to coordinate identity issuance, deduplication, and assistance effectively.

Central to a truly people-centered approach is addressing the critical challenge of 'survey fatigue'. Beneficiaries are frequently interviewed by multiple partners providing various forms of aid, creating an immense burden on people already in distress. To eliminate this fatigue and avoid repetitive registrations, the partner responsible for registration should serve as a central point, facilitating referrals to other service providers rather than subjecting people to multiple registration events.

In contexts of internal displacement, functional identity management serves specific operational goals: ensuring accountability, facilitating referrals to other services, and eliminating duplication. Its purpose is to enhance the efficiency of aid while ensuring assistance is people-centered and dignified. Crucially, these systems are not intended to establish a foundational legal identity. Therefore, the data we collect must remain strictly proportional to our humanitarian purpose. This principle compels us to scrutinize the use of biometrics carefully: when is it reasonable to demand sensitive biometric data from those seeking lifesaving support? We do not use biometrics universally, but only in specific contexts where no other reliable means of verification exists. It is also important to note that, unlike in refugee contexts, assistance for internally displaced persons is rarely based solely on legal status. Instead, it is vulnerability-based, often targeting a mix of internally displaced people, host communities, and migrants. Consequently, relying on status-based identity issuance can be challenging and less effective for delivering humanitarian assistance in these complex environments.

In internal displacement contexts, the primary use cases for identity systems are to maintain records for accountability, prevent exclusion and inclusion errors through a single registration, enrol people in multiple sectoral assistance programs through referrals, and finally, to transition people into social protection systems where national systems work. When digitalising humanitarian aid delivery, our priority must be to use existing foundational identity documentation, such as national IDs, wherever possible. In contexts where national systems are inactive or cannot be restored within the emergency timeframe, humanitarian partners must issue functional identities through registration. However, the broader goal remains bridging the gap between these temporary 'functional' identities—essential for emergency aid—and the foundational identity systems required for long-term recovery. As displacement becomes protracted, families' needs evolve from immediate shelter to durable solutions like employment or land tenure. Identity management serves as the critical link to these services as needs change. IOM operates in these protracted contexts with a clear vision: our identity work supports not just the provision of aid, but the ultimate goal of ending displacement.

While foundational identity management is typically a streamlined process led by the government, managing functional identities—an essential component for digitalising aid delivery—is far more complex. This is especially true in large-scale emergencies where the state requires international support, introducing a multitude of actors and systems into the response.

A coordinated approach is the bedrock of effective humanitarian action. It enables us to engage multiple partners to deliver services rapidly while upholding quality standards and preserving human dignity. Registration, the issuance of functional identity, and the digitalisation of aid delivery are no exceptions to this rule.

In large-scale responses requiring international support, the landscape is crowded with diverse actors: government ministries, NGOs, civil society organisations, UN agencies, INGOs, and the private sector, each bringing varying operational capacities and resources. Often, the creation of a functional identity happens at the first point of contact for assistance. We must therefore acknowledge that any

operational partner may be the one to conduct that initial registration. To address the challenges of fragmentation and duplication, it is imperative that this data be shared among all partners involved in registration and delivery. This is where a truly coordinated registration ecosystem becomes the key to success.

However, coordinating registration is distinct from other sectoral coordination mechanisms. Because the processes handle the personal data of beneficiaries, the partner processing the data is legally responsible and accountable for upholding the privacy and confidentiality of the data subjects. When a partner shares data with another entity, these responsibilities and accountabilities must be governed through legally binding data sharing agreements. This is why we view coordinated registration as a challenge of four-dimensional interoperability, encompassing legal, governance, technical, and semantic dimensions.

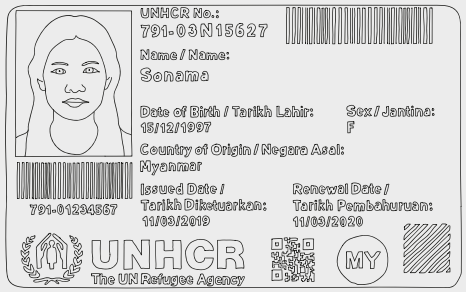
In Somalia and South Sudan, we have been working extensively to improve interoperability for functional identity and beneficiary data. However, establishing safe data sharing is difficult because humanitarian organisations operate under a variety of legal and data protection frameworks. UN agencies have specific privileges and immunities and manage data under their own policies; NGOs must often comply with national laws or GDPR; and government counterparts have their own sovereign requirements.[37] Furthermore, specific technologies from major tech firms may not be accepted in countries with strict laws regarding data processing and storage outside their borders.

To solve this, IOM is advocating for a federated beneficiary data management approach. Instead of trying to force all agencies into a single, centralised database—which is legally complex and creates a single point of failure—a federated system connects us. It enables data management among partners, creating an ecosystem where government counterparts, UN agencies, INGOs, and the private sector can seamlessly verify and access identity data in real-time without violating their respective legal frameworks. This approach respects each organisation's role as a data controller while ensuring that a registration record created by one agency can be trusted and used by another to deliver services more quickly.

We are currently piloting this federated approach through an European Civil Protection and Humanitarian Aid Operations (ECHO)-funded project. Building on the past work of the Collaborative Cash Delivery (CCD) Network and Dignified Identities in Cash Programming (DIGID), this initiative aims to provide a comprehensive framework for shared standards, corporate governance, coordinated operations, and distributed infrastructure. Crucially, this federated approach includes the required standards and governance for issuing functional identities; therefore, any partner with the operational capacity and required technology will be able to issue an identity with the same level of reliability and trust.

The current funding crisis makes this coordinated approach to functional identity and beneficiary data urgent. Furthermore, the UN80 agenda and the broader 'humanitarian reset' demand greater efficiency and effectiveness. Investing in a federated approach ensures that smaller national NGOs and government counterparts are systematically integrated into the response. Simultaneously, it allows large international actors to bring their resources and systems to plug in for scale-up and plug out when the response winds down, leaving local capacity intact and the system sustainable.

37 See Kokkinaki, C. V. (2025). 'Legal Tensions: Insights from UN-EU Correspondence on EU Data Protection Law and the Role of Privileges and Immunities in Enhancing Personal Data Protection'. Data Protection in Humanitarian Action: Responding to Crises in a Data-Driven World, London: Routledge, 178–192.




*Joseph Oliveros*

# Dignity With Data: The Limits of Rights Without Inclusion

*Joseph is the Global Cash Lead at the International Federation of Red Cross and Red Crescent Societies. He is based in Geneva, Switzerland.*

I had 10 years' experience in the private sector in management and tech consulting with a background in computer science, before I decided to contribute my skills and practical knowledge to a social purpose. For the past 7-8 years, I've been applying technology in the provision of humanitarian cash assistance to disaster and crisis-affected people. My initial role leading the IFRC's innovation portfolio for cash and voucher assistance led me quickly to identity management. There is a significant gap where people are being left out of assistance because they can't prove who they are. People lose documentation in floods or fires, or when they move due to conflict or climate crises. Some never had legal identification to begin with. The important question is, how can technology help ensure nobody is left out of humanitarian assistance?

The identity problem was something that needed to be addressed across the entire humanitarian sector, a highly challenging problem that greatly interested me. Traditional approaches to identity management have been siloed. So, when opportunities for grants to tackle this problem become available, I knew this has to be done in partnership and in collaboration with others. Innovation Norway funded our 'DIGID', the Dignified Identities in Cash Assistance consortium, which began in 2018. We partnered with other Norway-based organisations like Norwegian Red Cross, Norwegian Refugee Council, Save the Children Norway, and Norwegian Church Aid. They all provide cash assistance in the field though they have different approaches—some focus

on refugees, others have broader mandates, for example. All four organisations had projects and programmes in Kenya, sometimes targeting the same communities. Together, we agreed that identity was a common issue that couldn't be addressed through separate responses, which we had all tried in the past.

The main problem DIGID aimed to address in Kenya was people being left out of assistance due to lack of formal identity. We began to ask: when people affected don't have a legal identity, are there other forms of ID that can be established or leveraged to allow them to receive assistance? There is foundational ID but there is also functional ID; one is legal and government-mandated, the other is simply for accessing services. At IFRC we had long used paper documentation to acknowledge that a given household was eligible for services, and we would ask affected people to keep it and show it to volunteers when claiming their assistance. What if we thought of that functional document as a token? An attestation that a person is eligible and in need that could be translated into digital form.

2019 saw growing interest in verifiable credentials, self-sovereign identity (SSI), and blockchain. In other words, there was a green space for decentralised, user-centred approaches to ID. One organisation pitched SSI to us, and I was impressed by the promise. This approach could better protect people's identity credentials, and this was significant as GDPR and sensitive data protection were high on the agenda at the time. Rather than a centralised honeypot that could be easily hacked, SSI promised to provide strong encryption and information security through distributed data storage. Most importantly though, it was about giving ownership of data to aid recipients themselves. This conversation changed how we viewed identity provision. We recognised the principle of asking: what's the benefit to the recipient? Yes, we improve our own efficiency by providing digital ID, but how can recipients gain new benefits and forms of empowerment? That's why DIGID focussed on dignity. Traditionally, we would keep a centralised store of beneficiary data, but if someone wanted to revoke information, could we actually honour that request? This question became key.



The IFRC partnered with the Kenya Red Cross to conduct DIGID pilots for cash assistance during the COVID pandemic, serving people in rural areas with connectivity issues where normal phones are unaffordable and digital literacy is very low. The big challenge of SSI is that users need smartphones and digital literacy, but that's exactly what many vulnerable populations in these contexts lack. We fully documented the lessons learned from each pilot in our reports, which are publicly available.[38] The pilots were a real test of how much SSI could really be used at the margins where people live in extremely difficult conditions. It forced us to look at tech adaptation and question the promise of digitalisation. When dealing with attestations of identity where people don't have smartphones, it was interesting to explore alternatives. What do we give to an individual who doesn't have a phone? The best we could provide was issuing a paper QR code that allowed organisations to verify credentials linked to the QR code. We needed to explain what a QR code was, why people should keep it, and what it did. It was a stripped-down version, but it proved that we need basic, accessible, and context-specific solutions. We also looked at feature phones and provided an SMS version so people could see what information they had, giving some direct access. If someone had a smartphone, that represented the end of the spectrum where some self-governance of data could happen. Without expanding digital inclusion, expanding data rights and autonomy is challenging.

If we really want to fully benefit from the promise of SSI, it requires a highly digitally enabled environment. Not just humanitarians should invest in this more dignified future. The private sector and government need to provide infrastructure to increase the resilience of individuals through digital connectivity and literacy. Through verifiable credentials, the

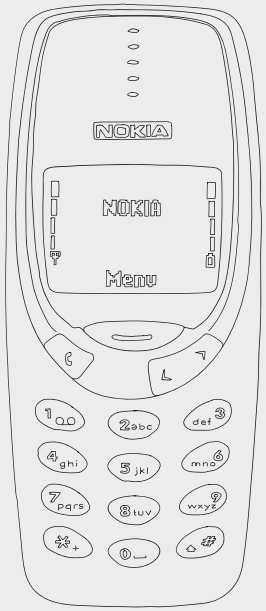
38 See IFRC's interoperability work: https://interoperability.ifrc.org/.

SSI stack[39] promised to create shared data standards. Digital identity would follow the same format and rules, making them universally readable and trustworthy across different systems and organisations. Our vision for interoperability was that it shouldn't depend on one provider. We worked with a blockchain company called Gravity at the time, but in principle you should be able to work with Microsoft or any other provider using the same standards. In reality, once you create your digital ID through one stack, delivering it with another provider requires significant work. We need more than standards to ensure other organisations will recognise the same identity using different technology. Humanitarian agencies need to agree on 'levels of assurance' to recognise credentials beyond their own organisation. We should be ensuring that once data is collected and verified by one organisation, other organisations can recognise it. This is how we will minimise the over-collection of data from aid recipients and fast track our assistance to them.

Regarding legal identity, we have no intention of creating a parallel system in lieu of legal identity, but it's difficult to explain to governments that this isn't what we're doing. When humanitarians talk about digital identity, we must be cognisant that governments, especially in migration contexts, are sensitive about the term 'identity'. That word falls under their mandate, and they might assume we're trying to create a parallel refugee or migrant identity. In Uganda, we stopped using the term 'identity' and started calling it 'credentials' or 'digital wallets' so authorities didn't think we were encroaching on their role. People affected sometimes have a much stronger basis of trust in functional humanitarian ID systems and the organisations backing them than the available government-led ID. Trust is a key issue. Maintaining trust requires strong data protection and not sharing data with any parties that could compromise that trust. Trust takes time to build but a single instance can destroy it. We need to consider these dynamics carefully when we integrate with government and social protection systems, which is ultimately important because the functional IDs we provide don't give people access to public services, banking, or help them pay taxes. When humanitarian funding stops and organisations leave, the people in need and local actors remain, and often so does the need for assistance. We need sustainability beyond the humanitarian piece, with referrals to longer-term resilience building.

The biggest barrier I see in humanitarian digital identity management is the siloed approach. Large, well-resourced organisations can invest in their own solutions to tackle the identity problem. Because of current funding constraints, now is the time to look at who is doing what, and if we're doing something similar, whether we can work together to ensure broader inclusivity. We need to promote inclusion among humanitarian organisations, including those with lower resources, especially local actors that international organisations fundamentally rely on and partner with to reach community levels. Just because a small organisation has low resources doesn't mean it has low capability; they can contribute significantly, especially when they're close to communities and can bring voices from people and context when designing programmes. It's a balancing act between looking for institutional efficiencies while driving dignity alongside that. I believe we need to prioritise dignity more, which will change our approach and shift power dynamics while recognising local and community-based actors. Without this, the default reaction when finances are short is the siloed approach—seeking immediate benefits for individual organisations, taking data without giving affected people access to their own data, and leaving it at that.

39 A stack refers to a collection of different software tools, systems, and technologies that work together as a complete solution. An SSI stack includes the different technologies needed to create, store, verify, and manage self-sovereign identities; blockchain networks, cryptographic tools, identity wallets, and verification systems all working together.




*Jaki Mebur*

# Exclusion by Design: Towards Human-Centred Systems

*Jaki works at the International Federation of the Red Cross. Based in Geneva, Switzerland, she leads the portfolio of digital products and services used by Red Cross and Red Crescent National Societies across the world.*

I began my career as a telecommunications engineer working on mobile networks in Kenya. I was already supporting the efforts of mobile network operators in humanitarian and disaster management, but I wanted to transition from working with machines to a more people-focused role. By 2018 I was working with the Global System for Mobile Communications Association (GSMA) Mobile for Humanitarian Innovation Programme, designing and developing products specifically for humanitarian contexts across the African continent. For the last year, I have been based at the International Federation of Red Cross and Red Crescent Societies (IFRC) in Geneva, building technology that supports national societies in their work across 191 countries, including cash distribution, early warning systems, volunteer management, and identity registration. Identity has always been a strong theme across all areas of my work.

Back in 2016, much of the focus centred on using mobile phone numbers as a proxy for identity, since they are unique and have Know Your Customer (KYC) processes attached to them. The question became how this could facilitate the delivery of humanitarian services. KYC requirements varied significantly between different populations: refugees in camps faced different requirements compared to those with freedom of movement, and displaced people who still held Kenyan identification documents had different needs, all based on Kenyan law. To address these variations, we mainly developed closed-loop systems because refugees weren't considered valid

for standard KYC processes. In the last decade, great progress has been made. Coalitions of refugee agencies like World Vision, UNHCR, WFP and others campaigned to Kenya's Ministry of Social Protection. We have seen these advocacy efforts culminate in the recognition of refugee IDs, allowing people in Kenya to access not only mobile money but also bank accounts.[40] Whilst the bigger advocacy goal is to remove encampment conditions entirely, this has been a big win for the three generations of refugees living in Kenya, who now have access to identity recognition for economic inclusion.

I have seen human-centred approaches to identity management gain traction over the last few years. We are beginning to shed the old-world ways of working. Dignity and thinking from the 'end user' perspective is more important now. Though budget crunches may push inclusive thinking to the back burner when funds are low. Despite this progress, we must remember that identity systems can always be exclusionary by design. I worked on an identity project in Somaliland, involving voice recognition to improve our verification of beneficiaries receiving cash through mobile money. On paper, the project was already a huge improvement on the paper-based system previously in place, which had extremely low identity verification rates, and beneficiaries had to travel long distances just to sign off each time. But we tackled significant bias issues with the machine learning underpinning the biometric system. In our initial rapid testing, the voice recognition worked brilliantly—with around 90% accuracy. As soon as we began testing in the field, this dropped to 50%. Why? We had assumed everyone spoke the same language in the same way. Even after addressing dialect issues and achieving 80% accuracy, problems persisted. We discovered that the mobile network operator delivering the service had mostly male engineers and staff testing the system, whilst most of our beneficiaries were women heads of households. This gender bias hadn't emerged during testing. After addressing that we achieved 96% accuracy. The remaining discrepancy was attributed to people with speaking disabilities, those with lisps, stammers, or elderly people with speaking difficulties. These users simply could not be accommodated. The lesson here is that digital systems will always have social biases. Inclusive, beneficiary-centred thinking is not just a nice-to-have when we are building identity systems: it makes them work.

We need to be accessible when we link identity to humanitarian services, delivering on multiple channels without assuming everyone has smartphones, can read, or speaks English or another dominant language. People should be able to use SMS, WhatsApp, or Telegram, and, in many cases, to access services without registering their identity in the first place. The latter point is particularly important. If someone simply wants to know where the nearest humanitarian service point is or where they can get a blanket or fresh water, they shouldn't have to register and provide personal information. The humanitarian sector should be clear on which levels of assistance don't require extensive authentication. At IFRC, we are working to ensure people can activate their right to be forgotten, synchronising this capability across all our products. Those moving for safety reasons due to crime or threats in their home areas don't feel safe having their data stored in digital systems, and they should be comfortable making this request, multiple times if need be. At the same time, we also want to help those who need us to keep their digital records safe. The ICRC has developed a solution called RedSafe which allows people to upload scanned documents like health records or education credentials and store and recover them with encryption protections.[41]

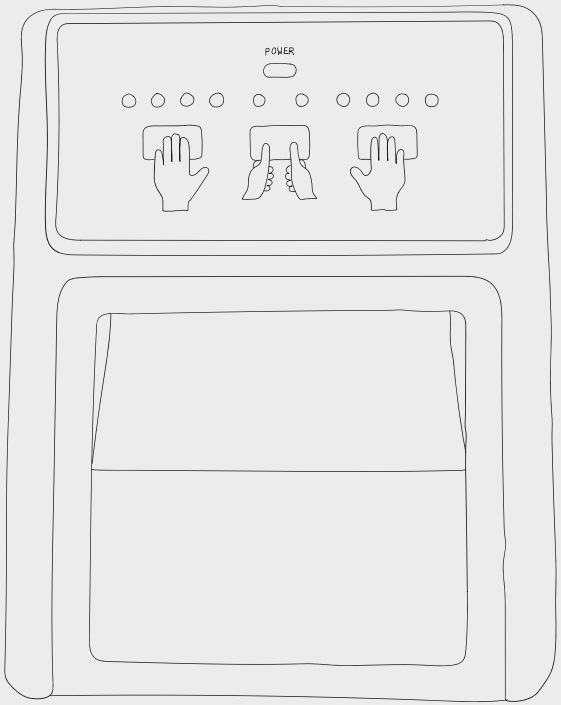
The current funding crisis means humanitarian agencies need to rethink our silos. In the race to maintain each organisation's

40 Recent research with migrants, asylum seekers, and refugees in Kenya reveals ongoing obstacles to obtaining identification. See Weitzberg, K., Loo, S., & Jaffar, A. (2025). 'Integration without Identification?: ID System Challenges for Refugees and Migrants in Kenya.' Caribou. https://www.cariboudigital.net/publication/integration-without-identification/.

41 See Bircher, R. (2025). 'The challenges of building RedSafe, a secure digital humanitarian platform: An Unsafe Journey?' in Data Protection in Humanitarian Action: Responding to Crises in a Data-Driven World, London: Routledge, 72–85.

relevance and funding, we risk losing sight of our real priority, which is beneficiaries—not to preserve the large beneficiary management system each agency has invested millions of dollars in. With my engineering and digital product background, I find the sunk costs mentality bizarre. We need radical honesty when a system doesn't do the best job it could do, and then to iterate, moving towards interoperable systems that support collaboration. This will ultimately benefit beneficiaries more. To build shared standards, we will all need to share resources, build open API endpoints, and be transparent about how we handle identity assurance. There's a tendency to lean heavily on GDPR compliance as a reason for not sharing data, but compliant sharing systems can be built. The donor community will have important influence over the future of identity management. Some of the Scandinavian donors are pushing for collaboration by telling organisations that if they work on ID systems, they need to work together. This steering is key.

It's hard to know what the next decade of humanitarian action will look like. There is urgency to become streamlined and efficient. Technology can help us to some extent, but we cannot simply apply new technology to old processes and expect it to solve fundamental problems. There's a tension between driving efficiencies for organisations to make their work easier and the potential for imposing new challenges on the people we serve. Whilst technology might enable one person to do the work of four analysts or field officers, it might also require beneficiaries to travel an extra two kilometres or add bureaucratic hurdles because there are fewer people reviewing individual cases. The critical question becomes: who is efficiency really for?




*Amos Doornbos*

# Governance Gaps: Why Technology Alone Cannot Fix Humanitarian Identity Systems

*Amos is the Director of Disaster Management Strategy and Systems at World Vision International.*

My journey into humanitarian work began with my family's own experience of displacement. Growing up in Canada as the child of immigrants, I heard my grandmother's story of fleeing when the dykes broke in the Netherlands. She evacuated to the next village with my mother and siblings, but everyone who stayed behind perished in the floods. At the community hall, children were distributed to different families. The histories of displacement on both sides of my family shaped my understanding of vulnerability and community support within immigrant networks, where helping your neighbours was simply what you did.

I worked growing flowers and shrubs and in construction. Then in 2003-4, I saw an advertisement in an outdoors magazine for a Toronto college programme in emergency management. The images of disasters resonated with me. I completed the one-year programme, learnt how to write proposals, and by 2004 found myself in Darfur. Since then, I've worked across the humanitarian sector globally, and looking back, identity management was central to my work from the beginning. I frequently organised response teams and managed information about who we were helping, why, and how. The fundamental question was always there: how do we confirm who people are? How do we verify information beyond bits of paper with lots of thumbprints on them?

In Darfur, working on humanitarian protection and sexual violence cases, I confronted the brutal reality that when doctors confirmed that rape had occurred, they could be killed. This taught me the lifelong lesson that identifying people always carries costs. During a tsunami response, I grappled with calculating the number of affected people. In those early stages, identity management was primarily about reporting numbers and determining what evidence existed for the people we claimed to be helping. While organisations had nice formulas, the ability to say 'this is Amos and we've helped him this many times in these specific ways' simply didn't exist years ago, and frankly still doesn't in many contexts.

The major transformation of identity management in the humanitarian sector has been digitisation. One pioneering example was the Last Mile Mobile Solution (LMMS) created by Otto Farkas from World Vision. Otto was checking into a São Paulo airline with his Aeroplan card when he realised: if airlines can quickly access traveller data from a card, why not give people in humanitarian crises similar cards that we can easily scan for their information? Around 2008-9, Otto developed LMMS. This was before Android operating systems and smartphone proliferation. We were using chunky devices like the Palm and a primary challenge then was the cost of devices. The smartphone revolution and its uptake among aid practitioners made those investments obsolete overnight. Now there's a proliferation of mobile tools. Many of those serving an identification function originally came from health practitioners more so than logistics.

The rise of personal devices has seen the rise of big tech companies' interests in humanitarian aid. A major shift in our sector occurred when the World Food Programme partnered with Palantir in 2019.[42] Donors and other major actors began to co-opt the messaging to frame identity management chiefly around organisational efficiency and fraud prevention—essentially, tracking people. Palantir's links to immigration enforcement were sold as part of the benefit. I see this fraud prevention messaging as rooted in colonialism and what you might call 'povertyism', the notion that people are poor by their own fault, prone to stealing and corruption, and therefore require continuous supervision. It didn't matter how many reports demonstrated that fraud was mainly happening up chain in organisations. This framing is even more prominent today. When we talk about identity management—who is it for? Most of the time, it's mainly for the organisation's efficiency goals, and to help them report to a donor. When tech reduces the burden of monitoring on humanitarian practitioners, staff and the time they spend with crisis-affected people also get eliminated.

Around 2015-16, the self-sovereign identity (SSI) movement grew more prominent, though it was always tangential to humanitarian work, a niche interest rather than mainstream. Some of us were drawn to SSI because it represented a strand of thinking around digital identity that put the vulnerable person in need of assistance at the centre. Part of the interest in SSI was exploring how to enable people to have more control over who has information about them. The concept of decentralised control over data was linked to the blockchain hype cycle. In my view, most SSI initiatives have died: they struggled to exist because they were not about organisational efficiency or fraud prevention. There's still a strong ethos within humanitarian organisations that everything needs to be centralised. SSI was about giving away power, so it has been pushed out.

Humanitarians often have 'shiny toy syndrome'.[43] Everyone loves technology—whether it's AI, blockchain, crypto, or simply smartphones. We want to be cutting edge. We care less about what the problem is than figuring out how to use the technology. One of the challenges throughout my career in humanitarian aid is this: when you focus on technology, you neglect technology governance. We need to learn how to work together collectively. That part is unsexy, time-

42 For reference, see Parker, B (2019) 'New UN deal with data mining firm Palantir raises protection concerns'. The New Humanitarian. https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

43 This argument is also made in: Scott-Smith, T. (2016). 'Humanitarian neophilia: the 'innovation turn' and its implications'. Third World Quarterly, 37(12), 2229–2251.

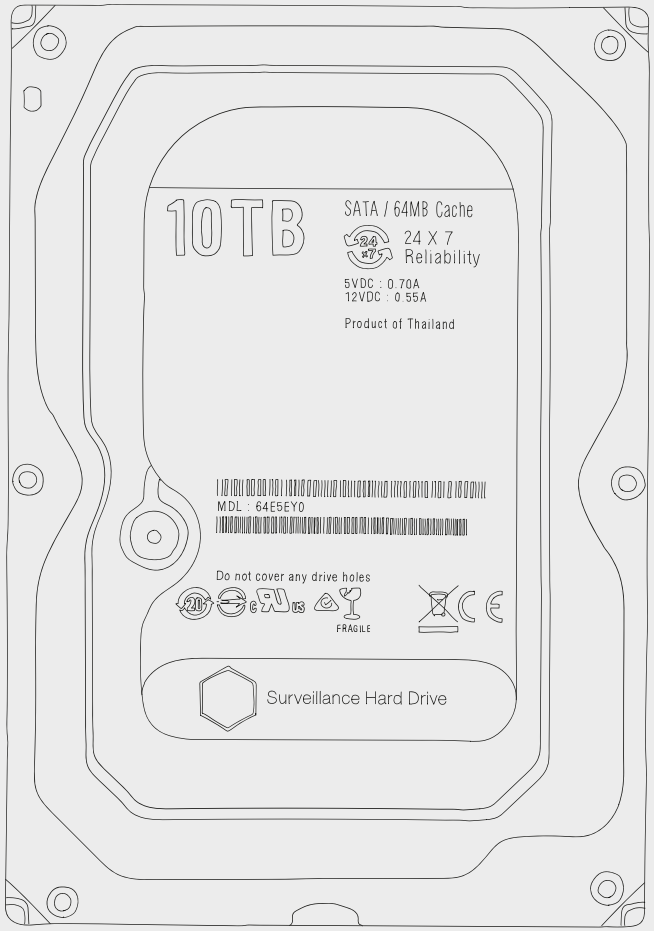
consuming, and it won't generate lovely marketing pitches, but it's what makes identification systems work. If we focus there, we'll have long-term gains. This industry operates on short-term thinking, whereas technology governance requires a longer timeframe. We have a proliferation of identity management solutions, which is precisely why we don't have strong governance principles and data sharing standards as an industry. We talk about improving the interoperability of our systems, but it quickly becomes about 'who's the biggest bully who will control the data everyone collects?' not 'how will we make collective decisions around what information gets shared?' Interoperability discussions rarely feature the role of the vulnerable person whom the data concerns.

Since the January 2025 funding crisis, humanitarian organisations have been circling their wagons, turning inwards and focusing on their own survival. This has been a period of power consolidation. Large organisations bid to have their solutions chosen as the shared system everyone uses, while refusing to share data with other smaller entities like NGOs. It is easy to talk about data standards and interoperability when you get to make the decisions and hold the power. This era of centralised data power will last a whilst yet, but it will inevitably implode. That's where my long-term optimism lies. To use an unusual analogy: consider farming and the rise of big agriculture in the US. Around 1900, you had small-scale local farms working closely with nature. World War II-era big agriculture destroyed the soil in the name of progress—progress being the god everyone still worships. But certain people, old farmers, kept doing things their own way. Families were laughed at or told they were backwards because they kept their soil alive, but regenerative agriculture was just how they did it. I see this as a fitting analogy for the humanitarian space. Big organisations may strive for power and control, but there are always pockets of people doing things differently, holding onto collective action and upholding humanitarian principles.

The precarity of the funding crisis is very difficult to navigate, but the primary principle going forward should be collective action, rooting our work in small local organisations that really know their communities. Our projects at the Collaborative Cash Delivery Network (CCD) around data stewardship build decision-making tools and resources for those people.[44] We've implemented in Ukraine and are working on Sudan and Gaza. In all organisations, there are excellent people genuinely interested in collective approaches. The Estonian Refugee Council, for example, has spent time developing tools that are all open source and low cost for any organisation to use. That's part of the challenge: technology sold as efficient comes with hooks like long-term dependency and costs, whether financial or human. Small organisations are the ones asking the crucial question: what's the appropriate technology for this project, context, or organisation? Sometimes the answer is a piece of paper or an Excel file. It doesn't make sense to invest heavily in shiny technology that will be obsolete in a few years or requires upgrades every six months.

One more forgotten aspect of identity management is language and translation. So much technology is written in English—from the code to the user interface—yet most humanitarian work occurs where English is a fourth or fifth language. We don't have all the answers yet, but we've been examining how to design through this issue, creating technology that can work in multiple languages, sensitive to different cultural naming conventions. The bottom line is identity management isn't reliant on technology: it's reliant on relationships. Without that relational piece, the conversation quickly becomes reduced to 'how do you know that everyone on the internet isn't a dog?'

44 See https://www.collaborativecash.org/.




*Melyn McKay*

# Rearranging Risk: From Institutional Compliance to Human Protection

*Dr Melyn McKay is a humanitarian consultant, anthropologist, and now runs the last-mile money platform Coala Pay. She is based in San Francisco, USA.*

Since its inception, international aid was overly centralised, sidelined local expertise, and often reinforced power imbalances. Throughout my career I've been concerned with removing structural barriers to localisation. I have worked with a range of people and contexts, but my starting point has always been a very ordinary yet deeply consequential problem: international organisations often cannot work effectively with local partners whose formal identity documents or bank account details do not line up neatly with institutional requirements. Most large organisations are structured around systems that only release funds if the entity name on a contract matches the name on a bank account. When that is not the case, everything stalls. Local organisations may be trusted, legally constituted, and deeply embedded in their communities, yet still lacking the kind of institutional identity credentials that international compliance frameworks expect.

Through my work with international NGOs, I eventually became immersed in household cash programming. I had little prior experience with it and was personally sceptical of the idea that vulnerability is best addressed at the level of the isolated individual—implying that struggle is a personal failing or that resilience is simply an individual trait rather than something rooted in community and shared infrastructures. But in humanitarian work, you often end up mitigating harm within systems that will move forward regardless of your personal views. I'd rather be in the room

shaping those processes than outside resisting to no effect. Cash programming has proven time and again to be one of the most effective and dignified means of supporting communities in crisis, even if such interventions alone likely cannot address the structural issues which ensure vulnerability persists.

The Coala Pay team has significant experience with cash and we have chronically encountered identity related obstacles: the necessity of deduplicating beneficiary lists, meeting KYC requirements, data sharing agreements that took half a year to negotiate, and deep anxieties about data ownership. In that context, we started to experiment with multi-signatory wallets[45] and due-diligence file structures that mirror the identity assurance normally created in the process of opening a bank account. The aim was simply to give compliance teams enough confidence to treat a digital wallet address as an institutional account, not to claim any technical glamour by association with blockchain. Out of this context, we also began developing solutions using a technology called 'data canisters'. This provided us with a practical way to manage beneficiary lists over multiple disbursement cycles. They are particularly compelling in the context of cash programming because they've allowed us to build a mechanism that organisations can use to coordinate without directly sharing personal data. Each organisation keeps full control of its own data, stored in an encrypted canister. If the data is formatted correctly, canisters can query one another. They identify overlaps or anomalies without exposing the underlying records. This avoids the need to pass spreadsheets around or negotiate burdensome data-sharing agreements that often outlast the programme itself. The model also allows a third canister to be introduced—for example, a sanctions or anti–money laundering database—so that datasets can be checked against external watchlists without centralising or revealing beneficiaries' personal information. At the same time, some elements of KYC can be embedded directly into smart contracts[46] in ways that reduce burdens on beneficiaries themselves.

Much of the work on decentralised digital identity is intellectually fascinating but not well matched to humanitarian field operations. There is a reason refugee ID cards persist despite endless assertions that better technologies exist. Adoption requires a degree of buy-in that is almost impossible to achieve if the shift demands heavy technical debt: new infrastructure, new workflows, or retraining thousands of staff. Tech culture often imagines change as going from zero to one hundred. But humanitarian systems exist within one- or two-year programme cycles, high turnover, bureaucratic inertia, and intense pressure to deliver quickly. If it takes six months simply to set up a new integration, the idea of rolling out a fully digital identity ecosystem in the lifespan of a single programme is laughable. Incrementalism, however unfashionable to technologists, is often the only viable approach. When I first worked with blockchain developers, they would often ask why we insisted on designing systems that mirrored existing workflows rather than adopting more 'efficient' designs. The answer is simple: you cannot uproot people from familiar tools in the middle of high-pressure environments. Humanitarian staff need systems that look and feel like what they already use; the innovation has to sit quietly in the background. We don't see this as a capitulation, but as a means of achieving genuinely sustainable changes in the way aid is delivered.

A recurring theme relating to digital identity is the different ways actors conceptualise risk. Local partners often think of risk in physical terms: who will be arrested, who will be threatened, whose door the military will knock on. International organisations tend to speak in actuarial terms: how identity data, financial records, or KYC compliance might expose them to audit issues, financial loss or reputational harm. These perspectives frequently collide. Years

45 Multi-signatory wallets require multiple authorised approvals (signatures) to access or transfer funds.

46 Smart contracts are digital agreements (for example, transaction protocols) on a blockchain that execute automatically when certain conditions are met.

ago, I wrote about this as 'subcontracting ethics':[47] the pattern where institutional bureaucracy pushes risk downwards onto those least protected and most exposed. During the 2021 coup in Myanmar, this tension became impossible to ignore. Local partners were clear that using the formal banking system would put them in direct danger, exposing KYC databases with identity details, official documents, contact information, financial profiles et cetera. The military was monitoring accounts and visiting people's homes, accusing them of financing terrorism despite the fact they were clearly humanitarian actors. Meanwhile, many international NGOs and UN agencies insisted they could not pay anyone unless strict KYC compliant banking formalities were met. This became untenable as local organisations' registrations expired and they refused to resubmit under the military regime for fear their activities would be constrained and politicised, with their staff and beneficiaries endangered. It took six months to find alternatives; six months in which people were operating under life-threatening conditions. That period radicalised my thinking about the need for alternative financial rails that minimise sensitive information. I had seen the same dynamic in Syria and South Sudan: regimes under sanctions capturing a portion of aid flows by controlling the banking system. In some cases, that capture can be thirty or forty per cent, later used to fund violence against civilians. When compared with that, the idea that diversion primarily occurs through beneficiary fraud—when a beneficiary receives a hundred dollars for basic household needs—is absurd.

This raises a central question: are our systems designed to protect people, or to protect institutions? A genuinely humanitarian approach would prioritise the former. In some contexts, heavy KYC requirements are disproportionate to the actual financial risk and significantly increase the physical risk. Yet these requirements persist because systems are designed around institutional self-protection rather than human protection. One thing blockchain has done—perhaps inadvertently—is force a more honest conversation about risk attribution. When funds are not held custodially by a bank or an NGO, the old habit of assigning blame to local partners becomes untenable. Everyone begins asking who actually carries responsibility. I have heard people insist that the financial service provider must be the one to 'hold the risk'—liability for compliance failures, accusations of weak controls or diversion, and so on—essentially because organisations want someone to point to if questioned by donors. On the other side, some crypto projects rush into high-risk contexts without understanding protection concerns at all, sometimes relaying stories of harm with extraordinary casualness. I have found myself repeatedly warning that just because something can be done technically does not mean it should be done ethically.

With the 2025 aid cuts, 20% of some organisations' budgets disappeared almost overnight. The cuts have left remaining staff struggling to meet unchanged compliance requirements with far fewer resources. Anything that reduces administrative burden becomes a form of triage. I am uneasy with the fetish for efficiency, but the reality now is that many organisations are trying to uphold their obligations with drastically reduced capacity. At the same time, there is a generation of technologists who build the structural foundations of our digital world through the logic of capital accumulation, without ever having engaged seriously with questions about ethics, power, or human experience. They optimise systems, making them more efficient without considering their social consequences. In the crypto space you see a split between those rooted in earlier, more politically aware traditions, and those who arrived later with a purely extractive mindset. I think there is a battle underway for the soul of blockchain, which could go either way. Tools like data canisters and alternative payment rails are not solutions in themselves; they are simply ways of rearranging risk. What matters is who governs them, who is protected through them, and whose safety is deprioritised. The challenge now is to build infrastructure that acknowledges the messy, political, human realities of the places it is meant to serve, rather than erasing them under the guise of innovation.

47 See M. McKay & A. de Carbonnel. (2016). 'Subcontracting Ethics: Mediating the commodification of 'local knowledge' in crisis and conflict' https://ora.ox.ac.uk/objects/uuid:20948a8c-03c2-43d1-b126-ccfafd4f311e/files/r44558f819.


*Sandra Hart*

# Grassroots Identification: Shifting Power from Institutions to Communities

*Sandra leads the Humanitarian Venture Lab at Mercy Corps Ventures. She is currently based in Bangkok, Thailand.*

For as long as I've worked in the humanitarian sector, my approach has been informed by my first degree in anthropology. I look to understand existing community relationships and cultural practices first rather than imposing solutions. Alternative value systems in the Pacific like shell or stone money inspired Unblocked Cash, Oxfam's blockchain-based cash transfer project which we launched in 2017. The project became an exercise in how to co-design technology with communities, and we scaled it up to several countries. I now work on the venture capital arm of Mercy Corps, which invests in local tech sectors, helping communities build technology on their own terms.

Identification is often the gateway to receiving humanitarian assistance, but it can also create serious vulnerabilities. Consider LGBT migrants in hostile countries, or Rohingya refugees facing persecution risks on-the-move between Bangladesh and safety in Malaysia. Exploitation of migrants is often linked to loss of control over identity documents. In all these cases, secure storage and selective disclosure of sensitive identity information is critical. These systems should serve a protective purpose combining the necessity of being selectively anonymous or pseudonymous. Identity management in humanitarian contexts isn't just about efficiency or fraud prevention; it can be a matter of life and death.

From around 2017, there was a real boom in self-sovereign, blockchain-based digital ID solutions for refugees and stateless people. Many of those initiatives emerged simply because everyone else was doing it, there was a fear of missing out. But often they were duplicating ID processes that were already there rather than improving identification pathways, and they were parallel solutions unnecessary in solving the problem of moving funds—mainstream cryptocurrencies already provided unique identifiers and allowed money to move transparently and safely across borders. Many of the sector's blockchain ID projects created organisation-specific ecosystems without broader integration in mainstream, recognised systems. They claimed to be decentralised and privacy-preserving, but they ironically relied on biometric verification, creating centralised, influential control points over identity data and potential privacy risks. That's a different approach than what was initially envisioned in terms of blockchain providing user control, portability across borders, and independence from any single authority.

This highlights how we need to better confront the hierarchies and inequities in how humanitarian resources are distributed, and which organisations have access to expertise and technology. The identity frameworks we design embed power relationships. When a single organisation controls both your identity and your access to resources, it reproduces the same power imbalances we claim to be addressing through humanitarian action. Some large international organisations have gained dominance because they have traditionally received the most funding, allowing them to concentrate control over digital identity systems. Large tech companies also have considerable influence that even exceeds governmental capacity in certain contexts. Humanitarian technology would benefit from being more open source rather than proprietary.

The real tech success stories aren't humanitarian organisation projects but grassroots ones. In Central America and the Caribbean, where there's lots of internal migration, it's not a coincidence that blockchain has caught on organically there; it's independent of jurisdictional financial infrastructure. People on the move choose crypto to remain invisible, exercising their right to be forgotten. That's the beauty of open decentralised systems, though they don't fit the traditional success-story-as-aid-industry-prototype narrative. We should acknowledge that if people are using crypto on their own, outside 'our' systems, we could support that instead of reinventing the wheel. Ultimately, whose agenda are we serving when we dismiss these alternative grassroots innovations? Fundamentally different perspectives exist on what constitutes a 'legitimate' digital identity or financial system. People living under oppressive governments may organically adopt non-traditional tools, supported by informal networks, ethnic groups, and civil society. Innovation doesn't have to be Global North led. Look at Bitcoin miners in Nigeria who've cobbled together their own servers, or locally developed blockchain applications in the Global South. We need to recognise that people do have cutting edge skills and capacities locally, rather than assume a paternalistic position.

I'm currently involved in a pilot project in Myanmar, where the 2021 military coup made it extremely dangerous for civil society to operate.[48] The military junta is clamping down on humanitarian actors, sometimes forcing them at gunpoint to provide information. They seize Know Your Customer (KYC) identity records from mobile money exchange bureaus and hand them over to the special police. The junta has also manipulated the exchange rate, exploding the stability of Myanmar's currency. The NGO[49] leading this pilot decided at the corporate level to institutionalise the use of stablecoins in exceptional environments where existing infrastructure isn't functioning. The NGO is not sending stablecoins directly to households but rather to civil society partners so they can continue implementing some of their programmes. We're working with a Myanmar-based financial technology company. Half the team is outside Myanmar, with the Burmese diaspora heavily involved. Crucially, they didn't need

48 The military coup in February 2021 overthrew Myanmar's democratically elected government, leading to ongoing conflict, humanitarian crisis, and persecution of civil society organisations.

49 Please note the NGO's name cannot be disclosed for security reasons.

us to teach them how to code or understand the differences between various stablecoins; the local tech founders already had that expertise.

The Myanmar pilot is low key, small in terms of money and participants, but proves stablecoins can work as an anonymous, discreet solution. The technical setup is deliberately incognito: the digital wallet serves as a unique identifier and transmits money to participants. Recipients receive an anonymous message via the encrypted messaging app Telegram. The message contains a code to log in that wouldn't mean anything to a stranger. They then open a disposable browser window where they create a wallet by logging into their social media account. The wallets are auto generated using Web3 authentication.[50] Recipients log in through Facebook—like single sign-on but for crypto. We're not sharing data with Facebook; we're just using the Facebook password as your PIN to verify it's the same individual accessing the wallet, using the unique sign-on to validate against another unique sign-on. This works well in Myanmar because Facebook is ubiquitous there, almost everyone already has an account, and they already know how to log in and use it. There's always a risk of phones being seized by the military. No app gets installed on the phone in case it's seized or an individual is tortured: the wallets are new each time and browser-based, so people can use it across multiple phones. Even if someone steals your device, your humanitarian funds remain secure because the value is stored on the blockchain, not on your phone itself. The passkey constantly changes so users don't have to remember it. This approach to identity management prioritises safety and deniability, which are principles that conventional humanitarian ID systems rarely incorporate.

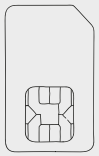
The pilot raises important questions about how the humanitarian sector could navigate mainstream versus alternative finance, and 'legitimate' versus 'illegitimate' systems. What happens when formal identity systems don't serve everyone equally? We need to address this question if we are serious about building a more equitable humanitarian system that remains accessible even in authoritarian contexts.

At its core, identity management is about agency and access. Who has the right to define and verify someone's identity? We need to ask what forms of identification people already have, which authorities support or accept those forms of ID, and how people can keep and share them securely. Can we deliver multi-profile wallets, so people manage their identity credentials themselves? Highly skilled migrants almost always have photo ID, so that app might work for them, but a one-size-fits-all approach never will. Identity systems that don't account for variations in access to root documentation can exclude the most vulnerable. One future use case I have identified is portable wallets for people in high-risk situations, such as pendular migrants, people who move back and forth across borders repeatedly. These people navigate precarious, transient conditions, the first to be excluded, climate-affected, or persecuted, and unlikely to have savings. Such vulnerable groups could have portable wallets that integrate stablecoin transactions, but also different ID layers. Like KYC 'tiers' in financial services, these could go from basic to fully verified identities. We could be programming humanitarian assistance that adapts according to the same migrant's identification needs and risks in different contexts. The core identity management challenge is creating systems that provide enough verification to ensure aid is accountable while prioritising and protecting beneficiaries' anonymity.

The current funding crisis in the aid sector demonstrates that now, more than ever, we cannot count on centralised systems. We cannot count on international systems. It's glaringly obvious that these legacies are unable to equip us for the future we all face. This is especially true when humanitarian organisations and solutions lack local grounding and a strong, vested, long-term interest in the context. That's a strong signal that decentralisation and localisation go hand-in-hand. If there is one big takeaway from my work, it's that emerging technologies like Web3 and AI have a role to play in

50 These are authentication standards for 'Web3', i.e. blockchain applications, that enable secure access without centralised credential storage, often using existing accounts (like Google or Facebook) to validate identity without sharing personal data. Web3 auth automates the process of creating your own wallet without having to deal with the keys directly.

accelerating localisation. Placing very powerful technologies in the hands of local players with the faith and trust that communities are agile, intelligent and resourceful enough to design and harness them to solve their own problems is essential, and doing so in a way that isn't owned or led by someone else is critical. Local organisations can do this far faster and at a fraction of the cost of what we've seen from various UN and INGO pilots. To me that is the only way forward: facilitate technological and digital access and pass on the power and choice to innovate. There simply isn't enough financing to do otherwise.



*Afterword by Bronwen Manby*

# Monopolies of Recognition? Governing Identity at Scale

*Bronwen is a leading authority on statelessness, comparative nationality law, and legal identity. She has worked closely with UNHCR on its global campaign against statelessness and has also advised the World Bank initiative on 'identification for development'. Bronwen is a Lecturer in international human rights law at the School of Advanced Study, University of London; a visiting senior fellow with the Department of International Development at the LSE; and Africa coordinator for the GLOBALCIT project of the European University Institute. She previously worked for the Open Society Foundations and Human Rights Watch.*

This anthology of 'reports from the field' of digital identity provides an immensely valuable album of snapshots of a rapidly changing landscape; looking back on the wave of innovations that came with the introduction of biometrics, and on the cusp of a new tsunami of potential changes proposed by the application of artificial intelligence.

On the one hand, these debates have always been the same: the tension between an identification system as itself a necessary 'technology' of any bureaucracy aiming to deliver services to a cohort of people too large to be known individually; and identification systems as mechanisms of surveillance and control. Digital and biometric identification systems fit into an old debate. On the other hand, we see how the new technologies are changing the very way that we think about identity. We are just at the beginning of understanding what the ability and need to prove uniqueness not only at a local or national but also at a global scale will do to humanitarian assistance—or anything else.

Many of the contributions focus on the utility of biometric identification both for the more dignified treatments of

beneficiaries of humanitarian assistance and for the agency's ability to verify that the intended people are receiving assistance (Steinacker; Mebur; Nallainathan). Others, however, point out that a focus on corruption among the intended beneficiaries is misplaced: of course, there will always be the need for measures to prevent this sort of abuse, but the major diversion of humanitarian assistance happens much higher up the literal and metaphorical food chain (Doornbos). They ask: does the focus on biometrics as an anticorruption measure expose the vulnerable to additional risks – such as misuse of their data—without impeding the truly corrupt? Risk management needs to focus on protection of the end user, as much as—or more than—of the agency distributing assistance (McKay).

Another familiar tension threads throughout many of the articles: that between linking humanitarian assistance into state-established 'foundational' identification systems and establishing agency-specific 'functional' databases for the intended recipients of specific types of assistance. States increasingly wish to assert sovereignty over identification and are suspicious of large-scale parallel systems (Steinacker; Nallainathan; Oliveros). There are also good reasons for refugees and other vulnerable groups to want inclusion into foundational identification systems to be able to access the benefits that are unlocked by possession of a state-issued identity token (Schimmel). But there are also risks, and beneficiaries may have much greater trust in a humanitarian agency than in their own government (Oliveros). It's also just easier in a crisis to stick with existing functional identity systems, rather than take on the substantial task of a carefully managed integration with a foundational system at the national level that does no harm to those registered. This in turn produces repeated multiplication of effort and risk, as every agency establishes a new biometric register (Schimmel).

A third theme is the new risks of technology created by the privatisation of identity registration and verification systems. Control is moving away from humanitarian agencies and even governments into private sector companies of very limited transparency and no tradition of adherence to ethical standards, hard to hold accountable in case of harm. There is a need to focus just as much on technology governance as on technology itself (Doornbos).

Finally, there is a hopeful strand, on the start-ups and pilot projects that have explored data-minimisation and user-control; context-specific, driven by local actors and priorities (Hart; Oliveros; Beech). But the question remains: much as these small-scale projects are important and perhaps signpost a better future trajectory in digital identity registration and verification, especially in humanitarian contexts, is it possible to envisage a patchwork of such systems that are sufficiently interoperable to move beyond the local, and sufficiently self-contained to protect the user? Overall, these authors are sceptical that tools such as self-sovereign ID and blockchain technology are the solution. Digital technology appears to have the characteristic of creating natural monopolies. Regulation of those monopolies will remain critical: and the only tool we have to do so will be the state—even if new norms at international level can establish some basic principles for the well-intended to follow. The challenge we face now is that the most important state for technology regulation is the USA.

Humanitarian aid is undergoing a profound transformation. As budgets shrink, institutions retreat, and digital systems take on ever greater responsibility, identity management has quietly become one of the defining infrastructures of contemporary humanitarianism. Aid and ID offers a timely, practitioner-led account of this transformation and its implications for the future of humanitarian action. Tracing historical shifts from paper records and indelible ink marks to biometrics and digital credentials, this collected volume reveals the political struggles embedded in the systems used to make crisis-affected groups legible. It asks whose interests these identification systems will serve as they persist long after the emergencies they were designed to address.

HAFAN BOOKS

Digital Sovereignty Observatory

Robert Bosch Stiftung