Forced Migration Review

Issue 73
May 2024

Digital disruption and displacement

Refugee Studies Centre
University of Oxford

Forced Migration Review

Forced Migration Review (FMR) brings together diverse, knowledgeable authors – especially those with lived experience – to foster practical learning and discussion that can improve outcomes for forcibly displaced people. Our free flagship magazine is accessible to a global audience in English, Arabic, French and Spanish, online and in print. Related audio/visual content is available online.

Forced Migration Review
Refugee Studies Centre
Oxford Department of International Development, University of Oxford,
3 Mansfield Road,
Oxford OX1 3TB, UK

fmr@qeh.ox.ac.uk

www.fmreview.org

ISSN 1460-9819

Magazine design: Hart Graphics (hartgraphics.co.uk)

Cover photo: Iris scanning. Malian refugee being registered with UNHCR during an out-of-camp registration exercise in Mauritania. Credit: UNHCR/Omar Doukali

From the **Editors**

Digital technologies are transforming our lives. Forcibly displaced people are using digital technologies in ways that inform and shape their migration and settlement in new places. At the same time, digital technologies are being used on (or against) forcibly displaced people in the public and humanitarian sectors.

'Digital technologies' in this issue refers to a range of technologies that together comprise digital systems and the hardware used to interact with those systems. Complex predictive modeling, geolocation tracking on mobile phones, biometric data use and dissemination, digital financial systems and the use of artificial intelligence in decision-making are among the digital technologies discussed. These diverse technologies span the range from promising to problematic. Often the impacts on forcibly displaced people are difficult to predict, and not easily classified as positive or negative.

In their foreword, UNHCR's Innovation and Digital Services team highlight the opportunities of digital technologies and the dangers of not acting to ensure forcibly displaced people have equitable access to these opportunities. Jessica Bither and Jassin Irscheid of The Robert Bosch Stiftung remind us that decisions being made today will shape the digital architecture that affects the safety, privacy and agency of people on the move – and ask whether we are adequately attending to that responsibility.

The authors in this issue discuss a range of digital technologies that are used by, or on, people experiencing forced displacement. Natalie Brinham and Ali Johar describe Jafar


Emily Arnold-Fernández


Catherine Meredith


Marie Godin


Derya Ozkul

Alam's experience of India's digital identity system, where a tool that promised new opportunities was repurposed to facilitate persecution. Kinan Alajak and his co-authors discuss a similar shift, as migrants find the mobile phones they use on their journeys are weaponised by governments to restrict asylum, while Abril Rios-Rivera uses research on CBP One to illuminate how digital dysfunction is used to curtail asylum access.

Other authors address the potential and necessity of digital technologies. Lala Zinkevych discusses the use of digital tools to enable critical service delivery, describing how three digital services have offered lifelines for displaced Ukrainians experiencing gender-based violence. Wala Mohammed describes the impact of digital exclusion on displaced people in South Sudan, while Saqib Sheik and Muhammad Noor discuss efforts to digitally preserve Rohingya cultural heritage in the context of large-scale displacement. Marie Godin and her co-authors describe how refugee-led organisations in Kenya have used digital platforms to create businesses and livelihoods, despite significant barriers.

Meanwhile, Nyi Nyi Kyaw complicates traditional power analyses around the use of digital technologies by describing how refugees in Thailand have used counter-surveillance, and asks whether this model could be replicated. Julia Camargo and Amanda Alencar challenge simplistic narratives about displaced people's understanding and opinion of biometric data collection, examining responses from displaced Venezuelans.

Power remains a central consideration in understanding how digital technologies are used, and by whom, in relation to forced migration. M Sanjeeb Hossain and his co-authors offer a nuanced exploration of the concept of consent in relation to the biometric data of Rohingya refugees. Francesca Palmiotto and Derya Ozkul examine the strategies and resources needed to challenge government use of automated systems in migration and refugee decision-making. Carolina Gottardo and her co-authors make a compelling case for human rights safeguards to mitigate the risks presented when digital technologies are used to facilitate alternatives to immigration detention, while Steffen Angenendt and Anne Koch remind us that politics may determine the impacts of migration forecasting.

The articles here illustrate that digital technologies are not deployed neutrally. In a world where participation in digital systems is unavoidable, making those systems as equitable, unbiased, and responsive to human needs as possible will help us respond to forced displacement in ways that yield improved outcomes and greater justice for forcibly displaced people. We hope this issue contributes to such efforts.

With best wishes,

Emily Arnold-Fernández (Managing Editor), **Catherine Meredith** (Deputy Editor), **Marie Godin** and **Derya Ozkul** (Expert Advisors for this issue)

Contents

We are grateful to the following donors: The Robert Bosch Stiftung, International Labour Organization (ILO) and UN High Commissioner for Refugees (UNHCR) for this issue; and UNHCR, Swiss Federal Department of Foreign Affairs, ADRA International, Danish Refugee Council and Women's Refugee Commission, who fund FMR's ongoing work to support better policies and practices globally by providing inclusive, insightful information and analysis on forced migration.

We would also like to thank all our **contributing authors**; our **expert advisors** for this issue Marie Godin and Derya Ozkul; our **reviewers** Emre Eren Korkmaz, Richard Williams, and from UNHCR, Nicholas Oakeshott, John Warnes and colleagues; and our **author mentors** Yu Furukawa and Amanda Wells.

Navigating digital opportunities and risks

Foreword by **UNHCR Innovation and Digital Services**

More than ever before, digital technology is integral to the lives of forcibly displaced people and the humanitarian systems they interact with. The connected society has the potential to improve the day-to-day lives of millions of people on the move. Ensuring that access to this technology develops equally, and that both the benefits and risks in its use are considered carefully, involves complex challenges.

In this context, UNHCR developed its Digital Transformation Strategy 2022-2026,[1] which highlights the transformative ways that digital technology can positively impact the lives of refugees and the work of UNHCR. It provides a framework for how UNHCR will approach the opportunities and risks of technology – such as online hate-speech, disinformation, misinformation, fraud and scams – now and in the future. An equal priority is further strengthening UNHCR's capacity to use digital technology in line with emerging ethical and protection standards, alongside engaging with governments and the private sector to promote the realisation of core protection principles in digital technology use in high-risk contexts, such as border control.

UNHCR has also been working with partners to advance the opportunities available to refugees in the digital economy, balancing safe and equal access with emerging digital risks, through a project funded through the PROSPECTS partnership.[2] While integration into the digital economy can prove highly advantageous, substantial efforts must be made to minimise risk and promote better labour standards for the wider benefits to be realised. We are glad to see such debates unfold in this issue of Forced Migration Review.

Economic, legal and social barriers can prevent forcibly displaced populations from benefiting from digital technology, and we are committed to developing holistic approaches to address those barriers. Efforts such as Connectivity for Refugees[3] – a multi-stakeholder initiative looking to advance the connectivity of over 20 million forcibly displaced people and the communities that host them by 2030 – are paying dividends and gathering increasing interest from governments and private sector service providers alike.

As with any emerging field of study, a wide variety of different perspectives are at play. UNHCR is committed to continuing to cultivate inclusive, evidence-based debates, recognising the importance of engaging in critical discussions with academia, fellow practitioners and – most importantly – the communities we work with and for.

We hope that the constellation of actors involved in the evolution of digital technology in humanitarianism will have more and more opportunities to discuss, to disagree and to connect and move together towards action that makes a difference in the lives of forcibly displaced people.

UNHCR Innovation and Digital Services
X: @UNHCRInnovation
linkedin.com/company/unhcr/

1. *www.unhcr.org/digitalstrategy/*
2. *For more information on PROSPECTS go to www.unhcr.org/innovation/prospects/*
3. *For more information go to www.refugeeconnectivity.org*

Building a responsible digital infrastructure

Foreword by **Jessica Bither and Jassin Irscheid**

Digital technologies are transforming the way human mobility is experienced and managed across borders. This issue offers insights into the different ways in which technologies are changing displacement-related settings around the world: from predictive modelling to anticipate climate-induced migration, biometric data collection in humanitarian operations and asylum seekers' experiences using the CBP One app in Mexico, to the use of mobile phone data by the Dutch and German authorities, and opportunities and challenges presented by the digital platform economy. These examples illustrate the often ambivalent nature of technology and the importance of context and nuance in understanding their implications.

We are at a crossroads. Choices regarding the values and safeguards we build into emerging digital architecture are being made now. The way human mobility is integrated in emerging technology regulation, such as the regulation of AI (artificial intelligence) or DPI (digital public infrastructure), will determine how we manage important risks related to issues of security, privacy and democratic oversight. There is also the potential for algorithmic bias or for enshrining existing inequalities, racism, and other forms of structural discrimination through automated systems.

If designed responsibly, digital infrastructure for human mobility could lay the groundwork for a system better attuned to the displacement and migration realties of today, and offer the backbone for more flexible and adaptable tools that can respond quickly to changing rules and demands. For example, digitalising visa processes could make it easier to incorporate new requirements, respond to changes in labour demands, or adapt to sudden disasters or crises.

At The Robert Bosch Stiftung, we focus on digital technologies and migration as one of our core issue areas and we work closely with key stakeholders and partners towards answering the question: How can we use digital technologies responsibly in the areas of migration and displacement? The answer must necessarily include identifying red lines where the risks are simply too great, being clear about what the purpose or motivation behind the deployment and use of digital technologies is, and critically assessing who makes the decisions about the rules that govern them. It also means seeing digital disruption as a way to transform old ways of thinking or outdated approaches that are no longer fit for purpose in managing human mobility in today's rapidly changing world.

We hope that this issue is another step in building a community to critically engage with these important questions, and to get closer to answering what a responsible and human-centred approach to digital technologies in migration or displacement settings should – and could – look like in practice.

Jessica Bither,
Senior Expert for Tech and Migration
Jassin Irscheid,
Project Manager for Migration
The Robert Bosch Stiftung GmbH,
Berlin, Germany

Refugee experiences of identity documents and digitisation in India and Myanmar

By **Natalie Brinham** and **Ali Johar**[1]

Drawing on the authors' joint activism on the rights of refugees and stateless people in India and Myanmar, this article considers how digital ID systems can be used to exclude minorities.

India's e-ID system has been hailed for increasing social inclusion and bureaucratic efficiency. Whilst it has brought benefits to many in India, refugee experiences reveal a darker side of digitisation. Combined with increasingly hostile registration and surveillance procedures for noncitizens, refugees suffer economic and social exclusion, harassment and human rights violations.

Myanmar has attempted to digitise its own ID system and has piloted technologies[2] from China, India and elsewhere in the midst of forced displacement and conflict. Myanmar's latest efforts to implement an e-ID system reportedly include further cooperation with the Indian Government. Myanmar's military regime already uses identity documents to reinforce systems of surveillance, control and persecution. There is a real risk that if Myanmar were to fully adopt a digital ID system, the rights of minority and opposition groups would be further curtailed.

One refugee's experience of ID systems in India

For Jafar Alam,[3] a Myanmar refugee in India, the Aadhaar card or Indian e-ID card does not only store biometric data, it also represents past hopes, current insecurities, and fears for the future. Born to stateless Rohingya parents in Rakhine State Myanmar in 1995, Jafar was denied Myanmar citizenship.[4] When he and his family fled the anti-Muslim violence in 2012, along with 140,000 others, the only papers that proved his family's residency in the country were destroyed in an arson attack.

At the time they arrived in Bangladesh, there was no refugee registration[5] available. Support for arrivals was ad-hoc and arrests frequent. The family struggled to make ends meet. In this context, Jafar and his older brother made the difficult decision to take the risky onward journey to India without documents.

Refugee registration was slow in India, but despite his lack of legal status, Jafar was able to find a small shelter to share and found work in the informal economy. After a year he was issued with a UNHCR ID card, which offered him limited protection from arrest and access to some basic services including cheaper healthcare. It also enabled him to register for a SIM card, reconnecting him with the world of knowledge and his scattered ethnic community.

Using his UNHCR card as proof of his status, Jafar was able to apply for a Long Term Visa (LTV), which he received in 2014. In turn, the LTV entitled him to a state-of-the-art e-ID card, or Aadhaar, issued to all residents in 2016. The Aadhaar stores an individual's biometric and demographic information and provides a unique 12-digit number that links all personal data. The Aadhaar card

A Rohingya refugee couple looking at their child's half-burned books after their camp, consisting of 55 families in Delhi, was entirely burned for the second time in a tragic fire incident in June 2021. Credit: Ali Johar

was hailed as a tool of social inclusion,[6] reducing the need for paperwork, increasing bureaucratic efficiency, and providing better access to welfare and services. For Jafar Alam, things were looking up. One of the first things he used his Aadhaar card for, was to open a bank account. This made it easier to get work and to receive and send money to family members. Best of all, the Aadhaar card allowed him to enrol in school.[7]

How digital IDs in India facilitated the exclusion and persecution of refugees

The context in India swiftly changed when, in August 2017, the Baratiya Janata Parti (BJP) government announced that Rohingya refugees were now considered 'illegal' and were to be deported to Myanmar. LTVs and Aadhaars were no longer issued to refugees; it became harder for them to access essential services, and they became more vulnerable[8] to harassment, arrest and detention. Eleven days after the announcement, the military in Myanmar launched the brutal 'clearance operations' against Rohingyas, sending almost a million people fleeing into Bangladesh. Rohingyas in India were at risk of *refoulement* (being forcibly returned) to a situation of genocide.[9]

Biometric and demographic data was not just stored on the Aadhaar system, but also included in a database of 'illegal immigrants.' In the same year – 2017 – the police in India conducted a 'verification and registration' exercise in Jafar Alam's refugee camp. He was arrested along with fourteen other refugees. The police claimed he had 'illegally obtained' the Aadhaar and charged him. The document that he had once been entitled to had landed him in prison. He served a one-year sentence. Jafar Alam was one of the lucky ones who was able to secure release at the end of his sentence. According to the community-based organisation Rohingya Human Rights Initiative,[10] there are currently at least 776 Myanmar refugees stuck in indefinite detention in India.

When Jafar Alam was released his life had changed. The Aadhaar card had been frozen. He could no longer continue his education. Mobile phone network providers now

required an Aadhaar for SIM registration. Aadhaar had become a mandatory document to receive remittance, so he and his fellow refugees could no longer receive financial support from family or friends. His UNHCR card offered less and less protection from arrest in an increasingly hostile environment.[11] Seen under the law as merely proof of residence, Aadhaar cards had unofficially become a single access point for almost all services including education, financial services, driving licences, SIM cards, passports, subsidies and utilities including gas, water and electricity. In 2018, the Indian Supreme Court ruled[12] that private entities could not compel their customers to provide Aadhaar cards to access services. However, this is not the way it works in reality. As refugees in India know, the same digital identity management system that first promised social inclusion, has now resulted in the further marginalisation of refugees and other disenfranchised groups.

Now Jafar Alam constantly fears being arrested again, or worse, being deported back to Myanmar. Following the military coup in Myanmar in 2021, his hometown has been engulfed by fighting between the Myanmar military and the Arakan Army (a predominantly Buddhist Rakhine group fighting for self-determination). Since 2017, the Indian government has deported an unknown number of Rohingya refugees to Myanmar, 18 of which have been documented and followed by Rohingya Human Rights Initiative. Some were detained in Myanmar on arrival, some separated from family, some fled again.

The current ID system in Myanmar and surveillance by the military regime

The Indian Government issued Jafar Alam a registration form in Burmese titled 'Verification of Illegals from Myanmar.' It asked for information about his relatives in Myanmar, which he worries may lead to them being targeted. Data from the 18 deported Rohingyas was shared with the Myanmar authorities, according to the Rohingya Human Rights Initiative. Deportees were issued with Myanmar's National Verification Card (NVC) on return. This card registers Rohingyas as non-citizens in Myanmar who need to have their nationality verified. The ID system in Myanmar[13] has long held in place systems of surveillance, persecution and segregation.

Since the military coup of 2021 in Myanmar, civil conflict has spread throughout the country. Registration and ID systems have been further weaponised by the military[14] against the opposition and minorities from the conflict zones. Used in tandem with check points and other surveillance infrastructure, movement restrictions have been put in place that make securing an income or fleeing to safety more difficult. The current ID system's inefficiencies have their benefits[15] for members of the opposition. Many are still able to circumvent military surveillance to operate within the country or flee to safety. The military, acutely aware of their weakness in this area, has been piloting[16] the use of biometrics on the displaced, the stateless and the opposition.

Myanmar's attempts to digitise registration data and effectively utilise biometrics requires foreign investment and technical support. Plans to secure foreign support have been stalled by both the genocidal violence of 2017 and civil conflict following the military coup of 2021. The latter led to sanctions, the pulling out of foreign investors and a diversion of development funding away from state actors. As the support of international lenders and tech companies has waned, the regime has increasingly turned to India, China[17] and Israel. For Jafar Alam, and other refugees who have experienced how digital

ID systems can increase the capacity of governments to exclude and make survival in the margins so much harder, concerns about how Myanmar's authorities may misuse identification technologies run very deep.

The potential for misuse of digital ID technologies in Myanmar

Digitising and upgrading ID systems is often viewed as an essential prerequisite for large economic and human development projects, for example the World Bank Group's ID4D programme.[18] They are also seen as essential in preventing statelessness.[19] Digitised systems supposedly immunise societies against the problems associated with paper-based and non-centralised systems such as loss and destruction of documents. However, digital systems can also exacerbate the power differentials between individuals and state authorities. Where state authorities become perpetrators, these technologies can become effective weapons against dissidents and minorities. For Jafar Alam's family whose paper documents were destroyed, even digital records will not protect them against administrative violence as long as the systems remain under the control of Myanmar's militarised state.

Promoters of digital identification systems have sometimes used India's Aadhaar system as an example of good practice. IDs issued on the basis of residency rather than citizenship theoretically circumvent issues relating to the exclusion of non-citizens. Yet, the experiences of refugees and stateless people in India shows that digital ID systems based on residency can also effectively endorse and exacerbate endemic structures of discrimination and exclusion by 'locking in' an irregular legal status[20] and 'locking out' marginalised groups from socio-economic spheres and welfare systems.

Digital ID systems, when utilised together with other border-control technologies, have links to forced migration – both causing and prolonging displacement. The 'four cuts strategy'[21] which has been deployed by the Myanmar military since the 1960s against opposition and minorities, aims to cut off food, funds, information and recruits. The paper-based ID system was used to kerb freedom of movement and segregate Rohingyas. This became a method to cut off access[22] to food, income, funds and humanitarian aid; and to block international access and the flow of information about atrocities.

Digitised ID systems that provide a single access point for utilities and services could hold in place surveillance regimes that prevent opponents of the military regime from operating underground or even from fleeing the country; they could be deployed to facilitate the stripping of nationality[23] and rights. As the Rohingya people have experienced, if you are denied a legal identity, you can more easily be stripped of your right of return. This can lead to protracted displacement and a lack of access to durable solutions. Without a legal ID, and increasingly enclosed by a system of digital borders, moving in search of security can become more expensive and more risky.[24]

Rohingya communities have resisted coercive and oppressive state identification practices that recategorise them as foreigners, utilising civil disobedience practices during the 2014 census and the roll out of National Verification Cards[25] (NVCs). While western governments and international organisations including the UN and World Bank Group have limited their engagement with Myanmar on these issues, statist and corporate interests continue to drive the transfer of oppressive technologies into the military's hands.

Conclusion

The digitisation of ID systems presents a mixture of protections and risks for both refugees and those at risk of statelessness and forced displacement. Biometrics and digital registration for refugees can improve the efficiency of services and aid delivery. Technologies can potentially improve access to refugee protections via a trusted system that can help authorities and service providers to easily identify the protection needs of individuals. However, refugees also need to trust that their data is safe[26] and that e-IDs lead to protections, not risks. In a climate that is increasingly hostile to refugees, digitisation further locks refugees out of economic and social spheres, and locks in their irregular status leading to more vulnerabilities and risks.

In the wrong hands, digitisation of registries and ID systems can consolidate the power of states to disenfranchise minorities and produce statelessness.[27] But, in the right hands, the digitisation of national ID systems and registries can serve to bolster social protections on multiple levels for marginalised groups, not least for those at risk of statelessness including returning IDPs and refugees.

Paper documents are easily lost or destroyed and non-digitised systems can be inefficient and prone to inaccuracies leading to greater challenges for those with precarious legal status in proving their identity, place of origin, family relationships, right to nationality and residency, and land ownership. Less than 20% of Myanmar's territory is under effective administrative control[28] of the military regime. The rest is increasingly governed by non-state administrations run by ethnic and political opposition. These groups control cross-border movement of goods and people, customs, taxation, land use and more. ID technologies could potentially be put to use or repurposed by forward thinking non-state administrations to provide proof of residency, birth place, citizenship, land rights and future-proof access to welfare schemes and rights.

Natalie Brinham
ESRC Postdoctoral Fellow,
University of Bristol
natalie.brinham@gmail.com
X: @natbrinham

Ali Johar
Refugee Fellow, Refugees International
alijohar20@gmail.com
X: @mtsjohar

1. *With thanks to the Rohingya Human Rights Initiative and the Institute on Statelessness and Inclusion. The work of Rohingya Human Rights Initiative has been integral to the co-authors research and work. Much of our work that has informed this article has been supported by The Institute on Statelessness and Inclusion. Natalie Brinham's current research is supported by the Economic and Social Research Council (ESRC).*
2. *bit.ly/digital-repression-Myanmar-2023*
3. *Not his real name. Name and other details have been changed to protect his identity.*
4. *bit.ly/institutesi-navigating-faulty-map*
5. *bit.ly/guardian-burma-rohingya-refugees-bangladesh*
6. *bit.ly/aadhaar-scheme-promise-inclusive-social-protection*
7. *bit.ly/rohingyas-struggle-schooling-india*
8. *bit.ly/fire-rohingya-camp-exposing-indias-refugee-policies*
9. *bit.ly/rohingya-genocide*
10. *www.rohringya.org/about-us.html*
11. *bit.ly/institutesi-rohingya-refugees-india*
12. *bit.ly/constitutionality-aadhaar-act-judgment*
13. *bit.ly/rohingyas-dangerous-encounters-papers-cards*
14. *bit.ly/institutesi-citizenship-without-consent-myanmar*
15. *bit.ly/myanmar-juntas-census-heralds-totalitarian-nightmare*
16. *bit.ly/myanmars-biometric-data-collection-rights-violation-fears*
17. *bit.ly/myanmars-census-witch-hunt*
18. *https://id4d.worldbank.org/about-us*
19. *bit.ly/digital-id-help-stateless-people*
20. *bit.ly/institutesi-locked-in-locked-out-rohingya*
21. *bit.ly/militarys-four-cuts-human-rights-myanmar*
22. *bit.ly/genocide-attrition*
23. *bit.ly/citizenship-stripping-myanmar*
24. *bit.ly/surviving-statelessness-trafficking-rohingya*
25. *bit.ly/rohingya-refugees-resisting-id-cards*
26. *bit.ly/rohingya-ids-deny-citizenship*
27. *bit.ly/india-citizenship-list-assam*
28. *bit.ly/situation-maps-burma*

The dangers and limitations of mobile phone screening in asylum processes

By **Kinan Alajak, Derya Ozkul, Koen Leurs, Rianne Dekker** and **Albert Ali Salah**

European authorities are increasingly screening asylum seekers' phones at the cost of their fundamental rights. In this piece, we suggest a procedural shift – prioritising fairness in the asylum procedure and voluntary cooperation towards purposeful goals.[1]

Asylum seekers use mobile phones for various purposes, including staying connected with their loved ones, planning their journeys, navigating travel routes, and securing housing and jobs. However, the dependence on mobile technology has also made asylum seekers particularly vulnerable to government surveillance, as their devices hold information about their movements and activities. European authorities are increasingly using data from mobile phones to gather evidence that can be used in decisions over asylum claims and, in some countries, to collect intelligence on migration-related crime and terrorism.

The practice of mobile phone screening has been severely criticised by civil society groups, including Gesellschaft für Freiheitsrechte[2] and Privacy International.[3] They argue that the practice is unlawful, invades privacy and lacks meaningful consent and safeguards to justify its necessity and proportionality. Moreover, the lack of transparency around data processing, the digital forensics software and the workings of algorithms used during the process could potentially undermine the fairness of the asylum procedure.

Despite these criticisms, several European countries persist in screening the mobile phones of asylum seekers. According to the European Migration Network's 2017 report,[4] mobile phone screening was standard practice in the Netherlands and Estonia, and optional in Croatia, Germany, Lithuania and Norway. In Latvia and Luxembourg, mobile phones were confiscated in the context of criminal procedures. Research[5] shows that data analysis of mobile phone content has been implemented in the Netherlands, Germany, Norway, and, to some extent, Denmark and the UK. Belgium, Austria and Switzerland have also amended their laws to permit such practices.

In this article, we compare findings from two similar studies conducted between 2021 and 2023 on the prevalence of mobile phone screening in Germany and the Netherlands.[6] The research team in the Netherlands filed Freedom of Information requests with the asylum authority *Immigratie en Naturalisatie Dienst* (IND) and the border police *Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel* (AVIM). They interviewed 13 state actors, civil society representatives, policy officers and law practitioners. In Germany, Derya Ozkul submitted several Freedom of Information requests to the Federal Office for Migration and Refugees - *Bundesamt für Migration und Flüchtlinge* (BAMF). Both studies also included interviews with individuals who underwent the asylum procedure. The team in the Netherlands interviewed seven individuals from Syria and Turkey, while the team in Germany interviewed eleven asylum seekers and refugees from Syria and Afghanistan. After providing a brief account of the screening practices in Germany and

the Netherlands, we argue that a number of flawed assumptions are being made based on 'data doubles' (profiles of individuals constructed from aggregated digital data) and discuss asylum seekers' reactions to the use of screening technology.

Mobile phone screening in Germany and the Netherlands

Immigration and border authorities in Germany and the Netherlands use mobile phone screening to identify asylum seekers and establish their country of origin. As part of this process, government officials confiscate the asylum seekers' mobile phones and other digital devices and either manually browse or automatically extract, analyse and use data from the phones during asylum assessments.

During our fieldwork, we found that both countries rely on private companies to provide them with hardware and software, support and maintenance. German authorities rely on Atos, a digital transformation-focused IT company that integrates products and services from two mobile forensic firms, MSAB and T3K-Forensics, to read and analyse data from electronic devices. In the Netherlands, the police produced their own software to automate data analysis, relying on companies like Cellebrite, an Israeli digital intelligence company, to supply the hardware (e.g., Universal Forensic Extraction Device "UFED") and software which extracts the data prior to analysis.

Despite many similarities in the practice, there are also some important differences. In Germany, the identification process is conducted as part of the asylum procedure, while in the Netherlands, it is conducted before an asylum application could be initiated. Therefore, in Germany, the analysis of phone data was the responsibility of the asylum authority, BAMF. In the Netherlands, however, the analysis of phone data was the responsibility of the border police (AVIM), not the asylum authority (IND).

The governing laws also differ. In the Netherlands, phone screening is covered under the Aliens Act 2000. Under this law, all adult asylum seekers are obliged to cooperate in a luggage search, a process which includes data carriers (including mobile phones and other digital devices). In contrast, in Germany, it is covered under the Asylum Act, and only those who do not have a valid passport or passport substitute are obliged to present their data carriers.

In the Netherlands, the main objectives of screening digital devices are to verify identities and collect signals related to national security. Therefore, information from the processing of data carriers could not be used by immigration authorities to verify asylum seekers' claims. Verification of someone's asylum claim was only recently proposed by parliament as an additional purpose, which would make smartphone screening part of the asylum procedure by the IND as well. In Germany, as the processing is part of the asylum procedure, the information obtained can be used more extensively in assessing asylum claims.

Common findings: mobile phone screening in practice

Mobile phone screening, as it is currently practised, violates fundamental human rights like those protected by Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the Charter of the Fundamental Rights of the European Union, as well as Article 8 of the Convention. Yet, state authorities are permitted to carry out similar invasive practices under the same laws in the name of national security.

In both Germany and the Netherlands, the primary stated objectives of mobile

phone screening are verifying identities and registering asylum seekers. In the Netherlands, it is also stated to be directly related to safeguarding national security. When asylum seekers in both countries were asked about their opinion of mobile phone screening, most of them agreed with the objectives pursued by the state authorities. In the Netherlands, they were specifically concerned about war criminals receiving protection rather than facing justice for the atrocities they committed in their country of origin. In Germany, not all participants raised concerns about the practice, but none believed the process was the best way to achieve these objectives.

Our fieldwork identified several issues that indicate that mobile phone screening is an ineffective means of realising the stated objectives. This includes technical issues due to the data being unusable, limited or contaminated, and the risk that flawed assumptions will be made about individuals on the basis of the aggregated digital data about them. Asylum seekers have followed various tactics to avoid the invasion of their privacy and safeguard their rights.

Unusable, limited or contaminated data

In Germany,[7] only some of the extracted mobile phone data was found to be usable. Around a quarter of the readouts (23% in the first quarter of 2019 and 26% in 2018) failed on the technical level. Among the successful readouts, more than the majority (55% in the first quarter of 2019 and 64% in 2018) contained no useful findings. Out of those phones with usable data, only 1% of reports (i.e., only 12 cases) contradicted asylum seekers' submissions In the Netherlands, no technical failures were reported, but collecting intelligence for national security purposes, specifically to identify suspects of terrorism, did not yield any matches. In addition, the Dutch Council of State[8] advised that the law should more clearly define which purposes smartphone data can be used for and how long the data can be retained for, as smartphones contain large amounts of data, including personally sensitive data.

Besides technical failures, the effectiveness of mobile phone screening is naturally dependent on the availability of data. Limited data availability can occur when a mobile phone has been inactive for an extended period or when it has only been used briefly. This can be because asylum seekers are often afraid of the authorities and may choose to buy a new phone before facing them. This was observed among several of our interviewees in both countries.

For example, one respondent in the Netherlands, a 29-year-old Syrian female, shared:

> *"Honestly, people know that they do this, so they don't take their personal phones, you know. They take new phones like a fresh phone because I don't like other people to have access to my personal data in this way."*

Another respondent in Germany, a Syrian female in her 20s, shared that she bought a new phone before registration for asylum because she "did not trust that they would be spying on her and her private conversations and pictures". She only wanted "to get done with this [process] and decided to pay for another phone".

Moreover, mobile phone data itself may be contaminated. This may occur because multiple individuals use a single device, or an individual may use a second-hand device. Many asylum seekers we spoke to in Germany and the Netherlands used second-hand mobile phones and expressed their concerns about possible findings from previous owners of their mobile phones and

the risk of their asylum application being rejected as a result.

One respondent in the Netherlands explained:

> *"Maybe the phone you get is an old phone of – I don't know – someone committed war crimes. So, you are getting that, and now you are coming with that to the Netherlands. That would be a problem."*

In these cases, contaminated data can wrongly elicit authorities' suspicion towards applicants. In the Netherlands, applicants can be questioned in relation to national security, which may lead to them being denied the opportunity to make an asylum claim. Even if further investigation does not lead to denial, it is likely that the asylum procedure will be stalled. In Germany, applicants can be questioned further in the context of asylum processing. Unfortunately, identifying contamination in digital forensics remains a challenging task, which means applicants may be questioned unnecessarily, further hindering the fairness of the asylum procedure.

Misinterpretation of data contents

In cases where the available data is usable and not contaminated, the screening remains susceptible to the risk of state authorities' misinterpretation. For example, state authorities may challenge someone's stated country of origin because their mobile phone data shows the person had frequently called numbers in a different country, disregarding that the person may have several reasons for doing so. For instance, asylum seekers whose phone calls are inconsistent could have their family members residing in a different location than the stated country of origin.

A more problematic example is when state authorities disregard the cultural context and misinterpret the contents. For example, the existence of photos of weapons can lead to the person being associated with crime, whereas, as one of our participants explained: "in some places, pictures of weapons are considered a way of indicating someone's status." As such, misinterpretation can result when the dataset is taken out of context and used as a proxy to stand in for an asylum applicant's life story. This risk is exacerbated when smartphone data are extracted and analysed automatically without human intervention. The automation is part of the problem, but specifically the underlying biases embedded in the system warrant scrutiny.

In the absence of official information about mobile phone screening, asylum seekers take initiatives to safeguard themselves from potential accusations stemming from systematic biases, as another respondent, a 28-Syrian male, told us:

> *"When someone told me that they took our phones, the only alarming thing was to check my 1,000 friends on Facebook to check for any contact that could be, I don't know, it could be weird for them. Like, there are people, sometimes they change their photo to look manly, you know, like from the Middle East, and so… those I deleted. I didn't want to have any problem."*

Reacting to the perceived racial biases by authorities, our respondent deleted all his 'Middle-Eastern' looking friends with beards who 'looked manly'. However, these reactions may raise state authorities' suspicion of asylum seekers even further.

Misinterpretation during the processing of data carriers can also have unintended consequences on asylum claims. Authorities can doubt an applicant's claims if their phone data contradicts or does not provide enough evidence to support their statements. As an

example, an asylum seeker may be denied their application in Germany if their claim is related to being a member of the LGBTQ+ community and their phone data fails to provide sufficient proof. However, in certain countries such as Iran, Syria and Russia, Grindr, a popular gay dating app, is prohibited by law. Additionally, the cultural context plays a significant role. As one of our participants explained, in some countries, "people didn't dare to download Grindr or to keep personal, intimate photos on their phones" in fear of prosecution. In such cases, authorities may conclude, based on the absence of such apps or materials in the smartphone data, that there is insufficient evidence to grant asylum based on the person's LGBTQ+ status.

Conclusion

We have discussed the practice of mobile phone screening and showed that current procedures may undermine its effectiveness and legality. The practice assumes that a person's online activities can be used to verify their identity and support their claims without taking into account cultural context and technical limitations. Furthermore, mobile phone screening may violate asylum seekers' rights to privacy, protection of personal data, and a fair asylum procedure. We have also discussed asylum seekers' tactics to halt the practice and protect their privacy. Given the limitations to this practice, it is crucial to question why it is still being carried out. Future research should focus on evaluating whether the potential risks associated with phone screening and the stress it causes applicants are worth the cause, and whether upholding the 'human in the loop' principle which ensures data is interpreted by humans in its specific context may be a sufficient condition for mitigating systematic biases embedded in algorithmic decision making.

We propose a shift towards the voluntary provision of mobile phones to asylum authorities only if applicants deem them useful in support of their claim. This approach would respect their fundamental rights and ensure they are not subjected to unnecessary scrutiny.

Kinan Alajak
Research Assistant, Department of Media and Culture Studies, Utrecht University
k.alajak@uu.nl X: @KinanAlajak

Derya Ozkul
Assistant Professor, Department of Sociology, University of Warwick
derya.ozkul@warwick.ac.uk
X: @DeryaOzkul

Koen Leurs
Associate Professor, Department of Media and Culture Studies, Utrecht University
k.h.a.leurs@uu.nl X: @koenleurs

Rianne Dekker
Assistant Professor, School of Governance, Utrecht University
*r.dekker1@uu.nl X: @RianneDekker_*

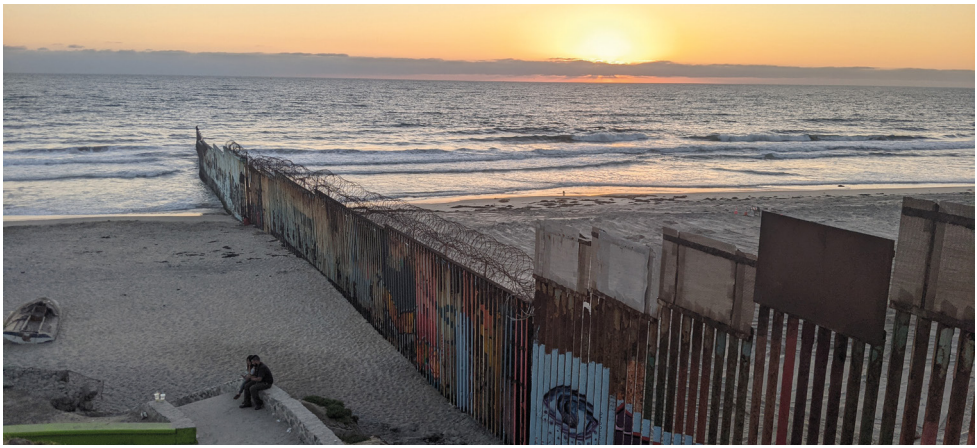
Albert Ali Salah
Professor, Department of Information and Computing Sciences, Utrecht University
a.a.salah@uu.nl X: @SzassTam

1. *We are grateful for the work of Maarten Bolhuis, Evelien Brouwer and Mirjam Twigt whose scholarship informed this review. The findings cited in this piece have been gathered in the context of the Algorithmic Fairness and Asylum Seekers and Refugees Project funded by the Volkswagen Foundation and the Co-Designing a Fair Digital Asylum Procedure project funded by COMMIT and the Universities of the Netherlands.*
2. *bit.ly/refugee-phone-search*
3. *bit.ly/graham-wood-privacy-int*
4. *bit.ly/2017-emn-synthesis-report*
5. *bit.ly/automating-immigration-asylum*
6. *For more information about the case in the Netherlands, see Inspectie Veiligheid & Justitie. (2016, December 21). De Identificatie van Asielzoekers in Nederland. Vervolgonderzoek naar de registratie en identificatie van asielzoekers door politie en Koninklijke Marechaussee. Ministerie van Justitie en Veiligheid, Den Haag. For the case in Germany, see Biselli, A. and Beckmann, L. 2020. Invading Refugees' Phones; Palmiotto, F. and Ozkul, D. 2023. "Like Handing My Whole Life Over": The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures, VerfBlog, 2023/2/28.*
7. *bit.ly/invading-refugees-phones*
8. *bit.ly/government-gazette-netherlands*

The digitisation of US asylum application processes and externalisation in Mexico

By **Abril Ríos-Rivera**

The US government's app CBP One is part of a digital migration control regime that favours border externalisation, paralyses human mobility and saturates the capacity of organisations that support asylum seekers and other migrants in Mexico.



Sunset at the Mexico-U.S. border wall from the Mexican side. Tijuana, Baja California, Mexico. May 2023. Credit: Abril Ríos-Rivera

In theory anyone can seek asylum[1] in the US regardless of their immigration status. In reality, most of those who want to seek asylum in the US need internet access and a phone to download and use the CBP One application (app). With this app, asylum-seekers can schedule appointments to start the application process in the US. The appointment scheduling function can be accessed in the centre and the north of Mexico. As such, the US American asylum application process begins in Mexico, the vertical border[2] that divides the US and Latin America.

This article analyses the CBP One app as part of a digital migration control regime and explores how its use shapes asylum-migration policy and practice on both sides of the border. I draw on ethnographic research I conducted from October 2022 to July 2023 in Tapachula, Chiapas (southern border), Mexico City and Tijuana, Baja California (northern border), Mexico.

Smartphones are an integral part of migration processes. Phones are essential to design travel routes, maintain and create social relations, keep and share information, send and receive money, and apply for or renew visas. Phones are used to store evidence relevant to asylum applications. They can also enable coordination between migrants and organisations that support them; this can help asylum seekers to advance their own agendas and achieve their goals.

However, although digital technologies can

serve the interests of migrants (including asylum seekers), they also instrumentalise surveillance and control. For example, the US immigration authority's SmartLINK app monitors migrants through virtual checks and regular communication with immigration agents. Other digital technologies like SISCONARE,[3] the digital platform for asylum application processes in Brazil, are used for immigration enforcement. While these technologies facilitate communication and may save time for authorities and some migrants, they limit[4] its use to those who have access to technological devices – those who are literate and digitally skilled – they also threaten human rights and affect users' psychological wellbeing. The use of mobile phone apps like CBP One increases the number of checks along migratory routes and turns migrants' phones into mobile borders.[5]

Why was the CBP One app introduced?

The United States Customs and Border Protection (CBP) launched CBP One in 2020 as a portal[6] to services. Although the app was not designed for asylum seekers, from January 2023 it became the main way to apply for asylum and humanitarian parole in the US from Mexico.

Before 2023,[7] CBP mostly relied on third parties to input information on behalf of individuals. During Title 42 restrictions, authorised organisations would send the CBP information, on behalf of people seeking humanitarian exemptions to Title 42. From April 2022, CBP allowed Ukrainian citizens under the programme 'Uniting for Ukraine' to register their information. This programme allowed hundreds of Ukrainians to enter the USA, while other migrants and asylum seekers had to wait in Mexico. In January 2023, the CBP granted migrants of other nationalities the right to register their own information.

The transformation of CBP One into a migration management tool was due to changes in US immigration policy. The following four policies[8] led up to this transformation:

(i) Waiting lists or metering (February 2016)

This policy operated in border cities in the north of Mexico, first with paper lists and then digital ones. Asylum seekers, and then Mexican organisations and authorities kept the lists. Every day, the CBP asked for the list and let a number of people into the US. In November 2021 this policy was declared to be illegal and was withdrawn.

(ii) Migrant Protection Protocols (MMP) or 'Remain in Mexico' (January 2019)

This policy allowed applications for asylum at the southern US border to be processed while sending people back to Mexico to wait for their hearings in the US. It was suspended in January 2021, terminated in June 2021, modified and reinstated in December 2021, and ceased in October 2022. There are no new records or hearings.

(iii) Title 42 (March 2020)

This policy allowed the US government to expel migrants and asylum seekers on the grounds of protecting public health. At least 2.8 million expulsions took place under Title 42, and it was criticised for its lack of substance related to public health issues. The public health emergency declaration that justified the expulsions expired on 11th May 2023.

(iv) Circumvention of Lawful Pathways (CLP) or 'Asylum ban' (May 2023)

This rule presumes that those who cross the US southern border without authorisation are ineligible for asylum if they do not have a CBP One appointment, or if they were granted asylum in a third country en route to the US. Exemptions apply to those who

were provided with authorisation to travel to the US to pursue a humanitarian parole process, those with a CBP One scheduled appointment, those who were unable to access and use the app, those who were denied asylum in a third country and unaccompanied children. The rule has been the subject of two lawsuits.

Digital technologies have supported the implementation of these policies, which have enabled the US authorities to use Mexico as an external border. Under economic pressures, including tariffs on Mexican exports, Mexico has accepted this condition. CBP One is an instrument of control, a form of metering 2.0 that keeps asylum seekers within the Global South.

The way CBP One functions has changed over time. Every day CBP assigns a limited number of appointments. People fill their applications out and they are put into a lottery type system and notified the following day whether they have an appointment, which is usually a few weeks later.

Migration-asylum policy and practice paralyse mobility

The use and the effects of CBP One do not begin at the US-Mexico border. Many people already know about the app from the onset of their journeys. Due to the numerous changes in migration policies, migrants and asylum seekers have to change their plans constantly; they have to request asylum in Mexico even if they do not want it, and wait in cities where they do not have support networks. During my research, numerous changes were made to US-American and Mexican migration policies, and Mexico remained one of the countries with the highest number of new asylum applications worldwide. Detentions of irregular migrants in Mexico reached record levels in 2023.[9]

Why is it important to think about asylum and irregular migration in Mexico in relation to CBP One? Thousands of people cross Mexico's southern border in search of safety and opportunities in the US, Canada and Mexico. The current migration policies and practices undermine their journeys. The use of refugee status and complementary protection in Mexico is part of a deterrence strategy.

Let's think about the case of Nicole and Ale (25 and 30 years old), a transgender heterosexual couple from Central America who fled transphobic violence and waited months in Tapachula for documents.[10] Thousands of people are stranded in Tapachula[11] waiting for a resolution on their refugee status or other documents that let them move around Mexico safely and avoid irregular routes. Despite not wanting to stay in Mexico for fear of being identified by their perpetrators, Nicole and Ale applied for and got refugee status in Mexico.

Gabriela, (Salvadorian refugee, 29 years old) also told me:

> *"I did not want refugee status... it was to be able to move forward..."*

Refugee status is being used as a transit permit and it is almost the only way to gain access to migration documentation in Mexico. The process takes months and in some instances asylum seekers are left with their cases unresolved indefinitely. In 2023, only 20% of the total asylum applications were assessed. "The strategy is to tire people out," said human rights defender Guillermo Naranjo.

It is a problem that Mexico uses refugee status as the main documentation for forced migrants. This is not only because the position of Mexico being a 'safe country' is questionable, but also because seeking refugee protection in Mexico might affect

the applicant's chances of gaining asylum in the US. Under the CLP rule, one of the exemptions applies to those who were denied asylum in a third country, including Mexico. However, how can asylum seekers fulfil this criterion if Mexico lacks the capacity to assess asylum applications? The widespread use of refugee status is a border externalisation strategy that links the US asylum process with Mexico's.

CBP One is a form of documentation that, in some cases, enables transit through Mexico. Migrants and asylum seekers I interviewed confirmed that, without immigration papers, the bus companies refused to sell them tickets for the trip. These companies and the Mexican migration authorities often ask them for proof from CBP One that states that the person in question must be in the centre or north of Mexico.

Madison (an Ecuadorian refugee and transwoman, 22 years old) who I met in Tapachula explained that even though she had been granted a humanitarian visa, that allows travel through Mexico, the bus company would not let her board until she had confirmation from CBP One:

> *"I got confirmation from CBP One that I had to get to a port of entry so that I could travel. Then they let us on, we went to Mexico City."* – Madison

The use of refugee status and CBP One in Mexico helps keep forced migrants within the limits of Latin America. Compared to previous migration control systems, the strategy has been effective at spreading forced migrants throughout the country, but it has overwhelmed receiving cities and shelters especially in the southern and northern borders of Mexico. Asylum seekers continue to wait for long periods in areas where they do not have jobs or networks of support, lengthening periods of uncertainty and exacerbating physical and psychosocial risks.

The (dis)advantages of CBP One: what can we learn?

One of the main advantages of CBP One is that it speeds up the administrative process for the US authorities. It enables them to monitor people, systematically obtain information and limit the number of people who get into the US. Although the app has some advantages, the benefits are for the authorities and not for those who need protection.

Migrant rights organisations have repeatedly reported[12] that the app stands for the violation of the right to asylum, it diverts resources on phones and phone credit, and it has numerous technical flaws. The app is only available in English, Spanish and Haitian Creole. This has caused problems, especially for indigenous communities, who speak other languages, and for those who do not know how to read – most of them being women. In family groups, the app tends to be controlled by men. This exacerbates the subordination of women and perpetuates unequal power relations.

CBP One was designed to support the reduction of people smuggling and organised crime. However, the app encourages fraud and illegal trade. Many migrants are paying[13] for people to help them use the CBP One app or to register people outside northern and central Mexico through the app via a Virtual Private Network (VPN). CBP One promotes digital crime and strengthens a digital economy of migration control imposed from above and perpetuated from below.

The use of this technology amplifies waiting periods, produces forced immobility and results in the saturation of shelters in Mexico. Migrant shelters and organisations meet

only some of the migrants' and asylum seekers' needs. Nicole and Ale waited a year in the south, centre and north of Mexico. In Tijuana, Nicole told me

> *"I am still in the shelter. The app hasn't given me an appointment... The internet connection is unstable in the shelter because everyone is applying for the appointment."*

Civil society and other organisations that support refugees and other migrants mainly provide shelter (or lodging) and food, some provide internet access, psychosocial support, legal advice, information, education and transport. Organisations take on the work that arises from restrictive and changing policies. Although the work of these organisations is fundamental to the survival of migrants, their work is limited to short-term solutions.

The experience of CBP One shows that digital technologies have the potential to enhance migration processes, but they also cause harm by hindering access to international protection. I offer a set of recommendations:

(i) Short-term

a. CBP should correct the technical flaws with the app.
b. The app should include other languages, especially indigenous languages.
c. CBP should integrate visual user-friendly strategies for those who do not know how to read.
d. CBP should develop, update and share informative material about the app and problem solving.
e. The asylum ban rule in the US should be terminated.
f. Gender-sensitive programming is critical to reduce gender-diverse migrants' vulnerabilities as they wait in Mexico. Work programmes for gender-diverse people can help them expand their livelihood opportunities and avoid engaging in sex-work as the only available option.

(ii) Medium-term

a. CBP should remove the requirement to have an appointment at a port of entry and offer solutions within the US territory.
b. Canada should be involved in the relocation and assistance processes. For thousands of migrants the destination is Canada.

The implementation of these recommendations is insufficient if the US-Mexico migration-asylum policy stays the same. The political rhetoric[14] in both countries is that of investing in humanitarian and development programmes, yet the investment goes into border protection. As de Haas[15] points out, global migration is not at an all-time high and border restrictions produce more migration. It is important to invest in programmes that promote mobility as being a real option and not as the only alternative.

> "*Nobody wants to migrate from their country and leave their people, it is out of necessity*" – Gabriela, Salvadorian refugee, 29 years old.

Abril Ríos-Rivera
DPhil candidate, Centre on Migration Policy and Society, University of Oxford
Abril.riosrivera@compas.ox.ac.uk
linkedin.com/in/abrilrios/

1. *bit.ly/asylum-eligibility-applications*
2. *bit.ly/migrants-trapped*
3. *bit.ly/conare-web-login*
4. *bit.ly/brazil-country-report*
5. *bit.ly/glitches-digitization-asylum*
6. *bit.ly/cbp-one-mobile-application*
7. *bit.ly/cbp-one-overview*
8. *bit.ly/us-border-primer*
9. *bit.ly/detencion-migrantes-mexico*
10. *Quotes are taken from interviews the author conducted, pseudonyms have been used.*
11. *bit.ly/migrants-set-out-mexico-s-border*
12. *bit.ly/challenge-cbp-one-turnback-policy*
13. *bit.ly/asylum-seekers-cbp-one-challenges*
14. *bit.ly/mexico-us-joint-communique*
15. *bit.ly/how-migration-really-works*

The essential role of digital literacy in contexts of forced displacement

By **Jenny Casswell**

Digital technology can be a catalyst for positive change for forcibly displaced people if individuals have the requisite digital literacy to participate equally, meaningfully and safely in the digital world.

A class mentor guides a student through a lesson at the centre in Nairobi, Kenya, where UNHCR's partner, the Danish Refugee Council, facilitates training for Kenyans and refugees in digital literacy. Credit: UNHCR/Charity Nzomo

Historically, the essential role of digital literacy in forced displacement contexts has been underestimated, misunderstood and, at best, an afterthought.

However, with the increasing adoption of technology across society, there is growing recognition and understanding of the essential role that digital literacy plays in the digital inclusion and protection of forcibly displaced and stateless people. Although progress is being made, a concerted effort is needed to improve digital literacy interventions to ensure displaced communities and host communities can use technology effectively and safely, minimising their exposure to digital risk.

This article shares the growing evidence base on this topic and offers innovative examples of digital literacy interventions. It also reflects on common pitfalls, providing recommendations for rolling out digital literacy interventions more effectively in forced displacement contexts.

Defining digital literacy and skills

Digital literacy is a broad topic ranging from basic/foundational skills, like the ability to access the internet and search for content via internet browsers or apps, to more advanced digital skills, like digital content creation, coding and data science.

The lack of consensus on a standard definition of digital literacy and digital skills has made the design and implementation of interventions challenging. In humanitarian contexts this lack of clarity has contributed to ad-hoc approaches[1] being taken to enhancing the digital literacy and skills of forcibly displaced populations, with missed opportunities for knowledge sharing and learning, often resulting in low-quality, ineffective digital programming.

So, how can we define the terms? 'Digital skills' broadly focus on the technical – 'what and how' – of using digital technologies whilst 'digital literacy' is more focused on the contextual and creative problem-solving elements – 'why, when, who and for whom.'[2] Technological advancements and associated proliferating digital risks make it increasingly important for digital competencies to span beyond operational/technical skill sets, to 'softer' skills.

UNHCR and other organisations working with displaced populations are addressing this new reality by incorporating digital skills under the wider umbrella of digital literacy. USAID's 'digital literacy' definition[3] is applicable to low and middle-income countries and device agnostic (inclusive of mobile phones, a device sometimes disregarded in digital literacy definitions). Three-quarters of refugees[4] live in low and middle-income countries where people primarily connect to the internet via mobile phones, making this definition well-suited to forced displacement contexts:

'Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life.' USAID, 2022.

Adopting such a definition can encourage humanitarian practitioners to incorporate the softer skills of digital literacy, including digital risks, into programming, in addition to the technical skills, which have traditionally been the sole focus. A more nuanced understanding of the topic can also encourage more consistent and considered approaches across the humanitarian sector, encouraging lesson sharing of good and poor practice on digital literacy.

Growing the evidence base on digital literacy

Until recently, there was a dearth of evidence to understand forced displacement communities' digital literacy levels,[5] concerns, priorities and needs, despite this being a necessary place to start[6] for any digital intervention.

In 2022, GSMA and UNHCR conducted research[7] in Lebanon, Papua New Guinea (PNG) and South Sudan to better understand how displacement-affected communities were using mobile phones. A stand-out finding was that digital literacy and skills were a consistent barrier to digital inclusion for communities across all contexts.

In PNG, nearly two-thirds of phone users who did not use the internet cited the main reason for their digital exclusion as "not knowing how to use the internet by themselves." Across all contexts, low literacy and digital literacy levels were particular barriers for older people and persons with disabilities. These findings are consistent with prior research[8] with persons with disabilities in Nairobi, Kenya. In Sudan and PNG, low digital literacy and

trust in mobile money systems led to fear over the security of funds and personal information, often resulting in limited use of digital financial services.

> *"I don't know much about phones, [let] alone mobile money... I could try to find out [if only] I had a phone."* – Internally displaced woman, Bor, South Sudan.

The connection between digital literacy and protection

Beyond being a pre-requisite for digital inclusion, digital literacy is essential for digital protection.[9] Low levels of digital literacy and high exposure to technology put people at risk, particularly the most marginalised.

UNHCR research in Uganda[10] found that refugees often feel powerless to protect themselves against online threats and digital risks. Research in Lebanon[11] found aid-related scams common, and false information about humanitarian services made delivery and access to services more challenging. One-tenth of phone users targeted by a scam reported being harmed by that scam – for example, by paying to access fake resettlement schemes, wasting time, or pursuing false information on humanitarian assistance.

Such examples demonstrate that for the humanitarian sector to maintain its commitment to 'do no harm' principles, it must ensure that forcibly displaced and stateless people have the requisite skills and knowledge to minimise risks associated with technology. Failing to act will increase the risk of displaced populations falling victim to digital predators.

Guidance for implementing effective digital literacy interventions

As technology has become an integral part of daily life, more attempts are being made to train displaced populations on digital technologies. However, digital literacy interventions are not easy to do well and often the intended long-term outcomes of trainings (e.g. employment/livelihood opportunities, financial inclusion, improved online safety etc.) are not realised.

Examples of poor-quality training include ad-hoc, short-term training (often a few hours/days) delivered on a device (usually a laptop) which participants have no access to outside the training, teaching technical skills that are too advanced and/or irrelevant for the target audience.

Based on UNHCR's assessments of interventions across numerous forced displacement contexts, there are a number of important factors to consider when designing and implementing effective digital literacy training.

1. **Involve communities in co-creation, design and delivery of training**
   Understanding of the existing skills, capacities and preferences of local communities is essential, particularly to ensure that existing organic skills-building through local digital pioneers, for example, can be leveraged.
2. **Draw from existing digital literacy/skills curricula**
   A broad array of digital literacy training courses have already been tried and tested. It's important to avoid reinventing the wheel by designing these from scratch every time. Scoping national approaches to digital literacy building is also important.
3. **Tailor content and training to the specific needs and lives of communities**
   Digital literacy training is only effective if it is of relevance to people's daily lives and needs. This includes a nuanced understanding of the types of outcomes

they want to achieve with digital skills. Training local individuals to deliver training and partnering with expert organisations to develop and tailor training to specific groups can support this.

4. **Consider in-depth how to successfully deliver training to marginalised groups**
   Have you generated an in-depth understanding of all segments of your audience and their digital literacy level, needs and learning preferences? Digital divides[12] are often larger in humanitarian contexts and therefore digital skills programmes need to be specifically designed with these groups in mind. Digital literacy interventions for marginalised groups are only effective when detailed needs assessments are conducted to inform appropriate tailoring for specific target audiences.
5. **Incorporate digital safety into your training**
   Groups already at enhanced risk of harm will likely face greater risk (e.g. abuse of personal data, cyberbullying, misinformation, scams/fraud, etc.) if digital safety elements are not incorporated into digital interventions.
6. **Develop an effective monitoring and evaluation framework**
   It is important to understand whether your training is effective and if participants are improving their digital skills and confidence levels. Go beyond assessing attendance or satisfaction levels by applying criteria to measure reaction, learning, behaviour and results (see Kirkpatrick model[13] of evaluation).
7. **Consider how to make the training sustainable**
   Adopting digital tools and services requires multiple opportunities for users to learn and partake in refresher activities. Time-bound interventions offer lower value compared with continuous and iterative digital literacy programming. Working with partners, governments, civil society and the private sector can create longer-term, more sustainable trainings that extend beyond individual programmes.

Innovative approaches to digital literacy

Organisations operating in humanitarian contexts are beginning to put these considerations into practice. UNHCR is driving innovative approaches to increasing digital literacy through the Digital Innovation Fund.[14] In Indonesia,[15] UNHCR and partners are demonstrating how to tailor digital literacy curriculums to needs by facilitating co-creation workshops with refugee communities. The project is embedding the curriculum into established learning centres, capitalising on existing resources and expertise while also increasing sustainability. More advanced digital skills, such as web development, are being taught in partnership with GoMyCode in Tunisia,[16] complemented with career orientation sessions to smooth the learning-to-earning pathway.[17]

Digital Opportunity Trust (DOT) and GSMA also offer successful examples of digital literacy training. Both organisations understand the value of identifying and training local individuals as trainers to maximise the sustainability and impact of initiatives. DOT leverages community leaders and digital ambassadors in their programmes. For example, in Rwanda, community members are being trained as digital career counsellors to support refugees to access online scholarships and jobs.

GSMA works with mobile operators who leverage mobile money agents in local communities to deliver training based on GSMA's Mobile Internet Skills and Training Toolkit[18] (MISTT). MISTT is a set of free resources that use a 'train the trainer'

approach to teach people the basic skills they need to access and use mobile internet, including sections on navigating digital risks. MISTT-based content has been used in more than 27 countries to train over 65 million people on digital skills. In partnership with the WFP, GSMA leveraged MISTT content to improve women's digital financial skills in Somalia[19] and Burundi.

Recommendations

The following recommendations are provided to boost digital literacy levels among forcibly displaced communities.

Adopt a consistent definition of digital literacy

Adopting a consistent digital literacy definition that acknowledges the importance of the softer skills required to use technology safely and effectively, such as understanding digital risk, is essential. This will ensure humanitarian practitioners go beyond delivering digital interventions that solely focus on technical skillsets, broadening approaches to achieve longer-term outcomes such as digital employment or financial inclusion.

Pay attention to common pitfalls and learn from best practice

Ad-hoc approaches to boosting digital literacy exist across the development and humanitarian sectors, with interventions making the same mistakes time and again. Pay attention to common pitfalls and the guidance outlined in this article when designing training. Additionally, learn from industry peers who are demonstrating innovative examples of enhancing forcibly displaced individuals' digital literacy levels, leading to broad-ranging positive outcomes.

Ensure digital literacy is integral to digital strategies

Digital programming must go beyond ensuring access to connectivity, digital devices, and digital services, to support the development of digital literacy among communities. With most humanitarian organisations implementing digital strategies, digital literacy must be an integral part. For example, UNHCR recognises digital literacy[20] is a pre-requisite to all three outcome areas in its Digital Transformation Strategy 2022–2026[21] (Digital Inclusion, Digital Protection and Digital Services), investing resources into this critical topic.

Ultimately, the transformational benefits of digital inclusion for forcibly displaced and stateless people will only be realised if digital literacy is placed at the forefront of digital humanitarian interventions and is no longer just an afterthought.

Jenny Casswell
Digital Literacy Specialist, UNHCR
jennycasswell@gmail.com
X: @jencasswell

1. *bit.ly/unhcr-digital-literacy-refugees*
2. *bit.ly/digital-skills-vs-digital-literacy*
3. *www.usaid.gov/digital-development/digital-literacy-primer*
4. *www.unhcr.org/mid-year-trends-report-2023*
5. *Historically, many assessments that touch on displaced communities' technology adoption emerged from media development and intersections with humanitarian action, including concepts of communicating with communities, community engagement, and accountability to affected people. Digital literacy components were seldom included in spite of the important correlation with channels, trust in information sources etc.*
6. *www.gsma.com/mobilefordevelopment/conua/*
7. *bit.ly/gsma-DigitalWorldsDAC*
8. *bit.ly/gsma-digital-inclusion-refugees-disabilities-Nairobi*
9. *UNHCR defines digital protection in their Digital Transformation Strategy, aiming to ensure communities can exercise their human rights online and are protected from digital risk, enabling them to have access to trusted channels, avoid harm and have agency in decision-making. www.unhcr.org/digitalstrategy/digital-protection/*
10. *bit.ly/unhcr-manage-digital-risks-refugee-connectivity-report*
11. *https://www.gsma.com/mobilefordevelopment/the-digital-worlds-of-displacement-affected-communities/*
12. *bit.ly/gsma-digital-lives-refugees*
13. *www.valamis.com/hub/kirkpatrick-model*
14. *www.unhcr.org/innovation/digital-innovation-fund/*
15. *bit.ly/unhcr-tailor-made-design-refugees*
16. *bit.ly/unhcr-innovating-digital-employment-pathways*
17. *bit.ly/unhcr-digital-learning-earning-gap*
18. *www.gsma.com/mobilefordevelopment/mistt/*
19. *bit.ly/reliefweb-wfp-gsma-bolster-humanitarian-assistance*
20. *bit.ly/unhcr-digital-literacy-skills*
21. *www.unhcr.org/digitalstrategy/*

Addressing the digital gender gap among displaced communities – lessons from Yemen

By **Kristy Crabtree** and **Rana Obadi**

Technology can be a great enabler in humanitarian settings, extending access to information and services to affected populations. However, gendered barriers to accessing internet-enabled devices should be addressed as part of the response.

In a world in which 95% of the global population lives "within the footprint of a mobile broadband network," and the majority own a smartphone,[1] technology has an important role to play in the humanitarian response to large-scale crises. Through internet and mobile networks humanitarian responders can provide life-saving information and virtual services for affected populations. The recent proliferation of aid-related digital products and platforms is a testament to this fact.

As aid programmes increasingly harness the advantages of technology for broader reach and impact, some humanitarians may mistakenly assume that equitable access to virtual services is universally guaranteed. In their Mobile Gender Gap Report 2023,[2] GSMA points out that "women in low and middle-income countries are 19% less likely than men to use [the Internet]."

Digital gender gap in humanitarian settings

International Rescue Committee (IRC) conducted research in 2017 and 2019 in Lebanon[3] and Uganda[4] to better understand the digital gender gap in humanitarian settings. The data uncovered several key barriers that women and girls face in relation to digital spaces. These include:

- **Prohibitive costs:** The number one barrier reported was the unaffordable cost of mobile devices and data.
- **Public space restrictions:** Women and girls are often restricted from public spaces that are largely inhabited by men (e.g. school, work, markets or other public gathering places), which weakens their natural exposure to mobile technology and the internet.
- **Lack of technical confidence:** Limited access to internet-enabled devices means that women and girls may lack technical confidence and desire for access.
- **Social disapproval:** Negative attitudes toward women and girls' use of phones and the internet affects their ability to build digital literacy organically, safely, and without intervention. Male figures in the household and community are quick to assert the hazards for women (many of which are related to the potential for maintaining romantic relationships which male family members deem unacceptable).

The barriers listed above for humanitarian settings are comparable to those reported in low and middle-income countries. USAID[5] similarly found affordability, availability, ability and appropriateness were the primary factors negatively affecting women and girls' access to internet-enabled devices.

Among all these obstacles, the barrier of social disapproval is unique to the experience of women and girls, restricting women and girl's desire, access or confidence in the

use of information and communications technology. The threat of generalised harassment from other community members adds yet another layer of fear.

Promoting inclusive digital programmes through device provision and training

The onus is on humanitarian response practitioners to develop inclusive ways for women and girls to equitably access digital or digitally-enabled programmes and services.

In 2020, spurred on by the rapid shift to virtual services (necessitated by Covid-19), IRC developed a gender-sensitive and safety-prioritising digital literacy curriculum for women and girls, called Safe Space to Learn.[6] IRC posited that if a programme loaned out mobile devices and provided access to the internet, along with digital skills training, there would be improvements in equitable uptake of technology.

The Safe Space to Learn curriculum includes several modules: 1) an introduction to digital spaces, 2) digital accounts and apps, 3) finding information online, 4) staying safe online, 5) social media, and 6) digital employment and education skills. To eliminate barriers to access, this curriculum was designed to be implemented in Women and Girls' Safe Spaces:[7] physical female only spaces where women and adolescent girls can gain knowledge and skills, access gender-based violence response services or other available services, and foster opportunities for mutual support and collective action in their community. The provision of mobile devices for loan countered issues around affordability.

Learning from the Safe Space to Learn digital literacy programme in Yemen

Yemen is one of the world's largest humanitarian crises, with 21.6 million people[8] in need of humanitarian assistance. The dire situation in the country, affecting 65% of the population, stems from an nine-year long conflict, which has caused high levels of unemployment and poverty, and limited access to basic necessities like food, water and healthcare, resulting in a majority of the population being on the brink of famine.[9]

Three-quarters of the 4.5 million displaced people are women and children. In this setting, as in many other situations of forced displacement, access to information and communication through social networks can be life-saving. The communication features of phones alone not only aid in connectedness but "enhance professional, educational and livelihood opportunities" GSMA. In Yemen, this holds particularly true because participants can now access recently launched community-led information services, such as Dalilak[10] (a Signpost[11] instance). These services empower clients during crises by providing actionable information to make critical decisions on the issues most relevant to them.

The Yemen Women and Girls' Safe Space, in the Khanfar district in the Abyan governorate, was chosen as a site to introduce the digital literacy curriculum because of proactive interest by the women and girls accessing the space. Khanfar, the largest district in Abyan Governorate, deals with sporadic conflict and hosts a significant number of displaced persons, estimated by staff to be around 20% of the population. While residents have mobile internet access, its speed is often inadequate, and interruptions in connectivity occur periodically. Fifty adult women from both rural and urban areas took part in the programme, with a slightly greater proportion of women from urban areas. Around half of the participants were women who bear the responsibility of supporting their families. The sessions were held twice a week for two hours each, and participants

were provided with a smartphone to use in the centre during the sessions.

Participants in the programme reported a four-fold increase in knowledge and higher confidence levels in practical elements of digital citizenship (the ability to effectively, safely and respectfully use the internet) such as online navigation, responsible account management, password management, and various strategies to support online safety. Participants viewed their access to information and opportunities as a great transformative benefit, citing newfound skills such as CV writing, access to new job platforms, and further skill building through certificate programmes.

Participants remarked on a significant shift in their digital confidence and online engagement. The programme fostered a supportive community amongst participants, promoting cooperation and knowledge sharing. This collaborative spirit extended beyond the programme, as evidenced by participants assisting family and friends with their digital navigation. One participant noted:

> *"I was able to support my sister. I helped her download apps, create a Google account, and navigate online safety practices. Witnessing her growing confidence in using technology safely has been incredibly rewarding for me."*

Another participant, a mother, conquered her initial hesitation regarding phone usage, and her involvement in the programme played a pivotal role in shifting her husband and son's cultural and religious views on women and girls using phones, leading to the normalisation of mobile phone usage within their family. This transformation culminated in the decision to purchase a smartphone for her daughter, and the mother and her adult son starting a business selling mobile phone data cards.

An unexpected outcome of the programme was participants asking for training in phone repair. The women who took part explained that typically, if a device breaks (a screen cracks or the charging port is damaged), they would be forced to get a new phone (often cost prohibitive) or ask permission to get help from a man at the market and give him full access to their devices. This raised concerns about photos of participants without a niqab (kept on their personal phone) potentially being used for blackmail. Their request: train us on how to fix the hardware, which will improve safety outcomes and provide a livelihood opportunity. The IRC has been exploring partnerships with local technical institutes as well as opportunities to connect digital literacy training with small business training.

While the digital literacy programme resulted in the strengthening of participant's practical and technical capabilities and broader empowerment, there were also challenges: unreliable connectivity, power outages and lack of personal device ownership. The absence of personal mobile devices for a subset of participants presents a potential obstacle to sustained engagement and independent application of acquired skills beyond the programme's duration. This could limit their ability to access online resources, maintain connections with the programme network and fully leverage their learning. However, loaned devices remain available at the Safe Space.

Based on insights from the implementation in Yemen, we can offer several recommendations to address the digital gender gap in contexts of forced displacement.

1. **Ensure equitable access to digital tools**
   Humanitarian agencies implementing virtual programmes should consider barriers to equitable access. Women, girls, the elderly, and rural populations

are less likely to have access to internet-enabled devices and technical confidence. Explore ways to address this through gender-sensitive digital up skilling. Online safety must be an essential component of any training and women-only spaces for training show positive results.

2. **Provide or loan smartphones**
   Loaning smartphones to participants or hosting a computer lab allows organisations to reach a larger number of participants without exhausting resources on gifted devices. This enables them to serve more communities and incentivises participants to actively engage in the training. Agreements on responsible device use can be discussed with participants to ensure shared expectations on usage. Consider gender-sensitive ways to facilitate this access.
3. **Incorporate messaging on social norms**
   Digital upskilling for women and girls is an important step towards digital equity; however, social and cultural barriers may persist. Programmes could consider including targeted social norms messaging on the use of technology. One example of this approach is Tech4Families, an Equal Access International initiative launched in 2019, which aims to bridge the digital gender gap in Northern Nigeria through mass media, skills training and family-based learning.
4. **Make connections between digital literacy and other activities**
   Digital literacy can be a launching pad for many other services and interventions. For example, participants in the Yemen digital literacy programme requested additional training on mobile phone repair.
5. **Explore ways to be more inclusive**
   Digital literacy programmes are commonly built with an assumption that users have basic literacy and numeracy skills. This excludes portions of the population without these skills. Yet, there are products that could be brought into digital literacy training to help overcome these barriers. For example, Google's Action Blocks[12] makes routine actions easier for users with customisable buttons that appear on the home screen. Icons on the screen can trigger pre-programmed actions.

When paired with a gender-sensitive and safety-prioritising approach, digital literacy training can protect women and girls' ability to exercise their human rights; extend their access to information; increase feelings of agency, and lead to more informed decision making. Digital literacy serves as a pathway to enhance digital inclusion and contributes significantly to society's progress toward gender equality by bridging the digital divide, enabling women and girls to actively engage in the digital age.

Kristy Crabtree
Senior Digital Innovation Advisor,
International Rescue Committee
kristy.crabtree@rescue.org
X: @kristycrabtree

Rana Obadi
Gender-Based Violence Information Management System Officer,
International Rescue Committee
rana.obadi@rescue.org

1. *bit.ly/state-of-mobile-internet-connectivity*
2. *www.gsma.com/r/gender-gap/*
3. *bit.ly/safety-planning-technology*
4. *Crabtree, K. (2020). Where are the women? How to design information and communication technology to be inclusive of women and girls in humanitarian settings. In M. N. Islam (Ed.), Information and communication technologies for humanitarian services (pp. 7-24). Institution of Engineering and Technology. (not available online)*
5. *bit.ly/gender-digital-divide*
6. *bit.ly/rescue-digital-literacy*
7. *bit.ly/womens-and-girls-safe-spaces*
8. *bit.ly/2023-unfpa-yemen*
9. *bit.ly/worldbank-yemen-overview*
10. *bit.ly/health-wash-yemen*
11. *www.signpost.ngo/*
12. *bit.ly/google-play-action-blocks*

Digital lifelines: addressing gender-based violence in Ukraine

By **Lala Zinkevych**

In Ukraine, a new wave of digital services has emerged to assist displaced populations vulnerable to conflict-related and domestic violence. This article considers the strengths and weaknesses of these innovative platforms.

As the war in Ukraine continues, gender-based violence (GBV) has become a major concern, especially for women facing displacement. Conflict-related sexual violence, domestic violence and human trafficking have become more prominent in a context where women make up the majority of the displaced population.[1]

Gender-based violence was already a prevalent issue in Ukraine, and its risks have escalated since the start of the war. In the first half of 2023, the National Social Services reported an almost twofold surge in services provided to GBV survivors. Concerns about trafficking, sexual exploitation and abuse have grown, especially at border crossings and in refugee accommodation. An estimated 2.5 million[2] people (83% being women and girls) are expected to need GBV-related services in 2024.

The fast-growing demand puts a significant strain on the country's protection and specialised GBV services.[3] Although Ukraine's GBV prevention and response system has made significant progress in the past decade, specialised services still encounter multiple challenges. Many people living in rural areas still lack access to services for survivors of gender-based violence. In 2023, 27% of households in the East region, which has been heavily impacted by combat actions and displacement, reported[4] that there were no services for survivors of GBV. Access to specialised GBV services is complicated by understaffing, particularly in key positions such as psychologists, social workers and legal staff. Additionally, in territories temporarily occupied by the Russian Federation, millions of Ukrainians struggle to access protection services and lifesaving supplies.

Challenges also arise at the individual level. Violence against women and girls remains significantly under-reported due to stigma, gender stereotypes and a culture of silence. Many GBV survivors tend to avoid reporting, fearing disclosure of their anonymity and further repercussions from the perpetrators.

Approaches and digital solutions

Digital service delivery has already been widely used to process Ukrainians fleeing the conflict. The most prominent example is the Diia[5] smartphone app, which has over 19 million users as of 2023 (used by 70% of all Ukrainians with smartphones) and is a digital tool for electronic versions of more than 117 official Ukrainian government documents with the same legal status as physical copies.

Initially created to make public services more accessible and enable the government to reach its citizens in remote areas and those with disabilities, the platform has also proven helpful for displaced and vulnerable populations without physical copies of important documents. The digital infrastructure in the region has played a

critical role in mitigating the challenges displaced Ukrainians face, with digital tools integrated at every stage of the assistance process, including protection services.[6]

UNFPA[7] has assisted the Ukrainian government in building up the system of specialised GBV services for more than two decades. Since the start of the war, UNFPA has worked with the Ukrainian government to develop digital solutions to fortify the existing system of specialised GBV services. Each of the tools complements the system in a unique way by a) equipping GBV survivors with timely information about GBV services tailored to their needs and mobility, b) providing anonymous emergency psychological help in and temporality out of government-controlled territories, and c) ensuring confidential contact with the National Police and emergency services in cases where there is an immediate threat of violence.

Aurora

The Aurora[8] website serves as a lifesaving tool, granting survivors of conflict-related violence, including sexual violence, access to safe, free and anonymous services irrespective of location (whether within Ukraine, abroad, or in areas temporarily beyond the government's control). Its primary objective is to offer specialised professional psychotherapy support to survivors using EMDR (Eye Movement Desensitization and Reprocessing) therapy as well as trauma-informed CBT, a highly effective tool for dealing with traumatic cases. The platform also offers online or telephone consultations with reproductive health, legal and protection specialists. Aurora is effectively integrated into the overall response system by collaborating with similar networks like survivors' relief centres and rehabilitation programmes. Additionally, the platform facilitates referrals to and from other services. Users can remain anonymous if they prefer not to disclose their identity.

After applying to Aurora, a survivor can be assisted by a coordinator who works based on the requests and consent of survivors. The coordinator is positioned to conduct needs assessments and may provide additional counselling as needed. Once these processes are completed, referrals can be made to help the survivor navigate available services, avoid re-traumatisation, and enhance the effectiveness of the aid provided. Notably, Aurora welcomes survivors from various backgrounds, although most users are women, representing over 90% of the total. The majority of users fall within the age range of 18-39. As of November 2023, 82% of Aurora's users reported that they experienced sexual violence, including conflict-related sexual violence. Almost a quarter of users are using the service from abroad. Most of the requests from within the country come from highly populated areas with a large concentration of internally displaced persons – including Kyiv, Odesa and Mykolaiv.

Survivors Relief Platform

The Survivor Relief Platform[9] is the first online platform in Ukraine that provides verified and comprehensive information about specialised and lifesaving services for those affected by the war and displacement. This platform helps citizens on the move quickly connect with the required services to get free and confidential social, legal, humanitarian and psychological support through chatbots, hotlines, and offline and online consultations from verified providers.

The platform aims to create a trusting environment between the affected individuals and service providers, while comprehensive professional support is the first step towards achieving justice. After

receiving assistance, survivors may be willing to approach law enforcement agencies to document cases of sexual violence used by occupiers as a weapon against the civilian population and hold wrongdoers accountable in the future. It is designed not only for the affected individuals but also for social protection professionals. The platform enables social workers to reach a significantly wider range of people affected by war and displacement with social support.

This tool complements other similar initiatives, such as Aurora and in-person survivors relief centres. There are plans to add features on job search, economic empowerment and children's education.

Kryla ('Wings')

Kryla[10] is a mobile application designed to help women who experience gender-based violence, regardless of their location within government-controlled territories. It provides emergency help and support to these women, even when they are on the move.

This application is designed as a menstruation calendar with a hidden feature that allows users to call the National Police of Ukraine and access information about emergency services. To do this, users must register for the service and enable geolocation. The application is designed in such a way that it is completely inconspicuous to the abuser, allowing women to install the app on their smartphones without fear. The open part of the application tracks the menstrual cycle and predicts ovulation. They hold down the wings symbol for three seconds to access the hidden feature, which includes a button to call the police, useful information and contacts for other support services. The app's name is not disclosed for the users' safety. It can be downloaded from both Google Play and the App Store.

The application facilitates assistance for women who cannot call the police due to speaking, hearing or other impairments; an abuser's total control over their personal lives; a lack of funds to make calls; or similar obstacles. The main advantages of the application are direct communication with the police through the SOS button and automatic location detection of GBV survivors through geolocation.

The Ministry of Internal Affairs and the UNFPA disseminate information about the application among women who need it through the survivors relief centres, host community leaders and influencers. Since its launch in August 2022, the application has been downloaded by over 34,000 users and has a high customer ranking (4.6 out of 5) in the App Store.

Successes

User uptake

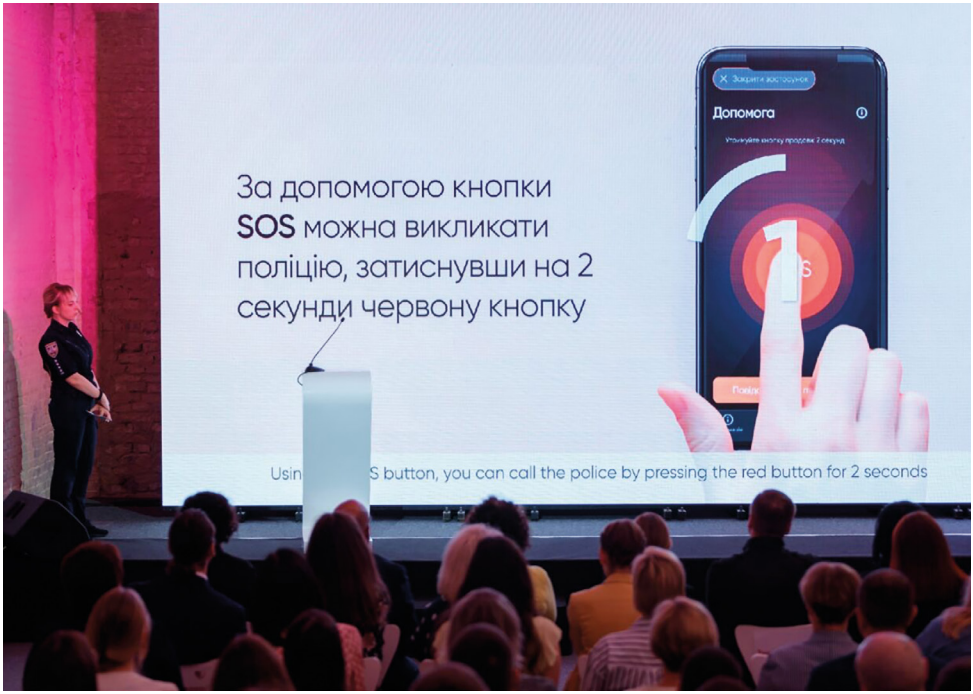
The digital tools described above have been successful in terms of user uptake and have increased the institutional capacity of the state system for specialised GBV services.

Integration with existing services

These solutions were integrated into the existing state system for GBV response as an extension of existing services. The speed with which these online services were introduced and their complementarity with the existing physical infrastructure, such as shelters, day centres, crisis rooms and hotlines, has helped people on the move to get comprehensive information and assistance whenever they needed it, even those who are staying in territories temporarily out of government control.

Public awareness

These tools were effectively integrated into the nationwide information platform 'Break the Circle,' which has gained sufficient reach among the wider public over the last few



A demonstration of the Kryla wings app with Kateryna Pavlichenko, Deputy Minister of the Ministry of Internal Affairs of Ukraine on stage. Credit: Andriy Krepkikh/UNFPA

years and ensured government support and promotion.

Challenges

There are a few factors that might limit the effectiveness of these tools.

Connectivity

Poor internet and mobile connections may hinder the provision of services, and applying for them may pose potential risks to survivors, especially in areas beyond the control of the Ukrainian government. Additionally, a lack of digital devices and digital literacy can be a barrier to using the tools, especially among older members of the population.

Under-reporting

Survivors may not report violence to officials in a timely manner. In many cases, survivors first seek assistance from civil society organisations to receive humanitarian aid, medical services, and essential legal aid services to restore their documents and obtain social benefits and entitlements. Many survivors only disclose their experiences after a lengthy period and once they have received psycho-social support and feel safe.

Inability to advertise

Digital solutions with hidden reporting functions cannot be openly promoted through media channels. Therefore, more sophisticated promotion strategies are necessary for women to feel secure having them on their phones.

Conclusions and ways forward

The digital tools discussed in the article collectively illustrate the potential of technology in advancing GBV protection efforts. The use of these tools in Ukraine during one of the largest displacement crises in Europe could serve as a test case for a range of GBV service provision solutions. These tools have the potential to be replicated in other regions and contexts with a sufficient level of technology and mobile services development.

To ensure that technology can be used effectively to address gender-based violence, especially in conditions of military conflict and displacement, the following steps should be taken.

Safety and privacy concerns

Any solution must prioritise the safety and privacy of survivors. Any data collected must be anonymised so that no one has access to sensitive or identifiable information. It is also important to carefully consider data storage, ownership and management. Any technological solution should include a mechanism to connect survivors with trained professionals to maximise their safety and consider issues of the quality and accessibility of the internet connection. Displaced women should be co-creators of any solution to ensure the best possible outcome.

Modular and adaptable solutions

When developing solutions, it is important to consider open-source and modular approaches that can be customised according to the specific needs of a particular context. This provides flexibility to adapt as needed. It is also important to map and assess the capacity of local partners, which can help identify appropriate services and reveal areas that need support in enhancing their ability to better respond to gender-based violence.

Ensure inclusivity

It is crucial to consider the age and background of users and their level of digital literacy when introducing digital solutions. The use of digital tools could deepen the digital divide if access is not considered upfront. Inclusive solutions that refer to the needs of people with impairments and limited knowledge of technology should be considered.

Lala Zinkevych
Gender Policy and GBV Prevention Adviser, UNFPA Ukraine
linkedin.com/in/lala-zinkevych/

Article contributors:

Kostiantyn Boichuk
GBV Programme Analyst,

Olga Chuyeva
UNFPA CRSV Response Specialist,

Oleskandr Dashutin
CRSV Programme Assistant,

Nina Bagraeva
Communications Specialist,

UNFPA Ukraine

1. *As of December 2023, 59% of the 3.7 million internally displaced persons are female. Similarly, 93% of the 4.5 million returnees reintegrating into the country and 88% of the 6.5 million refugees residing outside Ukraine are also female.*
2. *bit.ly/ukraine-plan*
3. *bit.ly/ukr-gender-based-violence*
4. *bit.ly/msna-gender-focus*
5. *diia.gov.ua/*
6. *bit.ly/ukraine-launches-e-service-idp*
7. *ukraine.unfpa.org/en*
8. *avrora-help.org.ua/home*
9. *www.help-platform.in.ua./*
10. *bit.ly/infotech-wviolence*

Safety, dignity and efficiency: the role of digital platforms in legal aid

By **Amir Shiva**

Digital legal aid platforms for displaced populations have transformative potential. This article discusses the Norwegian Refugee Council's experience of implementing a digital legal aid platform while navigating ethical considerations.

Legal aid plays a critical role in protecting the rights of displaced populations, ensuring their access to essential services in humanitarian contexts. However, there is often a shortage of access to legal service providers available to displaced people. In many cases, lawyers engaged by NGOs and UN agencies are the sole experts in this specialised area of law in conflict-affected countries.

Given the high demand for timely legal assistance from the target population and the substantial dependence on qualified professionals, legal aid programmes are prime candidates for digital transformation. Yet, the sensitive nature of legal aid interventions necessitates strong adherence to 'do-no-harm' principles. The challenge lies in balancing the pressing need for impactful digital solutions with the imperative to handle these interventions with the utmost care and attention to ethical considerations.

The Norwegian Refugee Council has introduced a digital legal aid platform – KOBLI[1] – to enable displaced people to access timely and accurate legal information online. KOBLI is a suite of tools tailored for supporting legal assistance in humanitarian settings, developed by the Information, Counseling and Legal Assistance (ICLA) team (i.e., NRC's legal aid programme). Legal aid programmes can use the digital tools to establish an online presence through mobile apps, social media, websites and messaging applications.

An advert for the KOBLI app. Credit: NRC

KOBLI has a staff-facing component and a beneficiary-facing component. Using the staff side, legal aid workers can organise, develop, review and publish content in different formats (such as chatbot, FAQs and guide paths). Using the beneficiary-facing component, refugees can explore legal scenarios, navigate through the chatbot, and track their progress on interactive self-help tools.

Following an extensive journey involving design, software development and testing, KOBLI was first piloted in Lebanon in 2023, followed by Ukraine and Jordan. The insights

gained from the pilot in Lebanon provide valuable lessons on both the opportunities and risks linked with digitising legal aid programmes in humanitarian contexts.

The potential reach of digital legal aid platforms

Digitalising legal aid services presents a distinctive opportunity for humanitarian actors to amplify their impact by expanding their reach, eliminating access barriers and enhancing the timeliness of communications.

The traditional methods of information provision[2] by NRC's legal aid teams involve in-person travel by staff or volunteers to community centres, mosques and churches to hold group information sessions for 20-40 people at a time. In comparison, KOBLI-Lebanon reached an estimated[3] 75,000 unique individuals through its website in 12 months and 15,000 individuals through its WhatsApp channel in six months.

In the web development industry, a user whose visit lasts more than one minute is considered an active user. On average KOBLI-Lebanon visitors spend 2.5 minutes on the website, explore five pages and return to the platform three times, indicating sustained engagement. Furthermore, a phone survey conducted with over 500 users of KOBLI in Lebanon, found that 99% were satisfied with the legal information provided on the platform and would recommend the platform to others.These metrics demonstrate the active participation and engagement of online users and underscore the positive reception of the digital approach by the target population.

Navigating access challenges

Despite its potential for widespread reach, digital legal aid is only available to individuals possessing a minimum level of tech literacy, access to the internet and a digital device, such as a smartphone. Depending on the displacement context, significant numbers of people may not meet these conditions. However, this critical fact might be obscured by reports showcasing an increase in the overall number of people reached after the adoption of digital modalities. Consequently, there is a risk of excluding the, often more vulnerable, populations without access to and knowledge of technology.

Hence, while digital tools offer invaluable access to legal support, it is vital to consider the unequal access to technology and connectivity among displaced individuals. Such consideration necessitates a programme design where digital and in-person methods complement each other.

At NRC, the strategy involves utilising digital approaches to address less complex legal issues faced by less vulnerable individuals. By doing so, we aim to redirect our staff's focus toward the more complicated legal challenges encountered by the more vulnerable. Tech suitability assessments enable informed decisions about each service modality's role in the legal aid programme. These assessments are guided by considerations of access, knowledge and preferences within the target population.

KOBLI's pilot in Lebanon was heavily influenced by the tech suitability assessment conducted beforehand. The survey showed that while over 90% of refugees had access to the internet, only 38% of respondents preferred to receive legal information through the internet (others preferred in-person or telephone modalities), and 63% stated they were comfortable with using the internet. Furthermore, among those with access to the internet, only 50% of the respondents had full access, with 42% only being able to use WhatsApp. As such, the ICLA-Lebanon programme uses KOBLI to complement its in-person assistance and helpline. The KOBLI WhatsApp channel

was launched four months after the website to accommodate those with access to WhatsApp only.

The digital approach necessitates a proactive effort to attract a diverse audience. The pre-launch tech suitability survey[4] revealed comparable levels of technology access and literacy among both males and females. However, the demographic data of our online visitors exhibited a notable bias towards male visitors, with 72.5% being male in January 2023. Whether this imbalance resulted from biases in online advertising campaigns on platforms like Facebook and Google or simply because KOBLI's content attracted more males than females, it posed a concern. We addressed this by implementing targeted ads for female audiences. Consequently, by November 2023, the gender distribution among our visitors became more balanced, with 51% being male and 49% female. Similar improvements were achieved for underrepresented refugees in particular geographical areas.

How digital platforms can support safety and dignity

The digitalisation of legal aid services can play a key role in mitigating some safety and dignity concerns. It serves as a secure alternative, particularly when safety risks such as checkpoints, lack of civil documentation, or other restrictions associated with traveling to humanitarian service facilities affect displaced individuals or when substantial inconvenience, such as long traveling time, impedes access to aid facilities.

Furthermore, digital tools can be an effective way for humanitarian organisations to combat misinformation, especially since the internet is often the breeding ground for such content. They enable the timely dissemination of crucial and accurate information to communities. By leveraging digital tools, humanitarian actors can effectively address and counteract the spread of false information, enhancing the overall information landscape in a timely and targeted manner.

Finally, the anonymous nature of digital platforms in legal aid can significantly benefit marginalised groups, particularly those facing circumstances where seeking assistance might lead to stigma or additional risks. For example, individuals seeking legal aid for divorce proceedings may fear social disapproval, retaliation, or potential harm if their actions are discovered. Additionally, in some contexts, there is a stigma attached to receiving assistance from Global North NGOs. Digital modalities offer a layer of confidentiality and privacy that is not always possible in traditional face-to-face interactions. By accessing legal aid anonymously online, these individuals can seek crucial assistance without the fear of being identified or judged within their communities. This anonymity encourages and empowers them to take the necessary steps to secure legal support, ensuring their safety while addressing their legal needs.

Risks: accuracy, safety and dignity in digital legal aid services

While digitalised legal aid programmes address some safety risks tied to physical services, they bring forth their own set of risks. The expansive reach and speed of digital tools are advantageous for amplifying valuable information, but they can similarly magnify errors and inaccuracies that are inadvertently made. Correcting mistakes is more complicated in the online setting with anonymous users. Furthermore, indiscriminate access to information may pose challenges in situations where a thorough assessment of the applicability of the law to the specific situation is required.

Finally, digital assistance may be perceived as less respectful than in-person legal aid. For example, the use of chatbots or messaging apps to answer legal questions could appear more distant, detached and impersonal.[5]

To maintain a high quality of digital legal aid, risks related to safety and dignity should be properly assessed, monitored and mitigated. Many of the concerns above can be avoided. A proper procedure for the development, review and publication of content will reduce the chances of mistakes and errors. A thorough legal and case analysis should be integrated with keeping the content up-to-date. Any errors can be promptly addressed when there is a clear channel for reporting. The developed procedure should assign responsibilities to individual team members not only to develop content but also to regularly ensure their relevance and accuracy.

Moreover, it is imperative to incorporate a seamless integration between digital and in-person responses. A notable example is the design of the KOBLI chatbot and Guide Path pages, which not only provide automated assistance but also enable users to connect with a real person at any point for further clarification and a deeper understanding of their legal queries. In KOBLI-Lebanon, 5% of KOBLI visitors (about 200 per month), used one of the KOBLI channels to get in touch with legal aid workers.

How digital platforms can support inclusivity and empowerment

The digitalisation of legal aid services, with an emphasis on the development of self-help tools, enables individuals to navigate legal scenarios independently and decide on the best course of action after weighing their options. In fact, the adoption of digital platforms has the potential to democratise access to legal information for displaced populations, thereby breaking down traditional barriers and creating a more inclusive and equitable legal landscape that empowers individuals to navigate complex processes, make informed decisions, and advocate for their rights. This, in turn, ultimately fosters greater resilience and self-determination within displaced communities.

Additionally, by fostering both active engagement with users and the passive monitoring of behavioural patterns, digital tools can play a pivotal role in reducing barriers to participation. These tools create accessible channels for interaction, providing refugees with opportunities to voice their concerns, share experiences, and actively participate in decision-making processes. At the same time, the digital analysis of the data enables programme designers and stakeholders to tailor initiatives effectively, ensuring that support programmes are precisely aligned with needs. In essence, the integration of digital tools not only facilitates engagement but also streamlines the process of data analysis, resulting in more targeted and responsive programmes that contribute to the overall empowerment of displaced populations.

Risks associated with the interpretation of data collected through digital channels

Digital tools offer a convenient means of connecting with displaced populations and understanding their challenges and needs. However, it is crucial to approach the data collected with caution to avoid potential misinterpretations. Firstly, it is important to recognise that online users might not fully represent the entire target population, and their perspectives may not encapsulate the diversity of experiences within that group. Secondly, interpreting the data derived from analytics requires robust methodologies to ensure that insights drawn from the data are

accurate and aligned with the actual context. This will prevent misleading interpretations and allow for a more comprehensive understanding of the displaced population's needs and challenges.

KOBLI is equipped with analytical tools that provide our digital legal aid team with insights into the most visited themes and topics. The chatbot analytics reveal the selected conversation flows and the extent of user engagement. However, it is essential to note that not every interaction is captured by analytical tools; for instance, when users deny permission for the platform to collect cookies. Additionally, not every interaction should be considered a genuine expression of interest in topics.

Take, for example, the employment law section on the KOBLI-Lebanon website, covering issues such as obtaining work permits and negotiating contracts. While this section receives a high number of visits, suggesting high interest, a closer examination of the data reveals low visit duration and interaction levels. This could be attributed to visitors landing on the KOBLI employment law page while searching for employment opportunities. To better identify the subset of users who truly engaged with the material, KOBLI-Lebanon adopted a policy that only visitors meeting a minimum engagement level (e.g., duration of visit and number of clicks) are included in the analytics. This approach enhances the accuracy of data, allowing for more informed decisions in content planning and updates.

Conclusion

In conclusion, the digital evolution of legal aid, exemplified by initiatives like KOBLI, introduces a significant paradigm shift in humanitarian assistance. While digital platforms offer expanded reach and operational efficiency, it is crucial to acknowledge and address challenges, including unequal access and potential risks to safety, accuracy and dignity. The experiences shared in this article, particularly the insights gained from KOBLI's implementation in Lebanon, underscore the importance of a thoughtful and balanced approach. This discussion highlights the delicate equilibrium required to harness technology's potential for empowerment while upholding ethical considerations.

In 2024, while KOBLI will continue to grow internally among NRC country offices, such as Iraq, Palestine, Egypt and Moldova, NRC is exploring opportunities to scale up sustainable access to the KOBLI platform for partners and local NGOs. This endeavour reflects a commitment to harness the transformative role of digital innovation in the humanitarian sector, aiming to enhance the accessibility and quality of legal aid for displaced populations.[6]

Amir Shiva
Global Project Manager for Digital Transformation of ICLA at NRC
Amir.shiva@nrc.no
linkedin.com/in/amir-shiva-b9a73b29/

1. *lebanon.kobli.no/en/page/AboutUs*
2. *NRC-ICLA provides legal aid through three main modalities, which differ based on their level of engagement with the target population: information provision, one-to-one counselling and legal assistance which covers legal representation.*
3. *The estimation accounts for the individuals who visit the website but reject cookies, and as such, their visit is not recorded by analytics tools. Different sources have different estimates of the number of users who reject cookies but conservative numbers are around 40%, which is adopted by KOBLI.*
4. *To access the full tech suitability assessment, visit this link: https://howto.kobli.no/en/page/TechSuitability*
5. *Two critical topics – data protection and the utilisation of artificial intelligence in digital legal aid – demand in-depth discussion that exceeds the confines of this article. With respect to data protection, the KOBLI team ensures the security of the platform by conducting frequent penetration tests and security audits. KOBLI upholds the highest privacy practices including compliance with General Data Protection Regulation (GDPR) in the EU.*
6. *With great appreciation for the support of Katrien Ringele, ICLA Global Lead; Martin Clutterbuck, ICLA Regional Adviser in MERO, and NRC-ICLA team in Lebanon.*

Structural barriers to the digital platform economy for forcibly displaced workers

By **Kathryn McDonald**

Regulatory vacuums contribute to the structural exclusion of forcibly displaced populations seeking work on digital labour platforms. Even where these issues can be overcome, questions remain as to the viability of these platforms as a path to economic empowerment.

Digital labour platforms have become increasingly prominent in the global labour market over the last decade. There are now over 700 unique digital labour platforms (DLPs), providing opportunities to an estimated[1] 50 to 150 million workers globally.

DLPs are characterised by a low barrier to entry, directly connecting clients in need of services with workers able to provide them, and organising work on a casual, piece-rate and temporary basis. This format can present opportunities for workers unable to secure stable, long-term employment.

Around the world, governments are embracing digital labour as part of an economic development strategy, focusing on its potential to bolster growth and featuring DLPs in their development plans and policy frameworks. Increasingly, such plans include forcibly displaced populations as groups that could benefit from the expansion of platform-based work. This has resulted in the convergence of development and humanitarian infrastructures, with actors like the UN, World Bank and Rockefeller Foundation promoting DLPs to displaced populations to ease economic strain on host economies and humanitarian support systems, and allow refugees to earn a living, integrate into host countries' economies and promote self-reliance.

Initiatives to integrate displaced people into the digital economy are a response to the constraints these populations face in accessing employment and income-generating opportunities. Though the right to work for refugees is established in the 1951 Refugee Convention and the Economic Covenant (ICESCR), in practice many host countries limit this right. Exclusion from certain industries, discriminatory practices, requirements around work permits, and policies restricting mobility keep refugees from attaining employment. Refugees in camp settings are further constrained by geography and limited resources. Amidst persistent labour market challenges, DLPs offer possibilities for economic inclusion for displaced people who face structural and practical barriers to exercising their right to work.

However, this model may be unsustainable – DLPs are associated with non-standard, informal and unregulated forms of work with persistent decent work deficits. DLPs may exacerbate existing social inequality and economic divides, compounding market frictions that result in inferior outcomes for already disadvantaged groups. Critics warn[2] that although these platforms can provide opportunities, they do so by tapping into a "readily available supply of migrant labor to service market demand, [...] extracting

surplus value by keeping labor costs low and providing minimal labor protections."

Issues related to 1) access and infrastructure and 2) status and rights, form the greatest structural challenges impacting workers in the platform economy. This article will address how these challenges create risks for forcibly displaced people engaging in platform work, highlight existing initiatives addressing these barriers, and propose good practices for practitioners working with displaced populations in the platform economy.

The challenges related to working on DLPs are intersectional. If DLPs are to benefit displaced people, it is essential to address their implications on issues like job quality, economic integration and livelihoods. Understanding the nature of these challenges can help advocates and organisations better serve these groups and facilitate their access to digitally-mediated opportunities.

Access and infrastructure

The most prevalent barriers affecting forcibly displaced people in the digital economy are linked to exclusionary requirements around formal identity recognition, which create challenges around access to financial services, digital connectivity and tools of work.

To access work on DLPs, platforms typically require workers to verify their identities by providing government-issued documentation. But in many cases, forcibly displaced people may not have access to credentials like national ID cards and passports. It is common for forcibly displaced people to lack such documents either because they never had them or because they were lost, seized or destroyed during displacement. Additionally, workers from countries subject to sanctions may be barred from accessing DLPs, and in cases like Syria, this can exclude millions from the platform economy.

Refugee ID cards, provided upon registration in host states, often do not enable the same levels of access to work and services as standard ID cards and are typically temporary. Some platform workers have had their platform accounts frozen after their IDs expired.

Identity documentation is also a precondition for accessing financial infrastructures, necessary for engaging in platform work. Both formal banks and mobile money programmes require identification documents to open accounts. This is important because platform workers will need a verified financial account to receive payments from platforms. Half of the global refugee population live in host countries that restrict their access[3] to bank accounts, thereby imposing barriers to livelihood opportunities.

Documentation issues also pose barriers to workers' abilities to access digital infrastructures. SIM card registration yields unique access challenges for displaced populations. Increasingly, governments are imposing regulations requiring that users provide legal IDs to purchase SIM cards. In 2021, 157 countries[4] had enacted mandatory SIM registration regulations and refugees have identified ID requirements as being a significant barrier to digital connectivity.

Initiatives aimed at improving access to digital labour platforms

Within the humanitarian-development-platform nexus, we find examples of practices and programmes attempting to mitigate access-related challenges by helping workers navigate barriers to entry and providing infrastructure. Some platforms have built lower-tech ways for workers to

access platforms, involving cash exchanges and face-to-face registration for platforms. While these measures provide ways around barriers to inclusion, they are not durable solutions and may limit long-term growth and the ability to operate at scale.

The cost of digital tools like laptops and smartphones is another significant barrier for refugees in the digital economy. Some refugee-focused programmes attempt to mitigate these barriers by facilitating access to platform work opportunities and providing infrastructure. For example, the Refugee Employment and Skills Initiative[5] (RESI), a programme funded through the Norwegian Refugee Council and the International Trade Centre was established in 1997 and began offering services in 1998, operating out of Dadaab and Kakuma camps in Kenya. RESI provides programme participants with laptops, high-speed internet and co-working spaces, as well as digital skills training regarding online work. RESI has also negotiated agreements directly with DLPs, resulting in their accepting alien ID cards, commonly used by refugees, for platform registration. These negotiations enabled 250 programme participants across both camps to begin working on platforms, though they did not address the eventual expiration of these documents. Staff have noted larger barriers related to the continuation of programme funding, the willingness of participants to assume the risks associated with platform work and the ability of workers to continue work independent of the programme's support.

These issues highlight the need for coordination and dialogue between platforms, governments and development actors to create policies that reflect the experiences of displaced people and the constraints of refugee assistance infrastructures. Policies that facilitate uninterrupted access to services for FDPs will enable them to effectively engage in income-earning opportunities in the platform economy.

Status and rights

Currently, digital labour platform work is poorly integrated into existing social institutions and regulatory frameworks, leaving workers without adequate coverage vis-a-vis employment standards, social benefits and workers' rights legislation. This is largely because platforms categorise workers as 'self-employed,' 'contractors' or 'entrepreneurs,' which has implications for the effectuation of basic rights. Whether platform workers are truly self-employed is a question of extensive debate.

Most jurisdictions extend labour and employment-related rights only to formal employees. When platform workers are treated as self-employed, they experience decent work deficits and an absence of many fundamental rights at work, such as stability and security of work, equal opportunity and treatment, safe work environments, social security and the right to organise and collectively bargain.

The complexity of these issues is compounded for displaced people who may face legal exclusion and discrimination in host countries, presenting additional challenges to effectuating their rights in the platform economy. UNHCR reports[6] that 70% of refugees live in countries that restrict their right to work.

The lack of clarity around platform workers' employment status and rights has been argued to both benefit and constrain forcibly displaced people. The regulatory vacuum may actually extend opportunities to displaced people because, if they cannot obtain work permits in host countries, they can slip into the informal and unregulated

platform economy. Some platforms[7] have actively lobbied against regulation and formalisation on the grounds that the "reclassification of platform labour as employment would make it more difficult, and in some cases impossible, for refugees to access this type of work."

On the other hand, advocates warn of the perils of this approach and its impacts on vulnerable workers. Where access to decent, formal work arrangements is limited, forcibly displaced people are more likely to accept informal, precarious and hazardous arrangements to support themselves and their families. Informal workers are more vulnerable to shocks like medical emergencies, economic downturns and market fluctuations.

In the absence of systematic regulation, DLPs use Terms of Service agreements with workers to govern working conditions. Platforms retain the right to deactivate and otherwise penalise workers' accounts at will, offering few mechanisms to contest these decisions. The threat of deactivation and the opaque nature of platform management creates a power imbalance. This leaves workers guessing how to best navigate platforms and frequently compels them to accept unfair or unsafe conditions. Consequently, decent work deficits are prevalent in the platform economy and risks for platform workers are exacerbated by the absence of statutory protections which ensure their fundamental rights.

Initiatives to promote decent work in the digital platform economy

The question of how to promote decent work in the platform economy is a subject of ongoing debate amongst stakeholders. There have largely been two approaches: formalising platform work, and voluntary regulation and social impact enterprises.

Some jurisdictions use novel classification structures to regulate work that is not easily categorised as employment or entrepreneurship. In the United Kingdom, the union for professional drivers, the GMB, successfully pursued[8] reclassification claims on behalf of 30,000 platform-based drivers, arguing the group rightfully belong to UK labour law's 'worker' category. Gaining this designation gave these drivers access to basic employment provisions (e.g. minimum wage, guaranteed breaks and holiday pay).

However, this category does not confer protection against unjust dismissal or guarantee the right to work, presenting further risks to workers. Over 66 arrests and ten deportations have been reported in the UK of platform-based drivers who were 'found to be working illegally.'[9] While platforms claimed to vet each driver with regard to their right to work, these workers were still placed in a precarious situation due to the legal ambiguity that surrounds platform work.

When it comes to formalisation, rather than relying on legal loopholes to include displaced workers, interventions should focus on integrating DLPs into regulations that provide all workers, including refugees, with fundamental rights. This approach has the potential to formalise platform work, and facilitate legal, social and economic integration for forcibly displaced people if regulations are enforced.

Voluntary measures, undertaken by individual firms, have also addressed status-related issues and decent work deficits in the platform economy. Specifically, some platforms have developed business models that improve pay, work-life balance, skills development and the power imbalance between platform operators and workers. These 'social impact platforms' aim to provide better conditions regardless of employment status,

with many specifically targeting displaced and otherwise marginalised workers.

An example of such a platform is 'Digital Lions'[10] – a World Fair Trade Organization-verified 'fair trade digital agency' offering web development, graphic design and video and animation services. They promote 'sustainable jobs' by implementing decent work standards like fair pay, non-discrimination, gender equity and good working conditions, and explicitly aim to employ workers from underserved communities.

Another socially-minded platform, Humans In The Loop,[11] engages with displaced communities in Türkiye, Iraq and Syria, for work like annotation and AI data training. In 2019, they contracted 167 workers. They are notable for their explicit aim to provide fair working conditions. Humans in the Loop has used its experience in supporting workers with refugee backgrounds to develop a Fair Work Policy that could be adapted by other platforms. Some of their commitments to workers include paid training, wage levels at or above national standards and opt-in health and accident insurance.

Conclusion

Research demonstrates that DLPs present both opportunities and risks for workers, and that for forcibly displaced people, existing risks can be exacerbated. Harnessing the potential of platform technologies requires robust policy solutions around access and status-related challenges, and the development of programming and resources aimed at building workers' capacity to effectively navigate online labour markets.

Humanitarian and development organisations operating in the platform space have typically focused on issues of inclusion and mitigating barriers to entry for displaced workers. Structural barriers, precarious working conditions and a lack of protections have been more difficult to address because these organisations lack the power to shape policy and influence stakeholders.

If this form of work is to be part of the solution to the economic inclusion of displaced populations, it is critical to promote an enabling environment to support the effective realisation of workers' rights. Ensuring that platforms offer decent work opportunities requires that all workers, including forcibly displaced ones, have and can exercise their fundamental rights irrespective of their refugee status or employment classification.

Regulation, formalisation and social dialogue are possible and critical, but will only be effective if forcibly displaced people are actively involved and if policies are designed to reflect the barriers they face and plug the structural gaps that deepen their vulnerability in the gig economy.

Kathryn MacDonald
kthryn.mcdnld@gmail.com

1. *bit.ly/promise-peril-online-gig-work*
2. *bit.ly/gig-work-migrant-work*
3. *bit.ly/unhcr-refugees-access-jobs-financial-services*
4. *bit.ly/gsma-access-mobile-services-proof-identity*
5. *bit.ly/intracen-resi-refugees-kenya-market*
6. *bit.ly/unhcr-livelihoods-economic-inclusion*
7. *bit.ly/ips-ukrainian-refugees-deserve-decent-work*
8. *bit.ly/ilo-representation-voice-bargaining-gig-economy*
9. *bit.ly/delivery-riders-London-clampdown-illegal-workers*
10. *digitallions.co/*
11. *humansintheloop.org/*

Inclusive and dignified digital work: linking markets and displaced people

By **Andhira Yousif Kara, Lorraine Charles, Giselle Gonzales** and **Selen Ucak**

A team of four experts – with experience upskilling refugees, facilitating job linkages, impact investing, researching economic inclusion, and lived experience as a refugee – discuss the barriers that displaced people face in accessing digital work and how these can be overcome.

Digital work is, in theory, a win-win for refugees and the host community. Refugees are able to earn money without competing with the host community for local jobs and companies are able to achieve diversity in their workforce. However, displaced people often face significant barriers to accessing formal and informal work in the digital sector, from getting market-relevant upskilling, to accessing paid opportunities after training, to unlocking capital to fund digital livelihoods. This article considers how these challenges can be addressed.

Andhira's experience with digital skills and work

I am a Sudanese refugee who has been living in Kenya for the past 20 years. For protracted refugees like myself, job training is often considered a key to unlocking opportunities, and digital work presents a more accessible and inclusive alternative to formal employment that requires fewer permits. So, I was keen to undertake training that might lead to job opportunities in this area.

My experience began with a month-long digital training offered by a non-profit organisation working with refugees. The training focused on basic computer skills and creating profiles on popular digital freelancing platforms. Although this was a promising opportunity, I struggled to secure a job online for six months as I required more than just basic computer skills. Furthermore, beyond the widely-recognised infrastructural challenges (such as needing a computer, reliable internet and electricity, and a payment account/platform – none of which was supported as part of the programme) I needed more advanced digital skills or specialised skills in transcription, translation or academic writing competencies to secure at least my first job and start building a strong profile.

Building skills for digital work

As Andhira's experience demonstrates, refugees seek employment in digital work to overcome restrictions on their rights to work locally and to access wider opportunities. Yet many lack the necessary skills, networks and sector knowledge to obtain income through online work. Developing skills for refugees to navigate the digital economy is essential to advance and sustain careers across geographic borders in the face of legal, logistical and attitudinal hurdles.

There is a global demand for workers who have both technical digital expertise and non-technical skills, or soft skills. Occupations that are predicted to grow[1] are disproportionately among those that require a high level of education and intensive skills in social and interpretative tasks. Growth will be seen in cutting-edge industries,[2] such

as AI and machine learning specialists, sustainability specialists, information security analysts and fintech engineers. This is backed up by data from freelancing platforms[3] where IT jobs such as machine learning, automation specialists and data analysts have seen significant growth in demand.

A need for non-technical soft skills

According to the World Economic Forum, the skills that employers perceive as most important for the jobs of the future are cognitive skills – analytical and creative thinking, self-efficacy, resilience, flexibility and agility (which many refugees possess due to their experience of displacement), motivation and self-awareness, and curiosity and life-long learning. In fact, within the global workforce, the talent gap in soft skills is more pronounced than in technical digital skills.

To take advantage of the opportunity to engage in digital work, refugees need to be equipped with these non-technical skills, plus know how to communicate and collaborate in a virtual setting, with an understanding of different work cultures. The focus on soft or non-technical skills is often overlooked in training curricula. Organisations such as **Na'amal**,[4] which support refugees through training and mentorship with a focus on soft skills and remote work, can help connect forcibly displaced people with opportunities. Na'amal also works with partners to address and advocate for improving access to digital infrastructure.

Missing market linkages for upskilled displaced talent

Yet, even with all the right market-driven training, one critical gap remains: market linkages between refugee talent and employers. Graduates from programmes by organisations supporting displaced communities face countless invisible barriers to accessing sustainable opportunities online.

Platform-enforced geographical restrictions exclude displaced and local communities from many popular freelancing and payment platforms that international businesses rely on to find, employ and pay skilled workers. This disproportionately impacts countries with the highest rates of displaced communities. Without this access, both refugees and locals struggle even to be considered for work, let alone bid for and secure opportunities. Even in host countries not blocklisted by platforms, talented individuals may not be found and trusted in an already competitive online labour market. Achieving refugee employment in the digital economy at scale will require deliberate and targeted market linkages. One way to encourage these linkages is by working within the private sector itself to redirect existing demand to an otherwise overlooked supply of talent.

How impact sourcing policies can encourage the recruitment of displaced people

While recruiting platforms and corporate networks exist to provide refugees with formal employment, there remains an underleveraged opportunity to connect refugee talent with fair freelancing projects via impact sourcing.[5] First formalised as a concept in 2013 by the Rockefeller Foundation, impact sourcing is "an inclusive employment practice through which companies in global supply chains intentionally hire and provide career development opportunities to people who otherwise would have limited prospects for formal employment."

Procurement processes for digital services are already a normal part of operations for enterprises, small and medium-sized businesses, start-ups, NGOs, and even

government organisations. In many cases initiatives around diversity, equity, inclusion and social impact already exist to source work to under-represented communities. So, without needing to change market behaviour, existing corporate practices and outsourcing projects can be leveraged to funnel work to talented displaced people.

Governments are increasingly introducing reporting requirements for companies to show social value through the goods and services they purchase, and are requiring their own public bodies to do the same. By sourcing work to organisations that support the employment of refugees, businesses can meet their social impact commitments, enhancing their competitiveness to secure contracts with business or government and to meet investor demands.

Connecting displaced people with dignified digital work

How can the private sector connect with talented displaced people? There is a role for intermediary organisations with the capacity to connect enterprises, start-ups, small to medium businesses, NGOs, or governments with talented teams from refugee communities and host communities. One example of such an organisation is **EqualReach**,[6] a social enterprise founded by co-author of this article Giselle Gonzales. Giselle identified a market demand for trusted contingent workforces, based on practices she observed in the private sector while working with Fortune 50 companies.

EqualReach connects vetted freelancing teams of displaced individuals who can work on digital projects with companies in the private sector. These teams can work on projects that require a wide range of skills. For example, one company is working with EqualReach on two projects: (1) process automation involving web development plus DevOps engineering and (2) low-complexity web research. This work is being delivered by two reliable, skilled teams in Ethiopia and Kenya, through EqualReach's trusted delivery partner, Na'amal, enabling workers to earn 4-10x higher wages than comparable opportunities available to refugees in the region.

Teams are identified by vetting and partnering with (1) refugee-led organisations, (2) social enterprises, and (3) NGO/government initiatives that are already supporting displaced and host communities with upskilling, infrastructure/digital access, mentorship, career guidance and navigating local regulations with hyper-local expertise.

EqualReach presents a curated selection of teams for businesses to choose from (pre-vetted for the requirements of a project), and facilitates the contracting, payments, and communication from start to finish. This removes many of the barriers refugees typically face securing work with international clients, while positioning talented displaced people as the primary customers to avoid exploitation and maximise the earnings they receive.

Unlocking capital for digital livelihoods

Innovative social enterprise models facilitating private sector engagement and companies that employ and source from refugees – especially those led by displaced communities – need investment to maximise the potential of digital work, but often face barriers to secure financing. The growing field of 'refugee lens investing' is well-positioned to mobilise impact-aligned capital to address this challenge while reducing the pressure on humanitarian funding needs and filling the gaps left by traditional investments.

The **Refugee Investment Network**[7] (RIN), the first blended finance and impact investing collaborative dedicated to solutions in global forced displacement, has developed a

refugee lens investing (RLI) framework[8] for this purpose. The lens enables investors to assess and track investments that advance refugee self-reliance. It includes investing in 'refugee-supporting companies,' i.e. those that intentionally offer employment to refugees, including digital jobs, or source from companies that do so.

Tim Docking, CEO of RIN, explains: "Through our RLI market analysis in East Africa, we have found that some of the best examples of refugee-led and supporting enterprises leverage the internet, with lower start-up costs and remote work possibilities. Investors are often familiar with tech business models and drawn to them as potential investments."

The investment community can be encouraged to deploy capital through the refugee lens with the provision of robust networks, tools and advice. Refugee-supporting firms can be strengthened to appeal more to investors through technical assistance to develop their capabilities around financial and digital literacy. Creating a robust pipeline of investable enterprises and a steady flow of business proposals and investment pitches is critical to fostering the refugee lens investing ecosystem, as is showcasing success stories.

One example is **Chatterbox,**[9] a UK-based, refugee-founded online language-learning programme for professionals that serves corporate clients while tapping into the talent of refugees and other marginalised communities and bringing them into the digital economy. The company has been backed by investors in Europe and Silicon Valley for its impact as a social enterprise and its financial viability.

However, traditional venture financing may not always align with digital livelihood projects in displacement and emerging market contexts. Blended capital, development finance and innovative approaches, such as outcomes-based financing, can help reduce perceived risks and align investor interest with local social impact.

Other examples of impact enterprises which provide jobs in the digital economy for refugee workforces include **Natakallam,**[10] a language learning and translation platform; **CONCAT,**[11] a web development agency, and **Humans in the Loop,**[12] a company that employs refugees in the Middle East and Africa in data annotation and other AI services.

Humans in the Loop uses its profits to support NGO partners and upskilling. Founder and CEO Iva Gumnishka explains: "We considered raising dilutive investment, but we couldn't get a good valuation from traditional and impact investors". Her comment highlights the need for capital on a wide spectrum of return and impact expectations to scale-up effective social enterprises in this space.

In addition to investing in employment models, ecosystem-building impact investments that increase digital literacy, enable financial inclusion and build the necessary digital infrastructure are important for supporting digital livelihoods. Investing in digital livelihoods with a refugee lens contributes to "promoting inclusive and sustainable economic growth, employment and decent work for all (Goal 8 [of the Sustainable Development Goals])" and supports the SDG Digital Acceleration Agenda.[13]

The way forward

While digital work presents an alternative for decent livelihood creation for refugees, the reality involves many invisible challenges. This includes lack of proper digital skills training – including advanced skills like

web development, programming and data science – as well as soft skills, language skills and career coaching. Along with transferable skills, refugees need access to professional networks, the opportunity to gain confidence and experience for improved employment, and be inspired to pursue higher goals in a positive social environment. Most importantly, initiatives that create market linkages to connect forcibly displaced people with dignified digital work and unlock capital to invest in relevant social enterprises and businesses are necessary.

In order to drive financial sustainability, lasting social impact, and fair and scalable employment, there is a need to:

- provide demand-driven training that covers both technical and non-technical skills and allows talented displaced people access to decent and dignified livelihoods that align with their aspirations;
- support fair marketplaces and refugee-employing intermediaries that connect global clients to talented displaced people via impact sourcing for contracts that enable individuals to gain experience and earn globally competitive incomes;
- mobilise the private sector and impact capital through a refugee lens, with financing that can seed innovative models and scale local enterprises that employ and source from refugees, to enable economic inclusion and self-reliance, and
- continue building public-private-and-philanthropic partnerships to invest in digital infrastructure, from computers to internet service, and increase access to refugee and host communities.

This multifaceted approach, engaging diverse stakeholders – from community organisations and entrepreneurs to corporations and funders – will create inclusive online economies that benefit both forcibly displaced people and their host communities.

Andhira Yousif Kara
Consultant Researcher and Refugee Advocate
annkakaliya@gmail.com
linkedin.com/in/andhira-kara-a72121a1/

Lorraine Charles
Executive Director of Na'amal and Research Associate, Centre for Business Research, University of Cambridge
lorraine@naamal.org
linkedin.com/in/lorraine-charles/

Giselle Gonzales
Founder and CEO of EqualReach
giselle@equalreach.io
linkedin.com/in/gisellegonzales/

Selen Ucak
Entrepreneurship Lead at Refugee Investment Network and Impact Consultant
selen.ucak@refugeeinvestments.org
linkedin.com/in/selenucak/

1. *bit.ly/ILO-digitalization*
2. *bit.ly/future-of-jobs-report-2023*
3. *bit.ly/in-demand-skills-2024*
4. *naamal.org/*
5. *bit.ly/transformational-change-cooperation*
6. *www.equalreach.io/*
7. *refugeeinvestments.org/*
8. *bit.ly/refugee-lens*
9. *www.chatterbox.io/*
10. *natakallam.com/*
11. *concat.tech/*
12. *humansintheloop.org/*
13. *www.sdg-digital.org/accelerationagenda*

The digital exclusion of refugees and IDPs in Sudan

By **Wala Mohammed**

Being left behind in a digital world can be devastating for forced migrants. This article reflects on the digital exclusion that refugees and internally displaced persons (IDPs) face in Sudan due to the repercussions of ongoing restrictions on accessing technology.

The civil war in Sudan, which began in April 2023, has displaced more than 8 million people.[1] As a result of this devastating conflict, acute food insecurity, disease outbreaks, civilian displacement and livelihood destruction, the entire country is in a state of near collapse.

Millions of Sudanese people have lost their livelihoods due to the conflict. The war has halted production and destroyed human capital and state capacities. Moreover, it has impacted financial stability by bringing down commerce, financial, and information and communications technology services. Data centre operators have lost access to their data and facilities, causing several essential internet-related services to go down. Sudan's Internet Society chapter reported[2] that only 12% of Sudan's .sd Country Code Top Level Domain websites and services were functional as of June 16, 2023.

Before the war, the informal sector comprised nearly 60% of the workforce; since war broke out many have lost their livelihoods and have no form of social protection. The number of children out of school[3] has also increased from seven million to 19 million.

The connection between economic sanctions and digital exclusion in Sudan

The undertaking of economic and trade sanctions impedes the free flow of digital communications and technologies that activists, innovators and ordinary users of these technologies so desperately need.

Sudan has been isolated from the international community since 1993, when it was designated a state sponsor of terrorism by the US government. In 1997 the US issued an executive order imposing comprehensive economic sanctions on Sudan. An international license issued by the US in 2015 for access to certain software, hardware and services related to personal communication alleviated the sanctions to some degree but some service providers chose not to apply for the relevant licenses to export services to Sudan because obtaining them could be difficult and required periodic renewal.

The sanctions around communication technologies were lifted in 2015, the trade embargo was lifted in 2017, and Sudan was removed from the State Sponsors of Terrorism list in 2020. Despite this, Sudanese people's access to technological and financial services remains limited. There is a long list of software, technology and equipment that are still restricted. Furthermore big tech

companies do not include Sudan on their lists of regions that can access services such as Google Workspace, Microsoft Azure, Azure Government and Microsoft Office 365, as well as online courses, platforms and other global services.

The exclusion of the whole nation from accessing wider opportunities to generate income during the ongoing war in Sudan will push more families below the poverty line.

The digital exclusion of IDPs and refugees in Sudan

In Sudan,[4] a protracted economic crisis is accompanied by pre-existing conflicts in some regions. Before April 2023, 15.8 million people were in need of humanitarian assistance; at the time of writing the number in need of humanitarian assistance had grown to 24.8 million with eight million people forcibly displaced as a result of the current war.

Digital labour platforms offer one means by which displaced people can establish a livelihood. They are particularly beneficial to groups of workers who have traditionally been disadvantaged and faced barriers to accessing the labour market,[5] such as women, disabled people, young people, refugees, migrants, and people of minority racial and ethnic backgrounds. But, displaced people in Sudan face major challenges in joining digital labour platforms, due to the isolation of banks in Sudan from the international banking systems, as well as Sudan not being listed in most of the digital labour platforms such as Upwork and Fiver. Some platforms stipulate in their terms of agreement that they do not permit people from countries that are subject to sanctions to register.

Refugees and other forcibly displaced persons around the world face challenges accessing basic services[6] involving technology, such as SIM registration, mobile phone connectivity and bank accounts, and Sudan is no exception. The requirements outlined in the country's laws and regulations on anti-money laundering and countering the financing of terrorism create legal barriers for refugees and asylum-seekers in accessing formal financial institutions, mobile money and other digital financial services. These problems are interconnected. Not having a place to put their money makes forcibly displaced people very vulnerable.

Sudanese law requires SIM cards to be registered using a recognised identity document (ID). Currently, Sudanese refugee ID cards do not meet the identity requirement to register a SIM card. Many refugees and asylum seekers gain access to SIM cards through friends and family members who have an acceptable form of ID, others through mobile network operator agents, and others through humanitarian organisations that distribute SIM cards registered in bulk under their name.

Although there are formal and informal workarounds to the SIM registration requirement as well as for accessing financial services, including mobile money, these workarounds are inferior to having a legal framework that is open and inclusive. As humanitarian organisations engage in cash assistance, workarounds carry risks and liabilities and discourage true financial inclusion for the affected populations. Thus, economic sanctions can severely affect humanitarian aid funding and delivery in various ways.

Recommendations to improve digital access in Sudan and elsewhere

Restrictions on accessing technology and government policies are affecting IDPs' and refugees' access to online labour platforms, SIM cards and other services. With the

ongoing war in Sudan, there will be an increase in the number of people who need humanitarian assistance while the delivery of aid will be challenging, with many regions becoming inaccessible for security reasons. Increased access to the internet and mobile technology can help marginalised groups to improve their conditions and ability to enjoy their rights, including accessing education, livelihood opportunities and information. The Sudanese authorities should work on facilitating access to SIM cards for refugees and marginalised communities by updating the NTC's General Regulations 2012.

There is a crucial need for warring factions and telecommunications actors to maintain communication networks in times of conflict since disruptions limit citizens' access to information and undermine media freedom and freedom of expression. Furthermore, disruptions hamper citizens' access to essential services and safe havens, as well as hindering the effectiveness of humanitarian efforts.[7]

Political and economic stability is key to addressing developmental and human rights issues in Sudan. The international community must remain committed to ending Sudan's ongoing conflict, promoting peace, freedom and justice, as well as supporting its transition toward a civilian-led government. The repercussions of past sanctions are still being felt, restricting the ability of the Sudanese population to afford and access technologies that contribute to achieving the Sustainable Development Goals. The International Community could learn from this and shift towards using more targeted sanctions on countries in the future. In relation to Sudan, they should also work on easing access to the wider services that are blocked even after the economic sanctions are lifted.

Wala Mohammed
Independent Researcher & Founder of Hopes & Actions Foundation
wala.ahmed@outlook.com
linkedin.com/in/wala-mohammed-b01858ab/

1. *bit.ly/sudan-situation-update*
2. *bit.ly/ongoing-conflict-sudan*
3. *uni.cf/3JzAUEA*
4. *www.unocha.org/sudan*
5. *bit.ly/platform-economy-association-bargaining*
6. *bit.ly/displaced-disconnected-e-africa*
7. *bit.ly/sudan-digital-communication*

Internally displaced and living with relatives in White Nile State, Sudan. Credit: UNHCR/Ala Kheir

Digital refugee economies in Nairobi: opportunities and challenges

By **Marie Godin, Ishimwe Jean-Marie** and **Evan Easton-Calabria**

Drawing on a collaborative and participatory research initiative conducted in partnership with refugee-led organisations – Kintsugi RLO and Youth Voices Community – this article sheds light on the existence, potential and drawbacks of 'digital livelihoods' for refugees.

In recent years, digital work has emerged as a promising avenue for socio-economic development and addressing unemployment issues in both refugee and host communities. Digital labour platforms (e.g. websites helping match workers and clients for tasks performed fully online) and the online gig economy (the economy of flexible, temporary, or freelance work performed online) could hold significant potential for creating new work opportunities, especially for young people.

While increasing attention is paid to digital work for refugees and other displaced people, there is a gap in the recognition of the variety of actors – specifically refugees themselves, including through refugee-led organisations (RLOs) – who support refugees to enter the digital economy. In Kenya, refugees have developed their own digital initiatives, both personally and collectively as digital entrepreneurs. This often occurs through capitalising on their local networks and diaspora connections.

These initiatives are well suited to refugees' needs and realities, offering more flexibility with time and ways to receive payment (as the majority of refugees do not have bank accounts and must find alternative ways to be paid). Increasing discussion and documentation on these refugee-led initiatives, including the impact they have on refugees and their own organisational challenges and barriers, can improve understanding of how digital livelihoods for refugees are fostered, including barriers, successes and outstanding needs. This, in turn, illuminates the potential role of digital work for refugees, particularly as part of local integration.

The digital work landscape in Kenya and its challenges

Examining refugees' engagement in the digital economy in Kenya, including the work of RLOs in fostering digital literacy and access to work, sheds light on how national regulations impact opportunities for entry and sustained involvement in digital work. Alongside being a major refugee-hosting country, hosting over 650,000 registered refugees and asylum-seekers (as of September 2023), Kenya is widely known as the regional ICT hub in East Africa.

Kenya leads regionally in broadband connectivity, general ICT infrastructure, mobile money and mobile banking. Opportunities presented by the digital economy have become the new neo-liberal mantra, with promises of fast, individual success online. To help this materialise, multiple humanitarian and development projects in Kenya have been designed to enable refugees to conduct remote work. One example is the Dutch government-funded initiative PROSPECTS[1] (Partnership for improving prospects for forcibly displaced persons and host communities), which

specifically supports digital employment initiatives and empowerment in different areas of Kenya such as Eastleigh (Nairobi), Turkana and Garissa.

Despite existing initiatives, refugees in Kenya still face challenges accessing decent digital livelihood opportunities, including in the gig economy. The new Refugees Act, which came into effect in February 2022, has been described as progressive by RLOs. On paper, the Act grants more opportunities, rights, protections and solutions for refugees and asylum seekers to integrate socio-economically into the country (see a 2023 report[2] by the Refugee Led Research Hub, Kituo Cha Sheria and RELON-Kenya). In 2023, the Government and UNHCR announced plans to transition refugee camps into integrated settlements that promote socio-economic inclusion. This multi-year plan, known as the *Shirika Plan*, builds on the 2021 Refugee Act and provides refugees with broader rights in Kenya, aiming to enable access to documentation and increase social and economic opportunities for refugees.

However, in reality, the Refugee Act has not yet been fully implemented and significant legal obstacles for refugees persist. For example, despite the government recognising refugee identity documents as legal documents, many refugees attempting to integrate into the digital economy are unable to open bank accounts because their refugee identity cards are not recognised by digital work platforms. Consequently, they are forced to depend on other people with more 'recognised' documentation, such as national ID cards and passports (either locally or transnationally), in order to access their online earnings; this can lead to additional transaction costs. While the Act has only been in force for a year at the time of writing, little tangible progress is apparent. In addition, many refugees must resort to using or even purchasing other people's accounts to access job opportunities. This opens up another range of risks such as wage theft or delays in receiving payments owed. Compounding this, the real obstacles to securing a Kenyan work permit, registering a business and obtaining a Kenya Revenue Authority (KRA) PIN to file taxes mean that the opportunities for refugees to advertise registered businesses online are negligible.

Refugee-led initiatives facilitating access to work online

Despite these significant challenges, there are various refugee initiatives promoting digital work. One workaround refugees have identified to the challenges outlined above is a collective online work account, which (when ethically executed) can pave the way for refugees to build their experience and reputation, earn a substantial income and access mentorship opportunities. This collaborative approach can also foster a supportive environment that assists refugees in navigating the challenges of the digital world. One such example is the work of Mohammed, a Somali refugee, who decided to become an online freelancer in 2018 after growing up in Dadaab refugee camp. Instead of bidding for gig jobs as an individual, he opened up Desert Freelancing Agency[3] on the online work platform UpWork. Opening up this business online was a way to work around the inability to start a legally registered company in Kenya as he is not allowed a work permit. He can now bid for work as a company on the platform and offer these jobs to approximately 50 colleagues in the camp. The company has now grown to offer voice-over, translation, transcribing and writing services, and many refugees now earn a livelihood through it. As Mohammed explained, "Getting a first task, a good job, or even good pay is difficult. But now, through the company, many other refugees are supported and connected to opportunities."

Some RLOs, such as Youth Voice Community (YVC)[4] based in Kayole, a neighbourhood of Nairobi, offer a range of programmes encompassing financial and business literacy courses, training in tailoring skills, and a Digital Literacy Course. YVC places a strong emphasis on livelihoods in all its economic programming, aspiring to not only help refugees gain skills but also to facilitate access to income opportunities, thereby reducing refugees' need for humanitarian assistance. YVC's Digital Literacy Course, 'Digital For Livelihoods', has been a pivotal programme. It initially covered basic computer skills, such as word processing and spreadsheet use, progressing to advanced training relevant to the digital era, such as freelancing, including translation, transcription and writing.

However, although the programme has been running for a year, it has not yet achieved the desired outcomes in terms of access to livelihood opportunities due to the significant challenges that RLOs like YVC face. These include having insufficient funds to deliver a strong curriculum and support the students to access software and learn highly technical related skills that could enable them to access lucrative work in the online gig economy. YVC is now planning to shift from providing digital skills access to ensuring decent work by establishing an inclusive digital incubation centre. This centre, equipped with internet access, computers and disability-friendly infrastructure, will provide refugee youth with the space to work full-time for six to twelve months post-training.

Future directions: digital livelihoods, refugee rights and local integration

Despite forays into the digital realm and visions of success within it, refugees in Kenya remain constrained by limited rights. Our study conducted with refugees in Nairobi indicates that they sought work in the digital economy after many failed attempts to find a job locally. This was due to limited employment opportunities for refugees and systemic challenges, such as lack of documentation and movement limitations, which hinder refugees from exploring a wider pool of opportunities in Kenya and beyond. These and other limitations have pushed many highly qualified refugees to consider alternative economic opportunities such as those available online.

Younger generations of refugees in Nairobi and in refugee camps, who have shifted from the urban informal economy to the digital informal one, often frame their reasons for seeking work online as a refusal to continue to be discriminated against, including always being paid less than their local counterparts due to their refugee status. They explain that refugee entrepreneurs are entering the digital economy to challenge some of the limitations they face accessing work elsewhere.

However, the limitations faced by refugees in the digital gig economy in Kenya illustrate that success at accessing work online cannot happen in a vacuum. While the Government of Kenya has officially established the Refugee Act – promising a potential improvement in refugees' rights to work and access to mobile phones, SIM card registrations and financial inclusion through mobile money – the primary challenge lies in the effective implementation and adherence to these regulations. There is a pressing need for extensive advocacy efforts to inform government officials, mobile phone companies and financial institutions of this new legislation. For instance, refugee documents are still not integrated into broader Kenyan identity databases, leading to persistent challenges in recognising refugee identity cards in all sectors, including in the digital economy.

Refugee agency and leadership is a critically important element of ensuring the promises

of the Act become a reality. Meaningful refugee participation is a valuable asset in the policy and programming of refugee responses. One organisation actualising this is R-SEAT[5] (Refugees Seeking Equal Access to the Table), which seeks to ensure refugees can participate meaningfully, at the state level, in the meetings and decisions of the global and regional refugee regimes. Such initiatives illustrate that if sustainably and meaningfully engaged, refugees in Kenya can support the implementation of the new Refugees Act. They can provide awareness-raising and training to fellow refugees and other stakeholders on new policies, and help shape a proper implementation through offering strategic advisory and community support and identifying gaps and needs in policy implementation. While such contributions could be highly influential in promoting conditions for successful digital work, the benefits would go far beyond this.

Conclusion

The case of digital initiatives for refugees in Kenya suggests that initiatives that contribute to local integration, rather than operate in its *absence*, are more likely to meaningfully support refugees. With more rights and opportunities, refugees could offer their digital skills and expertise to Kenyan businesses, earn income formally to pay taxes, or, at the very least, increase their purchasing power to contribute to their local economy. Many refugee-led organisations' agendas include pushing for refugees to enter the digital economy (either locally and/or globally) so that refugees can invest resources into their local communities.

However, for this to occur, the actual implementation of refugees' rights in Kenya needs to take place. The gap between the rhetoric and reality of digital livelihoods for refugees has raised concerns. There is also the risk that digital work is seen as a workaround to barriers refugees face in accessing local labour markets.

The Kenyan context suggests that local integration through the digital economy can only happen once barriers to identification and socio-economic inclusion are actually removed. Unless more work is done to support refugees' rights, promoting digital livelihoods for refugees is akin to a smoke and mirror policy, or in the words of one refugee leader, as nothing but the 'new scam' in the field of refugee livelihoods.

Marie Godin
Lecturer in Human Geography and British Academy Fellow, School of Geography, Geology and the Environment, University of Leicester and Research Associate at COMPAS/RSC, University of Oxford
Marie.Godin@leicester.ac.uk
X: @MarieGodin001
compas.ox.ac.uk/people/marie-godin

Ishimwe Jean-Marie
East Africa Regional Lead for Refugees Seeking Equal Access at the Table (R-SEAT), Journalist and Board Member at Inkomoko and Youth Voices Community
jean.ishimwe@refugeesseat.org
X: @ishimwemarie432
linkedin.com/in/ishimwe-jean-marie-11b932113

Evan Easton-Calabria
Senior Researcher at Feinstein International Center, Tufts University and Research Associate at the Refugee Studies Centre, University of Oxford
Evan.easton_calabria@tufts.edu
X: @evan_in_refuge
linkedin.com/in/evan-easton-calabria/

1. *bit.ly/ilo-prospects*
2. *bit.ly/finding-durable-solutions*
3. *www.desertfreelancing.com/services.html*
4. *youthvoicescommunity.org/*
5. *www.refugeesseat.org/*

Identity or survival? Digitally preserving Rohingya cultural heritage

By **Saqib Sheikh** and **Muhammad Noor**

The Rohingya people face the threat of loss of their own ethnic identity. A new digital archive offers a means of preserving documents and other material related to Rohingya cultural heritage, but this innovative project is also fraught with challenges.

The Rohingya people have indigenous roots to their land of Arakan, now called Rakhine State, in Myanmar. Since Myanmar became independent in 1948, the Rohingya have been subject to a series of persecutory measures by the authorities, leading later to exile and dispossession of citizenship. One of the forms of persecution has been restrictions on the expression of cultural practices. As a result of these restrictions and low literacy levels in the population, there has been a lack of Rohingya culture-preserving and promoting institutions. The International Court of Justice is currently hearing a case that accuses Myanmar of genocide[1] for its persecution of the Rohingya, and a key part of this has been the attempt to delegitimise the Rohingya ethnic identity by Myanmar authorities by asserting that the Rohingya are Bengali, without roots to the land of Arakan, and a fictionalised ethnic group.[2]

Since the last major exodus from their homeland in 2017, a majority of the estimated three to four million Rohingya live scattered across the region, either as earlier settled communities in Saudi Arabia and Pakistan, or large refugee migrant populations in Bangladesh and Malaysia. A large number of displaced Rohingya remain stateless and without legal documentation.

As generations have passed since the first expulsions in the 1970s, many of the Rohingya communities report that their members face assimilatory pressures to adapt to their host societies. This has resulted in signs of cultural erosion, which include loss of Rohingya language, customs and traditions in favour of those of the host community. A more subtle loss is that of cultural memory, specifically the communal historical awareness of Rohingya roots in their ancestral homeland of Arakan.

Efforts to digitally preserve Rohingya culture and history

In recent years several initiatives have been launched to address the wider collective identity crisis gripping the Rohingya community. For example, in 2021, IOM launched the Rohingya Cultural Memory Centre[3] in Cox's Bazar to showcase and share aspects of Rohingya ancestry and tradition with the surrounding community.

Unsurprisingly, given the scattered regional population, low literacy levels and lack of physical resources, many of the grassroots initiatives look towards digital means to promote Rohingya culture. This includes the setting up of online Rohingya media and news channels to report on the conflict in Rakhine State. The script of the Rohingya language[4] has been standardised and converted into a digital format and accepted within the Unicode Standard (the global coding system that turns written script into digital characters and numbers).

Recognising that aspects of the Rohingya cultural crisis required further attention, the Rohingya Historical Archive[5] or R-Archive was launched in 2021 to identify and archive various documents and other media of ancestral value to the Rohingya people. It was launched by the Rohingya Project, a grassroots organisation focused on using technology to address issues of statelessness for the Rohingya diaspora. The idea behind the R-Archive was that many documents and items relating to the connection of the people with their homeland were scattered, and their loss could jeopardise the people's future in terms of their communal memory. The R-Archive therefore is intended to serve as a community archive for the scattered Rohingya, a resource on Rohingya heritage for researchers and also provide evidentiary support in future legal proceedings towards accountability of crimes against these people. This initiative was funded through a catalyst grant provided by the Roddenberry Foundation and was executed in partnership with the tech company Arweave.

The R-Archive engaged Rohingya field officers based in Bangladesh, Malaysia and Saudi Arabia in the collection process within their communities. In the pilot phase, over 100 documents considered important to Rohingya heritage, such as old land deeds in Arakan, banned identity documents issued by Myanmar and family photographs, were scanned, with the consent and recorded testimonies of the document owners, and uploaded with encryption in a private web-based storage system.

The backend of the system, called the Blockweave (developed by Arweave), is a decentralised data storage protocol similar to a traditional Blockchain but allowing more cost-efficient scalability, typically in the range of three to eight dollars per GB at the time of creation of the archive (without subscription fees). This system was considered suitable for this project because of the anticipation of further storage needs given the larger memory size required for scanned files and audio-visual material as the scope of the R-Archive expands. Traditional blockchain systems often involve higher fees for on-chain uploads, particularly with higher file sizes. Blockweave, on the other hand, employs a unique consensus mechanism that decreases consensus requirements for hashing as the data in the system increases, reducing overall long-term storage costs.

On-the-ground challenges in digital preservation

Many of the obstacles faced in the digital preservation of Rohingya culture lie in the precarious security situations faced by the various diaspora and refugee communities. Rohingya refugees who are living as undocumented migrants try to keep a low profile away from the authorities. It can be difficult to find document owners and get their agreement to have documents preserved. Personal family documents preserved from Myanmar are an incredibly sensitive matter and the owners have real concerns that these records could be tracked back to them.

On top of this, Rohingya field officers and others involved in Rohingya cultural promotion activities have reported low levels of awareness of the need for cultural preservation and the possibility of intergenerational cultural loss. In the opinion of Dr. Qutub Shah, a Rohingya activist and teacher who is leading the project of translating the Rohingya translation of the Quran for the first time, it is a matter of preferring survival to preserving identity.[6] Immediate survival needs such as livelihoods and healthcare are paramount, and cultural preservation is seen as a more

A national ID card of an individual from northern Maungdaw issued by the immigration office of Burma in the late 1950s. Credit: Rohingya Project

'elite' endeavour. In host countries where sentiments towards the Rohingya have moved from solidarity to animosity, self-identification and promotion of Rohingya collective identity can be perceived as contrary to their group interests.

This sensitivity towards online exposure is slightly more acutely felt by the older generation of Rohingya, many of whom have directly witnessed the full frontal attack on Rohingya identity in Myanmar and carry the legacy of this persecution. Yet it is precisely this generation that possesses the communal memory of direct experience with their homeland that is increasingly being lost. Younger Rohingya have shown a propensity to use digital platforms, particularly YouTube, in cultural promotion programmes, though in times of increased scrutiny by host societies towards migrant communities such activities may also be curtailed.

While low literacy levels are an obstacle towards a deeper understanding of the need for digital preservation of culture, there is generally a high level of mobile access in most settled Rohingya communities and sharing of Rohingya-based media and news content. In particular circumstances though, notably in Cox's Bazar in Bangladesh, restrictions on internet access have been imposed, further complicating efforts at coordinating preservation work. In Cox's Bazar's camps, where many relevant documents may still be found, security conditions have deteriorated, and those Rohingya involved in preservation work have to take extra precautions in case other members of the community suspect

they have ulterior motives for asking for this information.

Lastly, digital preservation can be fraught with further concerns for the Rohingya, chiefly over the perception of the possibility of potential leakage or misuse of their personal data. While certain concerns of centralised data access and data security can be addressed by Blockchain systems, in particular through Blockweave which offers a more immutable decentralised transaction system to share the data among miners, there are concerns over the option of deletion of uploaded data that Rohingya users feel could potentially put the users at risk, and protocol and best practices in this regard may be prohibitive for more sensitive personal information.

The problem, as described by Dr. Anne Gilliland, Professor of Information Studies at UCLA and advisor to the ongoing R-Archive, is that while it is critical to protect the security and privacy of individuals giving data in such preservation work, at times certain safety measures taken may inadvertently compromise the evidentiary quality of the data taken.[7] The task involves juggling "competing rights", prioritising immediate individual rights and the need for informed consent while remaining cognisant of the existential risk to an entire community of data not being shared.

Conclusion

Based on the experience with the R-Archive, a significant amount of attention needs to be paid towards educating communities about the importance of their own cultural legacy, while respecting the fears and restraints they face in tough host societies. A focus on 'safer' cultural preservation formats focused on intangible cultural resources, such as oral storytelling, with broad community resonance may be a more pragmatic route. Respecting the community's perceived priorities must take precedence, while allowing them to appreciate the importance of an enterprise that seeks to retain key aspects of their collective identity. We also recommend trying to access existing digitised major archives from institutions where some of the data concerning the Rohingya has already been stored or has recently been declassified and simply needs to be searched for and identified.

Saqib Sheikh
Project Director, Rohingya Project &
Doctoral Researcher, S. Rajaratnam
School of International Studies, Nanyang
Technological University, Singapore
saqibmun001@ntu.edu.sg

Muhammad Noor
Managing Director, Rohingya Project
noor@rohingyaproject.com

1. *www.icj-cij.org/case/178*
2. *bit.ly/myanmar-rohingya-denial-history*
3. *bit.ly/cultural-memory-centre-rohingya*
4. *bit.ly/language-rohingya-digitised*
5. *bit.ly/rohingya-historical-archive*
6. *Shah, Qutub. Interview. Conducted by Saqib Sheikh. 26 December 2023.*
7. *Gilliland, Anne. Interview. Conducted by Saqib Sheikh. 1 January 2024.*

Ethically informed algorithmic matching and refugee resettlement

By **Ahmed Ezzeldin Mohamed** and **Craig Damian Smith**

This article discusses real-world projects using algorithms to match resettled refugees with sponsors and services. The authors argue that when done right, algorithms can support larger-scale and better-informed resettlement.

Techno-scepticism and techno-optimism

Research and advocacy around data and tech to manage international mobility can be divided into techno-sceptical and techno-optimistic camps. While the dichotomy is admittedly a broad heuristic, these parallel research tracks draw attention to the inherently dual-use function of any technology.

Techno-sceptical research and advocacy raise well-founded concerns around uses like biometrics and surveillance in border controls, automated visa decisions, or artificial intelligence (AI) for predicting asylum or displacement trends. It is largely informed by a commitment to migrants' rights to move and seek protection. For example, sceptical research calls attention to the ethical implications of data-gathering for monitoring migrants,[1] the absence of recourse to appeal automated decisions, and the threat of hard-coding group-based biases. In short, it focuses on the use of technology to curtail 'unwanted' migration, rather than facilitating international mobility.

One of the major unstated premises in techno-sceptical literature is the assumption that existing decision-making systems are somehow fairer and less biased than using data or tech. However, human decisions are at least equally (though probably more) prone to error, bias and subjective value judgments. When applied to refugee resettlement, for example, bureaucracies and civil society organisations rarely, if ever, keep verifiable records of why refugees are placed in specific locations, or the rationale behind decisions to match individuals or households with community sponsors or to specific locations.

On the techno-optimist side, experimental work using historical data has shown that algorithms can significantly improve integration outcomes for newly resettled refugees, particularly around labour market performance. Research[2] in the UK, Switzerland and the United States indicates that using algorithms to match refugees with destinations can significantly enhance employment outcomes. The drawback of this approach is that it can often flatten peoples' life courses to merely economic indicators, rely on unverified assumptions about refugees' priorities and aspirations, and raise ethical concerns around genuinely informed consent.

These parallel veins of research take place amid growing concern about the role of algorithms and AI in social and political fields. Countries and supranational organisations, in particular the European Union (EU), are working to catch up with the rapid pace of technological change by regulating AI and algorithms.[3] This extends to their deployment in immigration and asylum policy, which the European Commission

designated as a 'high risk' domain due to the vulnerability of affected populations and concerns about fundamental rights.[4]

A middle path: algorithm-supported interventions

While the two camps of advocacy and research rarely engage in dialogue, they offer complementary insights into how applying tech to international mobility is far from zero-sum. Our experience matching refugees[5] with sponsors and services in North America and Europe has shown that simply using the term 'algorithm' can lead to immediate ethical concerns, but also that algorithms are often conflated with AI – suggesting that algorithms use big data or train on inherently biased sources. For example, in the Re:Match programme, our algorithms suggest optimal matches for relocating displaced Ukrainians from Poland to Germany – which are then vetted and approved by programme staff. Journalists who interviewed us[6] about the project started with questions around bias and handing over decisions to machines. The line of questioning is both valid and welcome, but also typical of assumptions about how algorithms work in practice.

Algorithms can be written to facilitate mobility and improve outcomes, just as they can be trained to reject visas for nationalities deemed a 'risk' for asylum claims. Most often, applied algorithms are simply computational tools for addressing the complex problem of sorting through large amounts of data to optimise scarce resource allocation – like spots in community sponsorship programs, affordable housing, or services for refugees with particular needs. Once they are shown how ethically-informed algorithms can be used to facilitate rather than control migration, civil society actors understand the value of such algorithms in supporting resettlement work.

At the most fundamental level, algorithmic matching can help scale resettlement – as we explored in a Migration Policy Institute policy paper.[7] First, it frees up human resources to directly support refugees in the resettlement process and to focus on advocacy around upholding and improving international protection laws and norms. Second, it can improve resettlement by using objective rules to ensure a good fit between refugees and their destinations, promoting self-reliance as early as possible.

Matching refugees with destinations or community sponsors entails collecting, storing, and analysing large amounts of data. Running these procedures 'by hand' is incredibly labour-intensive, quickly runs into barriers to scaling and introduces inherent bias, regardless of good intentions. For example, many organisations assume refugees should be placed with diaspora populations in a receiving country. In our experience collecting preferences from refugees, a significant proportion rank diaspora connections lower than preferences around work, education, or closeness of fit with sponsor group family structures.

In addition, most matching programmes run by NGOs or civil servants boil down to a few people looking at dense spreadsheets and often making quick decisions. Bias is inherent because the inability to process and compare large volumes of data means relying on assumptions or consciously focusing on a few data points given personal experiences with previous populations or pre-determined protocols. Algorithms are a tool to alleviate these challenges.

Instances where algorithmic matching could improve resettlement experiences

We argue that in some circumstances, algorithmic matching could provide a closer fit between destinations and refugees'

attributes, goals, and preferences.

The EU's voluntary solidarity mechanism is designed to share protection responsibility across Europe, but it is marked by political impasses and an absence of objective criteria for identifying which refugees might fare better in different destinations. Recent policy literature[8] calls attention to the role that data and algorithms might play in responsibility-sharing.

Canada's various refugee resettlement streams are often held up as an unmitigated success in terms of compatibility between welcoming societies and positive integration outcomes for refugees. But a significant number of newly-arrived refugees leave their places of arrival within the first year – typically for better jobs, to be close to family, or better opportunities for children. On a much smaller scale, some experience relationship breakdowns with sponsors, often because of mismatched expectations. The same trends exist with refugees in the United States.

Secondary migration and sponsorship breakdown are perennial challenges and often result in service gaps – for example, when transferring social welfare benefits between sub-national jurisdictions – and a misallocation of scarce resources. Using objective criteria to match refugees with destinations that better fit professional and social characteristics means not only a better allocation of resources but also a more immediate start on integration journeys.

Furthermore, more refined matching can help foster direct and meaningful relationships between receiving communities and refugee newcomers, and thus help build positive public opinion around humanitarian immigration programmes. Algorithmic matching offers a unique and perhaps unparalleled opportunity to collect baseline data and genuinely understand relationships between social connections and long-term outcomes – assumptions[9] which underpin research around why sponsorship positively affects integration.

Practically, algorithmic matching ensures more robust baseline data collection (including about refugees' preferences) and outcome evaluations that go beyond relatively simple measurements like work and language, to include refugees' satisfaction with assigned sponsors and locations. More and better data can help unravel diverse and complex social processes by which refugees navigate social life in new communities, and those results can then be fed back into matching algorithms in order to iteratively improve outcomes. This type of learning for consistent program development isn't possible when refugees are matched by hand and records are incomplete or subjective.

Ethical algorithmic matching in practice

Our projects in North America and Europe have offered the opportunity to reflect on some overarching lessons for the ethical use of algorithms.

1. Ensure you have the right expertise

Staff who conceptualise, design and code algorithms should include experts in refugee resettlement, ethics of collecting and using data from vulnerable populations, and cyber security.

Algorithm designers should work closely with partner organisations and front-line staff to ensure the accuracy and completeness of refugee administrative data, and to solicit high-quality data from community sponsors, support agencies and different levels of government. Ensuring the quality of matching inputs will lead to better and more trustworthy outputs. Cyber security

experts are equally critical to protecting data and ensuring the privacy of refugees and sponsors.

Algorithm-proposed matches should be vetted by settlement organisations and either accepted or rejected by programme participants.

2. Consider refugees' preferences and agency

Algorithmic matching should consider the diversity of refugees' preferences and offer room to exercise their agency.

An exclusive focus on economic productivity can blur humanitarian and economic or skill-based immigration programmes. Collecting data on refugees' preferences illustrates diverse opinions on what factors should dictate placement. Throughout Europe, our programmes use interviews and preference-ranking surveys to include refugees' agency in matching. In our most recent work with displaced Ukrainians, their preferences dictated weights assigned to matching variables. Many ranked proximity to Ukrainian diasporas and culture, higher education and opportunities for children above work experience. In turn, this left room in matching assignments for participants with higher preferences for work.

Introducing preferences-as-data can build algorithms that limit bias and minimise reliance on unverified assumptions and stereotypes. Similar to labour-market assumptions, the common and seemingly innocuous assumption that refugees prefer relocation near co-nationals or co-religionists could have ethical repercussions, especially for those fleeing discrimination due to their identity factors like ethnicity, religion, or sexual orientation and gender expression. Including refugees' preferences in algorithms minimises these potential pitfalls.

With community sponsorship programmes, matching should also account for receiving community preferences. Sponsors provide scarce relocation resources, and maintaining their satisfaction and engagement is critical for programme success and possibly achieving wider social and political impact. In the best-case scenarios, refugees' preferences should be given equal weight to sponsors. Admittedly, an imperfect policy environment and logistical challenges communicating with refugees in resettlement pipelines often means relying on administrative data, but even one-sided preferences bring more voices into resettlement decisions and open the door for policy change.

3. Consider the ethical implications of matching

Ethics should be central to algorithm design and when considering matching implications.

Even if an algorithm is designed to provide fair and high-quality outcomes, potential ethical implications remain. Some key questions include: Does not being matched or receiving a low-quality match (which might rationally mean rejecting an assignment) preclude displaced people from resettlement or other services? When do protection or vulnerability concerns mean a quicker match is better than waiting for a higher-quality match? Should refugees opt-in to matching programmes, or is an opt-out system better if it means more will be resettled?

4. Algorithm processes should be legible to outside agencies

Algorithms and the matches they produce should be legible to policy-makers and partner organisations. This means removing algorithm processes and outcomes from a black box. While the proprietary rights of algorithm designers should be

protected to promote technical innovation in humanitarian realms, matching inputs and outcomes must be clear to ensure transparency.

Participants, including refugees, sponsors, implementing agencies and governments, should be made aware of the purpose and use of their data. Consent should be genuinely informed and, where possible, refugees should be allowed to refuse a match and be resettled under a traditional pathway.

5. Be clear about the limitations of algorithmic matching

Any organisation or research project advocating for algorithmic matching should communicate its limitations and manage expectations.

Algorithms are tools to optimise resource allocation, but their scope is constrained by the availability of such resources. It is essential to communicate that matches can only be as good as the resettlement locations on offer, and that they reflect the diversity of sponsors and refugees. While it's rarely possible to meet all preferences, algorithms can incorporate broad swaths of data to make the best possible matches given real-world constraints – but real-world constraints are always present.

Conclusion

Despite divided discourses around tech in migration policy, ethically-informed algorithmic solutions for refugee resettlement are something of a middle path. Demonstrating this path requires describing an algorithm's role and purpose. They can be likened to communication platforms where refugees, hosts, and available resources can be given voice-as-data, allowing those most affected by resettlement to influence outcomes. They contribute to decision-making structures that systematically integrate ethical rules to minimise bias and ensure fairness. They also serve as banks of knowledge that can store and sort valuable data for policy-makers and researchers to develop more effective refugee resettlement programmes. Algorithms are neither a silver bullet nor a scapegoat; they are one tool among many for fair and effective policymaking.

Ahmed Ezzeldin Mohamed
Assistant Professor of Political Science, Institute for Advanced Study in Toulouse School of Economics and Algorithm Engineer and Data Analyst, Pairity
amohamed@pairity.ca
linkedin.com/in/ahmed-ezzeldin-mohamed-4b6a07a2/

Craig Damian Smith
Co-Founder and Executive Director, Pairity and Research Affiliate, Centre for Refugee Studies, York University
csmith@pairity.ca
linkedin.com/in/craigdamiansmith/

1. *bit.ly/utoronto-automated-systems-report*
2. *bit.ly/improving-refugee-integration*
3. *algorithmwatch.org/en/ai-act-explained/*
4. *bit.ly/ai-schengen-borders*
5. *pairity.ca/where-we-work/*
6. *bit.ly/matching-algorithms-ukraine*
7. *bit.ly/matching-refugee-sponsorship*
8. *bit.ly/digital-technologies-eu-pact-migration*
9. *bit.ly/unhcr-government-refugee-resettlement*

Digital counter-surveillance by refugees from Myanmar in Thailand

By **Nyi Nyi Kyaw**

Host countries hold considerable powers to place forced migrants under surveillance, but, as this case study from Thailand illustrates, forced migrants may use what agency they have to launch digitally mediated counter-surveillance and reconnaissance.

Pictures, videos, media reports and information campaigns that show forced migrants across the world being stopped, arrested, imprisoned and/or deported could lead to the assumption that forced migrants lack agency and are constantly under state surveillance. However, although the agency and power of forced migrants is generally much less than that of security officials, this does not render forced migrants agencyless. In this article, I use the example of the digitally mediated reconnaissance by Myanmar refugees in Mae Sot, Thailand, to show how forced migrants can engage in counter-surveillance.

Forced migration, social media and (counter-) surveillance

Borders[1] are increasingly controlled digitally. Some governments[2] in Europe try to prevent forced and irregular migrants, such as those from Afghanistan, from coming to their borders and shores by using social media campaigns and spreading information that such migrants are not welcome. The Danish government even mounts surveillance on the Facebook profiles of those refugees claiming LGBTQ[3] identities,

On the other hand, refugees may use Facebook for two main reasons:[4] the need to belong to a community and the need for self-representation. The social media platform offers a sense of belonging and the ability to express oneself through producing and sharing posts, comments, pictures and videos. This expression and information sharing can be altruistic and socially oriented, for example, the use of Facebook to seek and share information in the aftermath of disasters.[5]

Information and expression flow in multiple directions among multiple persons or users on a social media or messaging platform. Asylum seekers, refugees and former refugees also use social media for information sharing, for example, for those heading to[6] or already in[7] the Global North. There is less material available on how forced migrants in the Global South share information digitally after fleeing their homes and remaining in neighbouring countries. In this article, I present a contemporary Global South example of Myanmar refugees in Thailand.

Myanmar refugees in Mae Sot, Thailand

Sharing a border with Myanmar to the west, the town of Mae Sot is located in Tak Province in lower northern Thailand. Mae Sot has hosted thousands of Myanmar refugees since the 1980s due to the conflict in Myanmar between ethnic armed groups and pro-democracy groups on the one hand and the Myanmar military on the other hand. Thousands of Myanmar refugees fled to Mae

Sot in the aftermath of brutal crack downs on dissent and resistance following the military coup in Myanmar on 1 February 2021.

Refugees from Myanmar are spread across Mae Sot and the surrounding areas in Tak Province. As a group, those who arrived following the 2021 military coup have relatively higher socio-economic and educational backgrounds than those who arrived prior to this. They include young students, academics, activists, social workers and government staff. Many, if not most of them, are tech-savvy, or more specifically Facebook-savvy, having enjoyed affordable, widespread internet access and freedoms of (digital) expression enabled by a liberalised telecommunications industry in Myanmar from 2011 until the coup.

Through lived experience, the new cohort have already mastered the art of circumventing and bypassing draconian internet restrictions and the Facebook ban imposed by the military junta after the coup. They had already created numerous public and private groups on Facebook, Signal and Telegram to share information when they were inside Myanmar. Therefore, the Myanmar refugees and asylum seekers who have arrived in Mae Sot from 2021 are well-prepared to use their tech-savviness. They see themselves as an army of comrades against military dictatorship back home. This strong sense of political camaraderie among them has been very helpful in creating networks and teams of counter-surveillance and reconnaissance to protect themselves in Thailand.

Physical surveillance by security officials in Mae Sot

Thailand is not a signatory to the 1951 Refugee Convention. So, the kingdom is not legally obliged to recognise and treat asylum seekers and refugees from Myanmar as such. While Thailand has largely avoided arresting and deporting the post-2021 refugees, it has not allowed this group of roughly 60,000 people to stay legally in Mae Sot. The border town is effectively a 'containment zone' where Myanmar refugees are not able to roam freely or to leave for other parts of Thailand. Without visas and work permits the refugees are rendered vulnerable to (temporary) arrests and extortion by security officials.

One barrier restricting the refugees' mobility is the use of checkpoints and patrols within and on the way out of the town. The checkpoints and patrols have two functions. The first one is official or lawful, that is to check documents, arrest those without them or with expired or invalid ones and take further action, including deportation. In reality, this official function is rarely fulfilled. The second function is unofficial, informal, or unlawful, that is, to pick up undocumented refugees and demand payments from them in exchange for avoiding arrest or deportation. This function is more common. Refugees have had to pay from a few thousand up to 30,000 baht (around 840 US dollars), or even more.

To avoid arrests and extortions, some Myanmar refugees do not go out at all, but this is not an option for all of them. Therefore, one or two persons from families or groups of people or friends living together usually shoulder the burden of going out. Those who must go out have three options. First, Thai regulations allow foreign workers, including those who entered the kingdom irregularly by crossing the border without a visa or border pass, to obtain labour documentation to work in labour-needy sectors such as fisheries or agriculture. However, refugees and asylum seekers who are not actually employed in these sectors sometimes pay to obtain this documentation as protection against arrest and extortion. Second, some

refugees strike informal – but somewhat effective – protection deals with local police by paying monthly fees or bribes of usually 300 baht via brokers. This is less effective than the first option. On many occasions, refugees who have paid bribes to a particular official and broker have faced extortion by another official when their own protector is unreachable. Third, the refugees try to avoid the checkpoints as much as possible. To do so, they need to mount counter-surveillance of the checkpoints and patrols.

Counter-surveillance and reconnaissance by Myanmar refugees in Mae Sot

As of January 2024, about 60,000 or more Myanmar asylum seekers and refugees remain displaced in Mae Sot, staying undocumented, largely immobile and at risk of arrest and extortion if they go out. The refugees have had to take care of and protect themselves from potential arrests, extortions and/or deportation by Thai security officials for more than two years since the coup in Myanmar. In doing so, asylum seekers and refugees not only express their own agency but also significantly enhance it through innovation, testing, usage and further development of the digital tools and platforms at hand.

There are demand and supply sides to Myanmar refugees' counter-surveillance and reconnaissance of the checkpoints and patrols in Mae Sot. Before going out, individual refugees or groups of them gather intelligence on the whereabouts of the checkpoints and patrols in the town by checking real-time information on Facebook, Telegram and Signal and map out safe routes. On all three platforms, there are private and public groups that may be joined with or without referral or approval by their owners, administrators and managers. This is the demand or user side. On the other hand, communally oriented and tech-savvy Myanmar people in Mae Sot create Facebook Groups, Telegram Channels and Signal Groups, act as or even hire paid or volunteer scouts, and post and share intelligence on the checkpoints and patrols. This is the supply side. The overarching feature of this counter-surveillance and reconnaissance is the use of digital media, although it also relies on human patrols and intelligence gathering on the ground.

From the interviews I conducted with 24 users of those Facebook Groups, Telegram Channels and Signal Groups, they are largely reliable and useful. It is not fail-proof however. The information cannot be accurate at all times; sometimes patrols and checkpoints appear unexpectedly and are not yet on the radar of Myanmar refugees. Compared to checkpoints that are relatively stable for a period of time, patrols in moving cars or motorbikes are more difficult to observe, take note of and report.

Having lived in Mae Sot for close to three years, Myanmar refugees have also managed to detect a pattern of time and location of several regular checkpoints (and of some patrols as well), enabling them to move about in the town relatively freely and without entirely relying on the information they gather online.

The digitally mediated counter-surveillance and reconnaissance by Myanmar refugees in Mae Sot may not be replicable in other locations. The relatively small size of Mae Sot and the limited number of geographic locations of checkpoints and patrols make it relatively easy for refugees to take note of and avoid them; this might not be realistic in bigger towns or a city such as Bangkok.

Similarly, these initiatives on Facebook, Telegram and Signal may not be sustainable in Mae Sot in the long run, as they are heavily reliant on the goodwill and digital efforts

The border checkpoint in Mae Sot on the Thailand-Myanmar Friendship Bridge

of concerned people and fellow citizens. Refugees surreptitiously monitoring Thai check points and patrols may prompt crackdowns by authorities. Due to this potential repercussion from the authorities, civil society and non-governmental organisations may be neither willing nor able to be involved in and run digital counter-surveillance and reconnaissance projects themselves.

Conclusion

The use of digital technology by Myanmar refugees in Mae Sot to monitor Thai security checkpoints and patrols demonstrates their relative power and agency in comparison to the disproportionately larger powers of the Thai state to stop, check, extort, arrest and deport them. It is important to acknowledge not only the role of digital mediation and connectivity but also the refugees' self-help and agency.

Nyi Nyi Kyaw
International Development Research Centre (IDRC) Research Chair on Forced Displacement in Southeast Asia, Chiang Mai University, Thailand
nnkster@gmail.com

1. *bit.ly/digital-passages-borders*
2. *bit.ly/leaving-afghanistan*
3. *bit.ly/social-media-surveillance*
4. *bit.ly/why-people-use-facebook*
5. *bit.ly/fb-info-seeking*
6. *bit.ly/smart-refugees-syrian*
7. *bit.ly/refugee-integration-social-media*

How art and social media transformed refugee movements in Lesvos

By **Berfin Nur Osso**

From the social media movement 'Now You See Me Moria' to the Hope Art Project, refugees in Lesvos are using digital platforms to disrupt restrictive legislation, practices and discourses inflicted on them by state authorities.[1]

In this article I reflect on refugees' visual-digital struggles. My reflections are grounded in two online ethnographic studies of the imagery (photographs, videos, screenshots and paintings) produced by refugees in Lesvos, that I carried out during 2022 and 2023. Refugees' expression of their rights claims through visual arts and social media has been especially significant given the rising hostility and silencing efforts against them, and the restrictions imposed by the Greek authorities on journalists,[2] human rights advocates and non-governmental organisations trying to monitor the situation on the Greek islands.

Creating visual stories of refugeehood at the Hope Art Project

The Hope Project[3] was established on the Greek island of Lesvos following the summer of migration in 2015. The founders, Philippa and Eric Kempson, initially aimed to provide for the basic, urgent necessities of people arriving at the island. Over time, they recognised the need for catharsis and healing through art, and they began an art project in 2018. Since then, many refugees inhabiting the notorious Moria camp have attended workshops on diverse themes, including theatre, music and painting.

Painting has been an important getaway space, a mental sanctuary for the artists, away from the camp's turmoil.[4] Artists from various countries, such as Syria, Afghanistan, Iraq, Sudan, South Sudan and Congo, have produced paintings at the Hope Art Project. In the right-hand corner of each, the artists sign their shared identity: 'Moria refugee'. Philippa describes these paintings as, 'slightly edgy and political'; they reflect on the impact of the EU and Greek asylum laws and policies, refugees' arduous migratory journeys towards Greece, their living conditions in Moria, and their hopes and dreams concerning an often-uncertain future.

To date, the artists have produced over 10,000 paintings, some of which have been displayed in online and on-site exhibitions and shared digitally. Several artworks have been exhibited[5] in renowned places like St James's Church in London. In an art exhibition entitled 'A Place in My Mind',[6] curated both online and offline by Norwegian artists in 2021, artworks created by many artists at the Hope Project were able to reach a wider audience across borders. Well-known news outlets have covered stories of the Hope Project artists and their artworks.

The artists were unable to travel freely even to the Greek mainland, so they could not attend the physical exhibitions of their artworks outside Lesvos or meet with other artists and people promoting their artworks, yet they were able to collaborate in cyberspace. Many of the artists, most of whom finally settled in European countries

Untitled, painting by Abdullah Rahmani, 2020. Reproduced with the permission of the artist.

after years of being in legal limbo in Lesvos, endeavoured to publicise their artworks through their personal social media accounts. Elleni Kempson, daughter of Eric and Philippa and social media coordinator at the Hope Project, has shared many of the artworks through the Instagram account 'Hope Art Project'[7] and Fine Art America,[8] an online repository where visual artists can share and sell their artwork.

The wide dissemination of the visual stories told by refugee artists at the Hope Project Greece was made possible through their active use of digital technologies, particularly social media. These technologies created collaboration opportunities and enabled the artists to reach a broader audience. At the same time, art and digital technologies have transformed even the most mundane depoliticised spaces,[9] namely the art workshops and painting canvases, into spaces where refugee artists speak their mind with their own narratives. These narratives disrupt the dehumanising portrayal of refugees by some media outlets and decision makers.

Challenging the status quo: 'Now You See Me Moria'

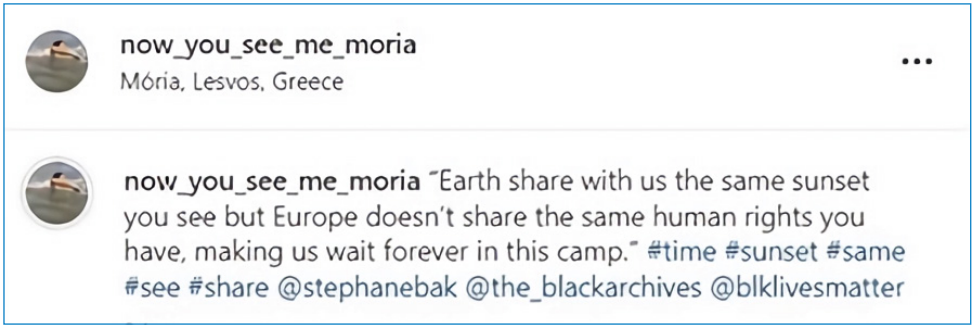
For refugees who do not have access to art workshops in Moria where they can recount their own stories, smartphones are vital tools for communicating with the outside world and for survival in everyday life. Smartphones (with sufficient internet connection) are also digital tools for raising refugee voices against the atrocities and abysmal living conditions refugees encounter in Lesvos. Smartphones help refugees narrate and disseminate[10] their own stories of refugeehood. That is how the 'Now You See Me Moria'[11] campaign emerged as a collaboration of Moria inhabitants

and 'outsiders', to show the world what is happening and demand respect for refugee rights.

Now You See Me Moria was started in 2020 by two people who met online: Amir, an Afghan refugee inhabiting the Moria refugee camp, and Noemí, a Spanish photographer and photo editor based in the Netherlands. Their initiative quickly became a social media movement with the participation of over 600 refugees on Instagram,[12] with over 41,300 followers (March 2024), hundreds of engagements, likes and comments by their audience. Since August 2020, refugees have clandestinely recorded and disclosed over 4,500 posts (photographs, videos and screenshots) and countless 'Insta stories' from their everyday life in Lesvos. While exposing imagery from inside Moria and the Lesvos Closed Controlled Access Centre (CCAC), they also make the cruelties and inhumane conditions refugees encounter visible.

It has been widely documented by non-governmental organisations that the CCACs inaugurated on the five Greek islands are 'prison like',[13] and in 2023 the European Court of Human Rights reiterated[14] that the Greek hotspots have undignified conditions. Now You See Me Moria aims to stop the construction of the new Lesvos CCAC, which they consider 'a prison' that will create an equally degrading environment. Their #nochildinaprison campaign demands that no children are subject to detention in refugee camps, 'far away from the colourful world they deserve'.

Now You See Me Moria could not exist or have expanded without cyberspace. The rapid growth of this photography project is noteworthy, especially considering the absence of centralised leadership. Each refugee freely participates, records and



An image posted on 'Now You See Me Moria' Instagram page, 12 October 2022. Reproduced with permission.

shares online what they see in Lesvos without any directives. Their advocacy efforts have frequently received external support; refugees and their allies across the globe have demonstrated how they can use social media to build a movement across borders. Using digital technologies, refugees involved in Now You See Me Moria attempt to reach EU decision makers and those who can influence them. Most of their posts are written in English to target an international audience.

Those acting for refugees have shown their support in various ways, both in cyberspace and public spaces. Refugees, often together with their online audience, actively 'tag'[15] decision makers (such as the European Commission's President Ursula von der Leyen and Home Affairs Commissioner Ylva Johansson), human rights organisations (such as Amnesty International) and the media in their posts on Instagram. The audience has also endorsed the movement by drafting legal reports[16] to stop the construction of Lesvos CCAC, advocating for the rights of children detained in Lesvos, finding legal support, creating thought-provoking posters to raise awareness, and selling t-shirts to provide food vouchers for refugees and uphold their right to adequate food. With the collaboration of outsiders, the movement also published an action book (a tool for those who wish to protest) and organised poster and photography exhibitions[17] across Europe, including in Amsterdam, the Netherlands; in Brussels, Belgium; in Vienna, Austria; in Rome, Italy; and in Düsseldorf and Burgrieden, Germany.

Those involved in the movement face significant risks because of soaring hostility[18] towards refugees from outside Europe, the criminalisation[19] of refugee activism and advocacy efforts, and accusations of espionage[20] in Greece. For this reason, refugees sharing photographs from Lesvos try to remain anonymous, while sharing images that represent their everyday life and supplementing them with powerful political captions.

In the long run, the activists at Now You See Me Moria also aim to build a database that will function as an easily accessible online archive of visual materials for those who are interested in learning more about the plight of Moria refugees. The database could serve as a collective memory of refugeehood and as legal evidence to be used in the courts, including the European Court of Human Rights.

The politics of disruption and transformation in Lesvos

The Hope Art Project and Now You See Me Moria have helped many refugees in Lesvos to:

1. challenge stereotypes and dominant legal, policy, and media discourses portraying refugees as victims, invaders or criminals;
2. reclaim their voice[21] to narrate their own circumstances and future and claim an audience;
3. challenge the Greek and EU policies and practices on migration and asylum that they are exposed to, and
4. raise awareness about these policies and practices.

The two examples show that art and digital technologies can be disruptive and transformative in many ways. Refugees at both Now You See Me Moria and the Hope Art Project endeavour to widely share stories and experiences of refugeehood from their own perspectives and through their own voices. At the same time, they make the violence of Europe's borders visible with the aim of mobilising their audience to improve the situation of refugees in Europe. Social media posts by refugees at Now You See

Me Moria have even caught the attention of the Greek police on the island. Refugees claim[22] that the police tried to track refugees' smartphones to find who shared 'insider information' from the camps.

Refugees who were not able to express their opinions through peaceful assembly in public spaces did so through their digital and creative practices. Those I interviewed stated that many refugees were afraid to speak freely as their asylum applications could be adversely affected. For refugee artists at the Hope Project, art is their voice and social media helps them to spread their art. Refugees at Now You See Me Moria are also able to anonymously share images from their everyday life, speak up and reach a transnational audience with the help of digital technologies.

Understanding the ways in which the uses of digital technologies by refugees are disruptive and transformative comes also with understanding challenges for ethics, positionality and change. One needs to be mindful of the trap of 'voyeurism',[23] or lustful and desensitising effects of the images (especially photographs) showing the human rights abuses inflicted on refugees, to keep a safe, critical distance to these images. As a viewer of the imagery shared by refugees in cyberspace, a researcher's role lies also in transforming oneself from the viewing subject into the acting one through scientific research and its dissemination via reputable channels. This is especially important in a world where refugee stories are still not deemed credible or relevant,[24] a world where it is crucial to counter oversimplified and reductive depictions of refugees. As an immigrant-researcher, I have sought to reflect refugees' stories 'in their great diversity' and convey refugees' voices to a broader readership.

Refugee action through art and social media may not always incite change in ways that can be measured. Nonetheless, to echo Noemí's words, doing something, as opposed to nothing, may eventually lead to lasting and positive change for refugees. Art and social media can be effectively used to raise awareness of situations where refugees' rights are denied, their voices muted, and where their struggles would otherwise be invisible.

Berfin Nur Osso
Doctor of Laws (LLD) candidate,
University of Helsinki, Finland
berfin.osso@helsinki.fi X:@bossoloji

1. *With sincere thanks to Philippa Kempson, Eric Kempson, and Noemí for their collaboration, and hundreds of artists at the Hope Project and activists at Now You See Me Moria whose struggles inspired me in the preparation of this article. The real names of persons are used with their permissions, and last names are omitted for privacy.*
2. *perma.cc/AW7C-MJ54*
3. *www.hopeprojectgreece.org/about-us*
4. *Interview (online) by the author with Philippa Kempson and Eric Kempson, 14 May 2022.*
5. *bit.ly/we-never-chose-this*
6. *www.instagram.com/kunstenaahjelpe.no*
7. *www.instagram.com/hopeprojectart/*
8. *bit.ly/thehopeproject-moriarefugees*
9. *bit.ly/what-is-refugee-camp*
10. *bit.ly/border-countervisuality*
11. *nowyouseememoria.eu/*
12. *Interview (online) by the author with Noemí, 17 April 2023. www.instagram.com/now_you_see_me_moria*
13. *bit.ly/joint-statement-irc-gcr*
14. *bit.ly/ad-v-greece*
15. *bit.ly/moria-food*
16. *bit.ly/moria-legal-report*
17. *bit.ly/now-you-see-me-moria-2*
18. *bit.ly/violence-within-state-borders-greece*
19. *bit.ly/hostile-hospitality-greece*
20. *bit.ly/greek-target-ngos*
21. *bit.ly/speechless-emissaries*
22. *bit.ly/moria-police*
23. *bit.ly/regarding-pain-others*
24. *bit.ly/stories-lived-experience*

Exploring Venezuelans' perspectives on border technologies

By **Julia Camargo** and **Amanda Alencar**

This article aims to raise awareness and build understanding of the impact of the digitalisation of border spaces on Venezuelan refugees.

When Adri,[1] a 43-year-old Venezuelan lawyer and mother, crossed the border between Venezuela and Brazil, she was struck by the array of technological equipment awaiting her arrival:

> *"When entering the tent for processing the documentation, I had a big surprise: it was fully equipped with computers, and we could hear the noise of the keys. The organisation assisting us reviewed my entry permit. I had to leave the mark of all my fingers, even use a kind of binoculars that captured the images of my eyes, but I don't know why! Everything organised, respectful and military."*

Adri's account emphasises a global trend in the management of borders in forced displacement: the increasing use of digital technologies by both states and humanitarian response actors and the need for forcibly displaced people to provide significant amounts of personal data to access humanitarian services, often with little information or awareness about how their data will be processed.

Digital migration and border governance includes direct and indirect interactions with individuals in transit, involving activities such as biometric data collection[2] (through fingerprints, facial recognition and iris scanning), monitoring migration movements, digitisation of migration services, automated decision-making,[3] creation of applications, and support via chatbots or one-way channels on social networks.

The digitisation of the migratory process may enhance the efficiency of migration management bureaucracy, streamlining the tasks of international agencies involved in issuing identity documentation and distributing humanitarian assistance to refugees. However, there is a risk that the digitisation of these processes contributes to perpetuating the vulnerabilities of refugees, as their data may be used for purposes beyond basic identification and aid provision, such as profit making, government surveillance and other undisclosed intentions. They may be seen either as victims of failed policies in their countries of origin or as potential suspects of past or future illegal activities.

Amid the complex landscape of technology adoption within migratory border governance, this article presents the opinions and experiences of 15 Venezuelan refugees who underwent biometric data collection at the Brazil-Venezuela border between 2019 and 2021. These individuals were interviewed and participated in focus groups on digital migration governance organised by the authors of this article. Before delving into an analysis of their responses, it is important to contextualise the digital framework established to manage Venezuelan refugees in Brazil.

Digital migration governance in the Brazil-Venezuela border

The recent militarisation of the Brazil-Venezuela border triggered the digitalisation of Brazilian migration governance through the adoption of internationally used models and narratives emphasising border security. At the border, digitised screening devices are employed, facilitating data exchange and the use of technological systems for migration control.

In 2021, the Brazilian Industrial Development Agency (ABDI), in partnership with the State Government of Roraima, launched the 'Border Tech Project' at a cost of R$3.1 million Brazilian Reais, or $618,000 in US dollar equivalent, to monitor the border between Brazil and Venezuela. The small border city of Pacaraima, acquired technologies, such as smart dimmable lights, smart lights with integrated cameras and surveillance, facial recognition software, speed dome sensing cameras, a datacentre for storing and processing images and data, video wall screens, licence plate recognition cameras, licence plate recognition software and a drone with a thermal camera.[4]

As part of the reception of Venezuelans arriving in Brazil, basic identification data and other more complex information is requested. After mandatory passage through the Federal Police, Venezuelan refugees go through a process of data collection, management and storage carried out by two institutional humanitarian response protocols: the PRIMES System[5] (Population Registration and Identity Management EcoSystem), under the responsibility of UNHCR, and the Acolhedor System,[6] administered by the Brazilian Government. The PRIMES system manages biometric data on a global storage basis, which according to UNHCR, aims to offer refugees a digital identity that allows them access to services. Through the system, UNHCR can authorise data access to host governments for collaborative efforts in terms of delivering services together with UNHCR. The data collected by the UNHCR team is used to identify actions to assist refugees and for managing shelter, providing documentation and relocating refugees within Brazil.

On the other hand, the Acolhedor System was put in place by the Brazilian government and designated as the official registry and database for its relocation programme. Non-biometric data collected by the system, such as name, education, courses, professions, qualifications and family data, Individual Taxpayer Registration (CPF), work card and vaccinations, are also subsequently recorded digitally. The Acolhedor System database allows data access and sharing with partner organisations, including Brazilian ministries, local government sectors, UN agencies, INGOs and civil society.

Paradoxically, both systems operate in the context of growing digital inequality[7] facing Venezuelan refugees. On the one hand, migration governance is increasingly facilitated through platforms, providing training, financial resources, recreational activities, services, and digital recognition of refugee status; on the other hand, the journey of Venezuelan refugees to Brazil is marked by limited information and connectivity, highlighting the dimension of precariousness. Among the communication challenges[8] Venezuelans face, access to digital resources and Wi-Fi to obtain continuous and reliable information stands out as crucial.

In the tension between information precarity among Venezuelans and the digitalisation of migration borders, we seek to understand individual data provision practices and subjective notions of information privacy from the perspective of vulnerable

people. Among the Venezuelan migrants we interviewed, two prominent strategies emerged as a means to accomplish their objectives: 1) embracing a collaborative approach with authorities, and 2) navigating the complex balance between cooperative engagement and nuanced apprehension.

Logic of direct cooperation

Adopting a cooperative stance with migration authorities emerges as a pathway for Venezuelans to unlock the gateway to entry, stay and access to a myriad of benefits in Brazil. The following examples provide insights into Venezuelans' experiences with biometric data collection and willingness to cooperate with the procedure.

Andre expressed his surprise at seeing the biometric devices used for fingerprint scanning and iris recognition: *"It was different. I understood that it was to know better about who arrived in Brazil. I followed all the instructions and answered what they asked."*

Nora found biometric measurement devices strange until she learned that they were designed to identify unique characteristics of individuals:

> *"Well, I felt strange, but I understood that it was a way of identifying myself. At no time did I think anything bad, nor did I feel intimidated or anything. I was simply following the instructions they gave me."*

Maria was not surprised by the use of biometric technology and highlighted that going through the process of taking fingerprints and eye screening was necessary to cross international borders: *"It seemed very normal to me because I was already aware that to enter another country, they have to search you, they have to take your fingerprints, they have to go through that whole process, and it seemed normal to me, I didn't feel intimidated or harassed."*

Some of the refugees interviewed felt it was important to comply with the process to demonstrate their trustworthiness. Luz, a 41-year-old nurse, explained: *"I am transparent, I have nothing to hide. I came to work and help with whatever is needed. If that was the price to enter Brazil, deal done."*

There was also a perception of uniqueness or significance associated with undergoing biometric procedures. Edward reported that he was fascinated by the technology used in the biometric identification process: *"I was excited. I had never seen those electronic devices. I felt like I was in a James Bond movie; everything was computerised, modern and high-tech."*

Logic of cooperation accompanied by nuanced apprehension

Even while adopting a cooperative stance, Venezuelans simultaneously have concerns, contention and doubts regarding the provision of data to migration authorities. Sharing personal data was a daunting and apprehensive experience for certain refugees interviewed. Hector, a 19-year-old student, arrived in Brazil as a minor and recalled the anxiety he experienced:

> *"I had a little anxiety because I was a minor and thought they would send me back to Venezuela. When they put a machine to see my eyes, I thought: hmmm, can this machine tell my age?"*

Driven by his fear of being detected by the iris scanning machine, Hector felt compelled to disclose his age and the traumatic experience of enduring sexual violence as a means of sustaining himself. This disclosure ultimately enabled access to essential healthcare support and shelter. Others exhibited unease concerning the possible exchange of data between the Brazilian and Venezuelan governments. For instance, Yara, a 32-year-old digital influencer, expressed

her concerns about providing personal information because of political persecution by the Venezuelan regime.

Refugees' concerns over the provision of their data were also associated with the lack of information about the use and sharing of their data. Most interviewees had limited or no understanding of data management practices within humanitarian contexts. Some speculated that their data might be stored in a national security database and shared with other humanitarian organisations, like IOM. Mario recalled that when he was seeking employment with the organisation, they already possessed all his information, requiring him only to submit his curriculum vitae. Upon questioning the purpose of data collection, Karen received information from the border police stating that it was for security purposes and a requirement for entry into Brazil. However, they did not provide further clarification regarding the ownership or control of this data.

Further insights and recommendations

This article highlights the importance of critically assessing biometric data collection practices and developing collaborative public policies addressing the issue. Currently, access to benefits, including shelter and relocation, is contingent upon providing data to these systems, but Venezuelans are not granted access to manage their own information. Informing refugees about these systems and the data being collected is a vital initial step in fostering an environment where informed consent can be obtained with dignity and respect, but other aspects must be taken into consideration by policymakers, humanitarian organisations and technology developers:

- Digital access and literacy can be influenced by factors such as social class, gender, age, race and cultural background. These factors can shape refugees' experiences with reception, access to migration services, and the data collection process.
- It is crucial to ensure that refugees have unrestricted access to their own data storage platforms. Providing a dedicated space and autonomy for refugees to manage, update, correct inconsistencies, and even request the removal of their information through a formal withdrawal process are essential elements of a transparent data supply system.
- Consider the skills, insights and suggestions of refugees themselves to improve digital migration governance. Whether it involves creating platforms, data collection, information sharing, or implementing policies that impact refugee lives, it is crucial to incorporate refugees' evaluations and viewpoints to ensure their needs and experiences are adequately addressed.

Julia Camargo
Lecturer at the International Relations course, Universidade Federal de Roraima (UFRR – Federal University of Roraima) and PhD candidate, ESPM (Sao Paulo)
julia.camargo@ufrr.br

Amanda Alencar
Associate Professor of Media and Migration, Erasmus University Rotterdam
pazalencar@eshcc.eur.nl
linkedin.com/in/amanda-alencar-76563654/

1. *Names changed to protect respondents' identities.*
2. *bit.ly/technocolonialism-mirca-madianou*
3. *bit.ly/group-recognition-venezuelans-brazil*
4. *Part of the equipment purchased included products from Hikyvision, a globally renowned company specialising in electronic security solutions. However, this company had supplied similar equipment to the United Kingdom, Australia and the United States, which was subsequently deactivated in those countries due to concerns about unauthorised monitoring and data sharing.*
5. *bit.ly/registration-identity-management*
6. *bit.ly/sistema-acolhedor-venezuelanos*
7. *bit.ly/venezuelan-refugees-brazil*
8. *bit.ly/venezuelan-migration-northern-brazil*

Digital refugee resistance, power, representation and algorithmic censorship

By **Amanda Wells**

Refugees that attempt to use digital media for resistance face barriers, including algorithmic censorship and harassment, that solidify their position in the political margins. This demonstrates the need for greater transparency, accountability and democracy in digital governance.

Refugees and migrants' issues have often been embroiled in digital political action with varying degrees of success. The photos of Alan Kurdi, a two-year-old Syrian refugee who drowned while crossing the Mediterranean, are credited with fostering public empathy in the 2015 European 'refugee crisis' after their rapid spread through digital news and media platforms. Conversely, the use of social media to expose the conditions of Nauru's refugee detention centre in 2015 led to the eventual expulsion of oversight bodies like Save the Children from the grounds.

Here, I examine how social media is used *by* refugees seeking to garner public attention through visual outputs to the digital sphere like photographs and videos. Is social media an effective tool for refugee resistance? Drawing on the case studies of visual, embodied refugee resistance in Calais and Amsterdam, I demonstrate that current trends in digital governance push refugees further into the public margins and reduce their ability to weaponise digital media as a political tool.

Power and representation

Social media's particular strength is that it offers the ability for marginalised groups to express their political movements themselves rather than through the lens of a third party like news reporters and media outlets.

The accessibility of mobile phones and social media accounts quite literally places the power of representation into the hands of otherwise marginalised groups. They are thus free to conduct their political movements on their own terms. In the case of refugees, this is meaningful, as it offers an alternative to the traditional narratives that depict refugees as apolitical, passive subjects who are dependent on influential actors. From a purely visual standpoint, the proliferation of images depicting refugees in protest are a marked contrast to photos of refugees in the media – which often fail to show refugees' agency and instead emphasise vulnerability and precarity.

The 2016 protests in Calais' informal refugee settlement nicknamed 'the Jungle'[1] are an example of how refugees can use digital media to posit themselves as political actors outside of institutionalised political fora. In February of 2016, eight men who had been forcibly removed from their makeshift accommodations in the Jungle as part of a planned demolition, undertook lip-sewing to draw attention to the camp's resistance movement. The public-facing nature of the camp, coupled with the mobile technology of camp residents and NGO staff, resulted in a wide variety of visual outputs that remain relatively easily available online.

All of the eight protesters donned face coverings, hoods and scarves, to emphasise the collective nature of their protests. They held signs about the conditions of the camp, specifically calling out to their audience ('Representatives of the United Nations' one sign read), and referred to international human rights obligations. In doing so, the protesters demonstrated an understanding of the critical visual element to their resistance and attempted to shape the direction that their protests would take online.

Despite the protesters' active efforts to shape the media resulting from their acts, the photos were nonetheless altered by media outlets and photographers. A commonly circulated, professional photo changed the sign of one protester which read "Representatives of the United Nations and human rights come and bare witness; we are humans" to simply "We are humans." The photographer made a highly political decision to frame the subject in this way, and to edit the protesters' message, thinning the substantive thrust of the protesters' message, and in so doing, participating in a process of co-authorship over the constitution of the protests.

The example of the Calais lip-sewing protests demonstrates that although refugees are able to use social media for narrative change, they are ultimately subject to the interpretation and co-option of other actors. Even when protests may use digital media to bypass third parties or a lack of access to public political spaces, they remain highly subject to outside forces.

Algorithmic censorship and digital harassment

Social media censorship can occur through a literal deletion of content or the under-promotion of undesirable materials, thus limiting their audience and spread. There is a lack of publicly available information on the parameters and conditions by which social media algorithms operate, but they are broadly understood to censor or, at minimum, under promote graphic and offensive content. This would include whistle-blowing photos that report the conditions of refugee camps and detention centres, first-hand accounts of genocide and war, and protests that are centred within the body like lip-sewing and self-immolation.

Very little is known about how machine learning systems are trained for content moderation, but it is clear that algorithmic censorship is not nuanced. In an article in Philosophy and Technology Jeniffer Cobbe writes[2] "marginalised groups reclaiming abusive terms may seem to be abuse to the uninitiated" and therefore subversive material is censored alongside its target. Furthermore, a study by Koebler and Cox[3] found that algorithms are generally better at targeting and removing violent content than hate speech. This allows harassment surrounding refugee topics to proliferate while the voices from the centre of the issue themselves are further excluded.

Algorithmic censorship training occurs on datasets with pre-existing, real-word biases and inequalities. This means that content moderation models are poorly equipped to contend with racial and ethnic minorities, non-English materials, and non-dominant political leanings. These materials may be illegitimately censored[4] or under-promoted as a result.

In some cases, systemic algorithmic censorship and exclusion leads to the subjection of refugees to further digital harassment. In the case of Kambiz Roustayi, an Iranian refugee who self-immolated in Amsterdam's Dam Square in 2011, censorship

of the graphic images resulting from his protest meant that its only public record now exists largely on extremist websites and blogs. The only place that I located visual evidence of this event was on a small-scale website called 'Documenting Reality,' where the images were met with cruel comments. "We can all donate something for a good cause, to help people like this man. I am sending a gallon of petrol" read one comment. "God! People actually helped?" asked another.

Kambiz Roustayi now only exists in public memory in relation to the "smell" of his death, for being a "psychopath," and for being the "start to a bad day." This is an example of how, when graphic images resulting from refugee resistance are pushed into the political fringe due to censorship, they are subject to further discursive violence.

Karin Andriollo[5] writes of the ethics of attentiveness: "we ought to respond to the public self-sacrifice as if we turn the other way, protest suicides are killed twice, once by their own hands and once by the silence of our imaginations."

Memory is powerful, and social media can be an effective way to expand the public archive to include those who were marginalised throughout their lives. However, the case of Kambiz Roustayi demonstrates that growing automatic censorship, although perhaps intended to undercut harassment, may lead to its proliferation. This, in turn, reduces the potential utility of social media for political protest and a radical, inclusive ethics of attention. It instead gives way for the further oppression of refugees and migrants. In this way, algorithmic censorship creates the circumstances that allow for the cycle of discursive and physical violence against refugees to continue.

What is needed?

I have argued here that social media can be useful in refugee resistance, but that algorithmic censorship, which both prioritises content from privileged creators and removes graphic content from refugee resistors, weakens its potential.

In light of increasingly complicated issues in content moderation, such as AI generated propaganda and deep fakes, digital platforms must be transparent about the conditions of algorithmic censorship. Opaque algorithmic decision-making is a threat to the collective choice to define our public attention and memory. We, as digital end-users, practitioners, and lawmakers must push for greater accountability, democracy and transparency in digital governance.

Amanda Wells
Independent Researcher
amanda.morgan.wells@gmail.com

1. *The name "the Jungle" has been rightfully critiqued by many for its attempt to Other camp residents and paint them as barbaric and dangerous. I use the name here for clarity, as "the Jungle" refers to a specific time period and encampment structure in the lengthy history of migrant settlements in the area.*
2. *bit.ly/algorithmic-censorship-social*
3. *bit.ly/how-facebook-moderation-works*
4. *bit.ly/ai-moderation-freedom-expression*
5. *bit.ly/imagining-protest-suicide*

Technocolonialism and biometrics: reinvigorating the call to decolonise aid

By **Quito Tsui** and **Elizabeth Shaughnessy**

Humanitarian organisations are increasingly calling for the decolonisation of the sector, but this often overlooks colonialities reproduced by technology. By scrutinising the deployment and ubiquity of biometric technologies in the sector, this article seeks to reinvigorate sincere efforts towards decolonisation.

The legacy of colonialism runs deep in the humanitarian sector. Indeed, the uneven power relations and dynamics of the colonial era are on stark display in a sector where minority world organisations continue to assert their priorities above majority world communities. In recent years, humanitarian organisations have increasingly called for decolonisation, but these discussions are still nascent, and the shapeshifting nature of coloniality makes it an immense task. While these conversations and efforts rightly scrutinise power structures within humanitarian operations, for example in programming and fundraising, coloniality in technology is frequently overlooked. The lifecycle of humanitarian technology – how it is developed and deployed – and how subsequent data is collected and processed warrants scrutiny.

This article discusses the interplay between colonial and capitalist tendencies and humanitarian work. By querying the paternalistic idea that identification should be a prerequisite for service delivery for instance, we can start to unpick the colonial assumptions of integrity that are entangled with biometric technologies. Ultimately, in scrutinising the deployment and ubiquity of biometric technologies in the humanitarian sector, this article seeks to reinvigorate sincere efforts towards decolonisation.

Colonialism, coloniality, decolonisation and decolonial futures

Decolonising humanitarianism is a process that requires a simultaneous awareness and analysis of the past, present and future. Though colonialism itself refers to events in the past, of the subjugation and resource extraction of non-western territories and peoples, coloniality demonstrates the continued cultural, political and economic inheritance of colonial systems in the present day.

The humanitarian sector bears the mark of both colonialism and coloniality. Humanitarian colonialism for instance points to the complex relationship between humanitarian ideals and colonial narratives about the neediness of colonised groups. While this does not mean humanitarian work is undertaken with colonising intentions, it does mean that humanitarian work is shaped both implicitly and explicitly by coloniality.

Experiences with biometrics in the humanitarian sector demonstrate how technology can mimic, reintroduce and further entangle colonialist processes and power dynamics. This nexus of technology and coloniality is best described as technocolonialism, a term coined by Dr Mirca Madianou in 2019. Two key elements discussed of technocolonialism apply to

the use of biometrics: the reproduction of colonialities of power and the extraction of market value from humanitarian contexts.

Biometric technologies and humanitarian operations

The uptake of biometric data collection in registration and service delivery means the technology has become embedded in humanitarian operations. Following repeated recent examples where biometric data was improperly collected, shared or accessed, and where biometric technology failed or was misused, humanitarian organisations are questioning the role biometrics now play in the sector. But criticism of biometric systems has faltered despite new harms arising from the use of such systems including UNHCR sharing the biometric data[1] of Rohingya refugees with the Bangladesh government, which then shared it with Myanmar; the Taliban gaining access to sensitive biometric data[2] left by minority world donors; and displaced people being excluded from services because of their registration on biometric databases in both Kenya[3] and India.[4]

Those who defend the use of biometrics argue that they help to reduce fraud, make aid programmes more efficient, and benefit programme participants by providing a unique method of identification (e.g. their fingerprint or iris scan). However, research into this issue[5] has repeatedly revealed a lack of evidence to back up these claims. Moreover, increased focus on data protection and the data rights of individuals affected by humanitarian responses has led to questions about whether the risk of using biometrics is worth the potential benefit. Organisations have responded differently to these reflections resulting in the absence of a coherent sectoral approach to biometrics. Without clear norms and practices individuals harmed by biometric systems have been unsuccessful in their search for accountability.

Biometric narratives reproduce colonialities of power

A key aspect of colonialism is its insidiousness – the manner in which coloniality seeps into everyday actions and causes harm. In the case of biometrics it is important to scrutinise both the technology and the conversation around it: what claims are made about biometrics? The humanitarian purposes attributed to biometric use are built upon a set of assumptions around how humanitarian organisations should relate to impacted communities. Digging deeper into the foundational questions about why identification and verification with this particular technology are necessary uncovers how these assumptions are rooted in and reproduce coloniality.

For instance, narratives around the need for biometrics to address fraud assume not only that the person in need of aid may commit fraud in order to receive or access more aid, but also that the problem of fraud at beneficiary level is significant enough to warrant the mass collection of sensitive biometric data of all beneficiaries. Even when evidence[6] shows that fraud at the beneficiary level is minimal and that it is more of an issue in the supply chain, the narrative of the fraudulent beneficiary persists, reinforcing the criminalisation of already vulnerable people.

Narratives of fraud centre a power dynamic wherein recipients are positioned as untrustworthy actors within the resource-constrained environments of the humanitarian sector. Against this backdrop, the use of biometric technologies helps to reassert the primacy of humanitarian organisations as the arbiters of how limited resources should be fairly divided.

By positioning humanitarian organisations as the arbiters of access and recipients as untrustworthy actors who must prove themselves truthful and deserving, biometrics facilitate the continued categorisation of individuals according to minority world definitions of personhood. In this understanding biometric technologies are used to place the loci of control firmly within the grasp of humanitarian organisations. Impacted communities have limited ability to challenge or question the system, and crucially have few pathways to redress when systems go awry.

Funding streams driving mass biometric collection

The dominance of key decision makers in funding streams has cemented the influence and preferences of powerful Global North nation states and international organisations. Much of the sector's use of biometrics stems from UN agencies who have included the collection of biometric data within their long-term strategies. For example, through The Grand Bargain in 2016, UNHCR committed to expand[7] the use of biometrics for refugee registration to 75 operations globally by 2020. As of 2023, this has expanded to 90 operations.[8] Importantly, commitments by WFP and UNHCR to The Grand Bargain for increasing the use of biometrics in operations are related to the 'reduce management costs' workstream.

Notably, the organisations collecting biometrics are funded primarily by Global North governments, many of whom have an interest in the collection and use of biometric data. Though there are some public agreements between UN agencies and governments, often there is a lack of transparency around how biometric data will be used and by whom. The US government, for example, is both a funder of UNHCR and requires UNHCR to share biometric data for every refugee referred for resettlement in the US. This data is permanently stored[9] in a linked web of US government databases, even though less than a quarter of those referred are ultimately accepted for resettlement.

Inability to access data sharing agreements limits the ability of impacted individuals and civil society to gain insights into how data is governed. Where there is a lack of transparency, we cannot rule out the possibility that there is a connection between surveillance efforts, including counterterrorism and military purposes, and biometric collection.

Currently, the narrative of efficiency and fraud control has prevailed over discussions of harm; this includes the research noted above demonstrating the entanglement of biometric technologies in other extractive data practices, as well as discomfort and concern vocalised by impacted communities themselves. By embodying the preferences of funders, the use of biometrics prioritises external actors and limits the scope of choice, agency and possibility for local actors.

Extraction of market value from humanitarian contexts

Technology and coloniality in the humanitarian sector are both intertwined with and mutually reinforce other systems of power, including capitalism. Capitalism is by definition unequal and extractive (i.e. in a world of limited resources, there are those who have capital and those who do not have capital). Whereas decolonial theory posits that truly decolonial futures are anti-capitalist (and anti-racist and feminist), we have yet to meaningfully unpack the conflict of interest between for-profit (capitalist) technologies and non-profit (decolonising) humanitarian programmes. The increasing role of private sector companies in the

deployment of technology in humanitarian spaces warrants discussion. One example is WFP's partnership with Palantir,[10] a CIA-backed company that gained infamy due to its immigration enforcement support.

When technology is developed in the Global North by companies accountable for delivering dividends to their shareholders, many of the technologies ultimately deployed in the humanitarian sector are not designed by or for those who end up using it or those whose data is collected. Simply put, technology development is reflective of where funding comes from.

This extends to biometric technology. Issues with fingerprint scanners not operating properly on those with darker skin tones or who are agricultural or manual labourers, or diminished functionality of iris scanners with elderly people, can lead to exclusion from services. Currently, little data has been collected on the rates of failure, but in humanitarian contexts, where biometrics are often mandatory for accessing basic necessities, the consequences of biometric technology failing could prevent individuals accessing critical necessities and services.

Biometric technology is not typically developed for humanitarian contexts, or by or for those who must use it. In many of the examples where biometrics have been introduced into humanitarian programmes, this has been done mandatorily, either as the only option given to identify and verify a person or by the exclusion of alternatives. The enforced use of previously untested technology in the humanitarian sector raises concerns around the meaningful consent of communities.

The excitement – and funding opportunities – over 'innovation' in the sector, which sees humanitarian organisations increasingly introducing potential sources of risk through the adoption of unproven technology, renders humanitarian contexts a testing ground for experimentation. There is generally good recognition amongst humanitarian practitioners of the need for ethical and responsible pilot design. However, the growing experimentation with technology[11] in the sector, where private sector technology is used or where funding is directly provided by private companies, presents an inherent tension between desirable outcomes and the replication of a colonial pattern where technological advances are used to scrutinise those in the majority world.

Conclusion

Ultimately, biometrics are by nature physically invasive and extractive. As humanitarian agencies collect, measure and extract information from a person's physical body in order to assess their worthiness of trust and aid, biometrics mimic particularly nefarious expressions of historic colonialism. It is difficult then to justify this extraction of biometric data en masse, especially when paired with experimentation and financial benefit for technology developers.

Though there is an awareness and admission of the potential harms of biometric use, many organisations shy away from asking the fundamental question: are narratives about fraud and efficiency enough to balance out the risk of introducing these technologies? Given the degree of potential harm, we believe the answer is no. The reluctance and lethargy around confronting the real and acute trade-offs of biometric use render decolonisation efforts insincere.

Decolonising humanitarian operations in practice has proven incredibly complex. Moving too fast can shift burdens to local partners rather than power. Equally, moving too slow means the continuation of harmful

practices and the potential introduction of new forms of coloniality. Alternatives to highly extractive biometric technologies are possible; work by CISPA and the ICRC into privacy-preserving[12] humanitarian aid distribution and the use of non-biometric forms of identification in the humanitarian response in Ukraine[13] demonstrate the need to consider both the why and the how of technology uptake in the sector. Taking the decision to interrogate the use of such technologies is an important way to avoid replicating new colonialities in humanitarian work, and creates opportunities to meaningfully engage in holistic efforts to decolonise the wider humanitarian sector.

Quito Tsui
Research Consultant, Independent
linkedin.com/in/quito-t-2ab118133/

Elizabeth Shaughnessy
Digital Programmes Lead, Oxfam GB
linkedin.com/in/elizabethshaughnessy/

1. *bit.ly/un-shared-rohingya-data*
2. *bit.ly/biometric-data-systems-imperil-afghans*
3. *bit.ly/double-registration-kenyan*
4. *bit.ly/indias-biometric-voter-id-databases*
5. *bit.ly/biometrics-humanitarian-2023*
6. *bit.ly/biometrics-humanitarian-sector*
7. *bit.ly/the-grand-bargain*
8. *bit.ly/digital-identity-registration*
9. *bit.ly/dhs-collecting-biometrics*
10. *bit.ly/statement-wfp-palantir-partnership*
11. *bit.ly/challenges-humanitarian-experimentation*
12. *bit.ly/not-yet-another-digital-id*
13. *bit.ly/demand-sensitive-biometric-data*

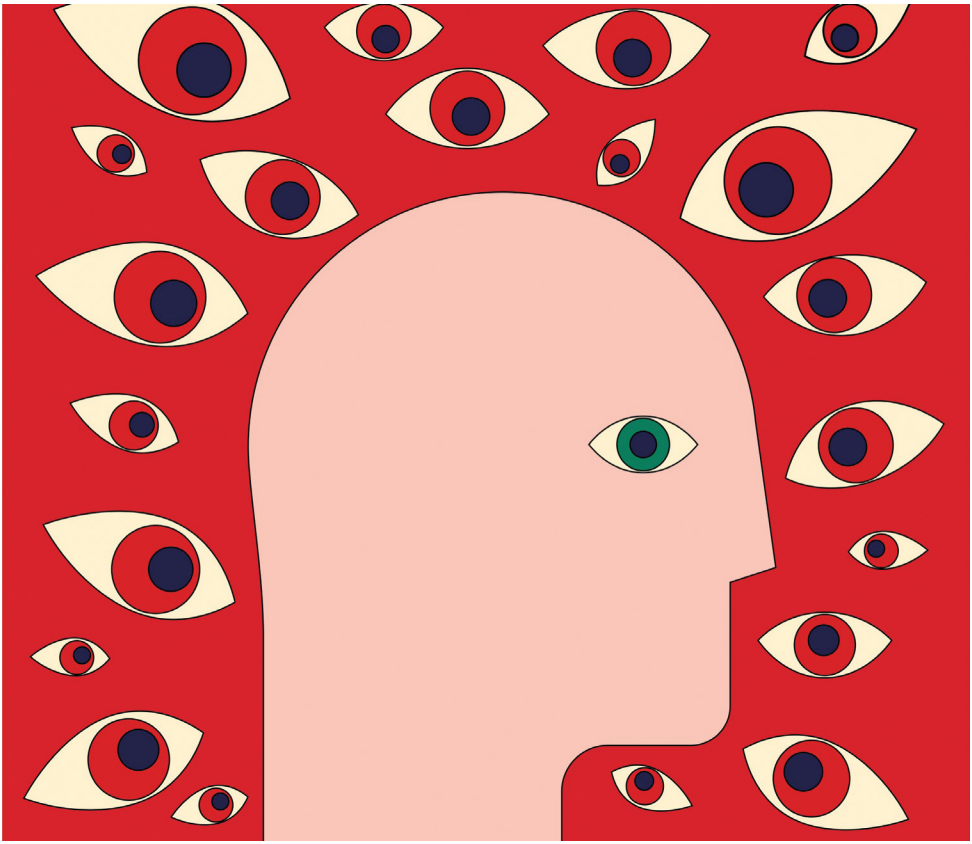


Image sourced from Unsplash

Challenges and risks associated with biometric-enabled cash assistance

By **Roda Siad**

Cash-based interventions may have the potential to foster empowerment, autonomy and self-reliance, but unequal implementation and politics surrounding biometric-enabled cash assistance threaten the chances of achieving these aims.

While biometric identification systems and cash-based interventions are not new and have long histories in the humanitarian aid sector, the binding of biometric verification to cash and voucher assistance (CVA) is a relatively new phenomenon. Beginning in 2013, the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP) introduced biometric verification technology in Kenya to ensure efficiency and accountability in how aid is distributed. Refugees are biometrically enrolled into the UNHCR registration system known as PRIMES using the Biometric Identity Management System.

Biometric technology captures the physiological characteristics used to uniquely identify an individual, including fingerprints, iris scans and facial recognition. In the case of CVAs, biometric technology is used in conjunction with other technologies that deliver cash assistance, including mobile technologies and distributed ledger technologies (i.e. blockchain technology). Over the past two decades, biometric technology has become an integral part of UNHCR operations and is on the rise because of its purported accountability and assurance to donors, as well as regulatory requirements from service providers. In Kenya, due to national legislation, cash programmes must adhere to the Know Your Customer (KYC) and other government requirements for obtaining SIM cards and bank accounts.

The CALP Network recently released *The State of the World's Cash Report 2023*,[1] which shows that CVAs now account for 21% of all humanitarian assistance. Cash-based intervention as a modality for delivering assistance offers many promises. First, it promises a rapid, efficient and cost-effective way for humanitarian actors to ensure that aid reaches areas affected by conflict and disasters. Secondly, it promises empowerment, autonomy and dignity of choice for affected peoples, including refugees, as well as stimulating the local economy. By tying biometrics to cash, humanitarian actors claim it will help with accountability, prevent duplication and fraud, and ensure that aid gets to the right individuals. However, biometric-enabled cash assistance can also be political.

This article offers insights into how (and why) cash distribution is approached and experienced differently in and within individual countries, in emergency and protracted crises. I argue that unequal approaches to cash delivery using biometrics could hinder any efforts to promote independence and dignity of choice and can intensify exclusion.

A refugee woman provides biometric data to verify her eligibility to receive the monthly cash-based assistance in the Kalobeyei settlement. Credit: Roda Siad

Variations in cash programming

The CVA ecosystem is complex and involves collaboration between a host of actors including UN agencies, donors, host governments, NGOs, tech companies and financial service providers (FSPs), each with their own requirements which have implications on the design of the intervention.

Kenya's Dadaab and Kakuma refugee camps and the Kalobeyi settlement offer good case studies for how cash transfer programmes can vary. Bamba Chakula (Swahili for "get your food") is the WFP's cash transfer programme and is delivered using a digital wallet and mobile phone. Through a partnership with Safaricom, WFP assumes guardianship for the SIMS it provides refugee beneficiaries. Money is transferred to the digital wallets of beneficiaries, who then redeem it with designated traders contracted by the agency. Refugees in the Dadaab camp are restricted to receiving this money in the form of digital vouchers meant for designated food vendors for fear that funds could be used for terrorism or other money laundering activities, while refugees in the Kalobeyei Integrated Settlement receive unrestricted cash.

Dadaab, which is made up predominantly of refugees from Somalia, has long been a point of contention, with the Kenyan government threatening to shut down the camp numerous times over the years citing security concerns. Kalobeyei, along with the

Kakuma camp, are home to mainly South Sudanese refugees. As one WFP worker in Dadaab explained to me, a programme can present differently in each location because agencies must adhere to the requirements set by the host government.

Problems with restricted cash transfer and biometrics not being recognised

> *"In Dadaab, I think the government is a bit hesitant to move to unrestricted cash for various reasons, one being insecurity because once you put a lump of money there, you never know what is happening with the money. Maybe it's sponsoring some of these activities the government doesn't support, like what is happening with Al-Shabaab."* – WFP Supply Chain Officer

I spoke with refugees in Dadaab about their experiences with biometrics and cash transfer. Their perspectives challenge the narrative that freedom and dignity of choice automatically come with CVA.

In Dadaab, Kakuma and Kalobeyei, refugees go through biometric verification each month to receive assistance. If they fail to appear for food distribution for three months, the card is deactivated. While biometrics are often presented as a reliable means to identify and verify beneficiaries, I spoke with some refugees who told me that their biometric data are not always recognised. I interviewed Haroun, a mechanic, who explained that sometimes his biometric data are not recognised, causing delays in accessing the cash:

> *"I missed Bamba Chakula last month because they said my fingerprints had not been detected. When my fingerprints are not found, my wife comes and scans her finger."*

Another camp resident, Zahra,[2] explained her frustation at not being able to purchase the food items she needed:

> *"Only some shops can accept, and they force us to take food items from their shops. If I ask for the 1000 shillings to buy other food, he says no. You can only take what is here. What I need, he doesn't have. So, if you're not free to get what you want, then what's it good for?"*

Although the cash transfer is intended for food, it is common for refugees to use it to purchase other necessities, such as medication, or pay for services, including school fees. I learned from one of my focus groups with refugees living in Ifo that it is common to ask vendors to exchange their vouchers for cash at a cost to buy medication – a cost that decreases the value of the voucher.

> *"You have to buy medicine if you have somebody sick at home... so you negotiate with that person [the vendor]. If you say it's for medicine, he will give it to you. As soon as he hears somebody is sick and you don't have money, he will pull the money and give you."* – George

The use of biometrics as a condition for cash assistance eligibility also helps to maintain a system where refugees feel trapped in the camp. Fingerprint verification is needed monthly to keep their cards active. The money cannot be accessed outside of the camp, in Nairobi for example. Some young people explained to me that the fear of losing Bamba Chakula is one of the factors keeping them there, even though there are limited work opportunities in the camp. If they were to leave, there would be no guarantee of finding work, which could make them more vulnerable.

Data protection risks

There are serious potential risks associated with collecting and storing biometric data. Since private and public actors may be involved, humanitarian agencies have little control over how data could be used once they are shared. Depending on how and where the data are stored, there may also be risks of hacking and data breaches.

The incorporation of biometrics and other technologies into CVA poses risks around consent, privacy, data protection and responsibility. There have already been public examples of what happens when sensitive and immutable data are not protected. In 2021, the government of Bangladesh shared the biometric data[3] (collected by UNHCR) of 830,000 Rohingya refugees with the government of Myanmar for repatriation assessment. That same year, biometric devices belonging to the US military were seized by the Taliban[4] during its takeover. This led to concerns from civil society groups that humanitarian data (including biometrics) collected in Afghanistan would also be compromised.

The use of biometrics varies across operations. We can see this in how UNHCR and its partners have responded to global emergencies. In recent emergency operations in Afghanistan, Yemen and Sudan, biometrics were a requirement to access cash assistance. UN agencies have attempted to implement various accountability measures, including biometrics and GPS tracking, in response to allegations of fraud and aid diversion, some of which resulted in disputes with local governments and the suspension of aid.[5]

Ukraine: a shift away from biometrics or an exception?

A different approach was taken in the response to the Ukraine crisis.[6] Agencies opted to forgo the biometric identification requirement and use other means to provide unrestricted, multipurpose cash assistance in one of the largest emergency responses, with projections of more than one billion disbursed since November 2022. A commentary from Human Rights Watch described the Ukrainian response as a *shift* and a "significant step in the direction of protecting the rights of people who use aid."[7]

A closer look, however, reveals that it may not be a shift but rather an exception. This was in part due to the unique context of the Ukraine crisis, where refugees and IDPs had pre-existing identification documents. The high literacy rate among Ukrainians may have helped them feel empowered to refuse the sharing of their personal data. There was also strong advocacy from the Ukrainian state, a coalition of NGOs and other civil society actors that pushed back against the use of biometrics. Many NGOs on the ground refused to collect biometric data and used other means of identification, including tax identity numbers, driver's licences and passports. The Ukraine Red Cross Society worked closely with the International Federation for the Red Cross and the Red Crescent Societies (IFRC), FSPs and government departments, including the Ministry of Social Policy, to monitor all aspects of the CVA. Ukraine also has clearly laid out national data protection laws and is governed by the European Union's General Data Protection Regulation (GDPR).

In December 2022, UNHCR deployed a blockchain-based payment solution[8] using the Stellar Network for cash distribution to affected people in Ukraine. Blockchain, a decentralised and distributed ledger that stores data permanently, was used in conjunction with mobile phones to give each person a digital wallet. Aid is distributed via a digital wallet using USDC,

a stablecoin pegged to the value of the US dollar. Recipients download an app, and a code is sent to their phone to verify that they are in possession of that phone. They confirm a unique piece of information about themselves, such as date of birth. Recipients can then use their driver's license to withdraw funds at a MoneyGram location. Similar to other cash assistance programmes such as AccessRC[9] which was developed by the IFRC, this is an opt-in programme which allows displaced Ukrainians to decide from one of three methods to receive assistance.

The risks of using biometric verification in the Global South

The use of biometric technology in humanitarian operations, and specifically in cash-based interventions, will likely not decrease but only continue to grow. As the use increases, so does the amount of personal data that is being collected, stored and shared. Such information may be accessed by the different public and private actors involved, including tech companies and FSPs.

Understanding the data security risks around cash programmes that require biometrics is key. Eighty-five per cent of displaced people are hosted in the Global South, where, unlike in Ukraine, data protection policies are often absent, underdeveloped or not enforced. Moreover, these laws rarely bring refugees and other displaced individuals into the folds of any protective frameworks.

Reflections on the broader implications

This article has shown how biometric-enabled cash assistance is administered and experienced differently across humanitarian operations. Host governments can influence how cash transfer programmes are designed and implemented (including refusing them entirely). As we have seen from Dadaab, biometrically enabled cash transfer programmes present several challenges for displaced people such as exclusion because their biometric data may not be recognised and limits on freedom and dignity of choice due to nationality and identity politics.

The distribution of cash through blockchain in the Ukraine response without biometric registration is an interesting development. However, it may not so much represent a shift in industry attitudes but rather an exception because of the strong advocacy from international and Ukrainian civil society. This demands the question: Who is going to advocate for the millions of refugees and displaced peoples in the Global South to ensure that they can benefit from cash assistance without compromising their privacy and freedom of choice?

Roda Siad
PhD Candidate, Communication Studies, McGill University
roda.siad@mail.mcgill.ca

1. *bit.ly/state-worlds-cash*
2. *Names changed to protect the identities of respondents*
3. *bit.ly/un-shared-rohingya-data*
4. *bit.ly/biometric-data-systems-imperil-afghans*
5. *bit.ly/houthis-wfp-aid-control*
6. *bit.ly/no-need-demand-biometric*
7. *Wille (2023)*
8. *bit.ly/unhcr-award*
9. *accessrc.ifrc.org/*

Navigating the legal landscape of double registration in Kenya

By **Wangui Gitahi**

Registration on the database of refugees in Kenya has placed Kenyan nationals at risk of statelessness. This article discusses how this came about and considers the importance of data security, privacy and subject rights.

Over 40,000 Kenyans are estimated to be victims of double registration, where their fingerprints appear in the database of refugees managed by UNHCR and the Kenyan government. This means that, although they are entitled to Kenyan citizenship, they cannot acquire national identity cards because they appear in the refugee database, leaving them in a form of registration limbo.[1] They cannot enjoy the full rights entitled to either refugees or Kenyans.

The national identity card and passport are the two documents that prove citizenship. When a person applies to the Kenyan government to obtain these documents, the government checks to see if their fingerprints match prints already in the UNHCR and government refugee database. If the prints are already in the refugee database, even if the person is not actually a refugee or is entitled to Kenyan citizenship, they will be denied Kenyan identity documents. This puts victims and their children at risk of statelessness.

Reasons for double registration

There are two underlying reasons a person might end up 'double registered,' that is, with fingerprints in the refugee database while being entitled to registration in the Kenyan government database of nationals:

i. When severely impoverished Kenyan nationals in communities near Dadaab and Kakuma camps realised that refugees were obtaining aid after registering in the UNHCR refugee database, some decided to register themselves in the refugee database in order to access aid.

ii. On citizenship, Kenya applies the principle of *jus sanguinis*, i.e. a child's citizenship is determined by that of their parents. The Constitution of Kenya requires only one of the parents to be Kenyan for the child to be a Kenyan, so a child born to a refugee and a Kenyan is entitled to citizenship. However, the children of Kenyans married to refugees were registered on the refugee database.

The influx of refugees from Somalia, Ethiopia and Sudan between 1991 and 2007 saw the introduction of the encampment policy in Kenya, with the establishment of Dadaab and Kakuma refugee camps. In addition, the government of Kenya surrendered its refugee management role to UNHCR. UNHCR was responsible for receiving and registering refugees and carrying out refugee status determination for asylum seekers. Subsequently in 2007, when the Refugees Act of 2006 was operationalised, the Department of Refugee Affairs (DRA) took over refugee management from UNHCR and took over the refugee database[2] in 2016.

In the 1990s Kenya was getting a huge

influx of refugees from Somalia as well as grappling with periodic droughts in northern Kenya where Dadaab and Kakuma refugee camps are located. Due to the history of marginalisation in the northern parts of Kenya, the droughts and under-development hit the local Kenyan communities hard. As a result, some ethnic Somali Kenyans from the host communities registered themselves and their children as refugees to access services provided by UNHCR and partner organisations like food aid, education, healthcare and, in a few cases, an opportunity for resettlement.

The problems with double registration began with the implementation of the biometrics system[3] by UNHCR from around 2007. UNHCR introduced biometric registration to better manage the hundreds of thousands of refugees living in the camps and address fraudulent cases that arose during food distribution. Food rations were given according to the number of people in a household. Some households were using the ration cards of absent family members to collect extra rations. Sometimes, extra food was traded for money, services, or other goods.

The biometric system made it easier for UNHCR to verify individuals' identities, but it also led to unintended consequences. Many Kenyan nationals were registered as minors without their consent and only realised that they were in the refugee database when they applied for the Kenyan national identity card at 18, when it was subsequently denied.

Furthermore, interactions between host community members and refugees led to marriages that bore children. Kenyan women who were married to refugees lived in the refugee camps, and their children, would be registered as refugees despite being Kenyan citizens by birth.

The impact of double registration on individuals

Without a national identity card, a person's movement is limited to within the locality of the camps. Limited freedom of movement limits their social and economic opportunities. Additionally, they cannot access government services, register a bank account, get a SIM card, register for MPESA (mobile banking) or engage in formal employment (although the law was changed in September 2023 to allow the refugee ID to be recognised for these purposes, the change has not yet been implemented in practice). One victim named Aden[4] explained that his political ambitions were thwarted: Since he could not register as a voter, he lost an opportunity to be nominated as a Member of the County Assembly (MCA) in his home county, Garissa. Aden eventually got his national identity card in July 2023 after participating in a vetting exercise conducted by UNHCR and the Department of Refugee Services (DRS).

In March 2021, the Kenyan government issued a 14-day ultimatum demanding that UNHCR develop a plan for the closure of Dadaab and Kakuma camps, failing which, refugees would be forcibly repatriated to their countries of origin. The ultimatum caused panic among victims of double registration who feared they would be forced out of their own country. The NGO Haki na Sheria filed a petition[5] challenging the government's actions and obtained interim court orders halting the repatriation. The main petition is yet to be determined. However, a separate petition filed by the Kituo cha Sheria and others challenging the government's ultimatum on camps closure was allowed on 15th March 2024.

Resolving the issue of double registration

Double registration raises pertinent questions about data security, privacy,

consent and data processing. The effects of these challenges are only now being felt years after the data of most double registrants was collected. UNHCR adopted its first policy on data protection in 2015 and adopted the most recent iteration[6] in 2022. Kenya's Data Protection Act (DPA) was passed into law in 2019. Both the policy and the DPA now have provisions that should remedy the challenges of double registration if they are followed to the letter.

Under the DPA, victims of double registration fall under the category of data subjects. The act defines a data subject as an identified or identifiable natural person who is the subject of personal data. Section 26 of the DPA gives the provisions of the rights of a data subject. They include the right to:

a) be informed of the use to which their personal data is to be put;

b) access their personal data in custody of data controller or data processor;

c) object to the processing of all or part of their personal data;

d) correction of false or misleading data; and

e) deletion of false or misleading data about them.

If this option had been provided earlier, victims of double registration who had their biometrics taken when they were minors would have had the opportunity to correct the error before the data was transferred from UNHCR to the Kenyan government.

The DPA also contains provisions on data security and data privacy. In Kenya, the right to privacy is guaranteed in the Constitution of Kenya, 2010. The DPA gives effect to this right by providing regulations on the processing of personal data, establishing the rights of data subjects, and setting forth the obligations of those who control and process data. Most importantly, the act provides for the Office of the Data Protection Commissioner whose main mandate is overseeing the enforcement of the act.

The Kenyan government is well aware of the double registration problem and has been conducting vetting exercises[7] to remedy the situation; the most recent one took place in August 2023. The government embarked on a vetting exercise to de-register Kenyans who are in the refugee database. The exercise takes a long time because the security and intelligence personnel in the Kenyan government have to be engaged to avoid cases of fraud.

In 2023, the Kenyan government embarked on the formulation of a socio-economic inclusion plan for refugees and host communities dubbed Shirika plan[8] in line with the provisions of the Refugees Act, 2021. The plan aims to:

a) ease the pressure on refugee-hosting communities in Garissa, Turkana and urban areas by mobilising additional financial, technical and material support in the spirit of responsibility sharing;

b) facilitate the transition from refugee camps to integrated human settlements and robust economic hubs;

c) enhance refugee and host community socio-economic inclusion for enhanced self-reliance and resilience; and

d) facilitate the transition of refugee basic service delivery from a humanitarian-led approach to government systems.

The Shirika plan envisions six key components with the first one focusing on systems building and enabling policy frameworks. Although the issue of double

An example of a Kenyan national identity card. Credit: Wangui Gitahi

registration is not explicitly stated in the plan, it falls under this component, which primarily deals with the rule of law and justice.

Conclusion: raising awareness of data security and the risks of double registration

According to Haki na Sheria's 2021 report, it is estimated that there are over 40,000 victims of double registration. The Refugees Act of 2021 attempts to address this issue by criminalising double registration in Section 41(3).

"A person commits an offence if that person: Being a Kenyan citizen, knowingly applies or obtains recognition, admission, or registration as an asylum seeker or refugee in Kenya; Being a refugee, knowingly applies for a Kenyan identity card or passport…."

The law states that anyone convicted of the charges above will pay a fine of up to Kshs 500,000 or 3 years imprisonment or both. Although there have not been any reports of refugees or Kenyans charged under this section, the law takes a very drastic approach. Given the humanitarian circumstances that drove most victims to register as refugees due to drought and under-development in their counties, the law may be further marginalising an already marginalised group of people.

In conclusion, the digital revolution has undoubtedly revolutionised refugee management and the storage of personal data while presenting opportunities as well as challenges. This article has shed light on the complexities surrounding double registration from a legal standpoint. It is evident that while digital technology has improved refugee management, it has also posed risks to privacy, data security and statelessness. Moving forward, enhancing public awareness and education regarding the implications of double registration and the vulnerabilities of personal data in digital databases is crucial. Both refugees and host community members ought to be empowered about the potential risks involved to foster a more informed society.

Wangui Gitahi
Senior Protection Officer, Amnesty International Kenya
wangui.gitahi@amnesty.or.ke
linkedin.com/in/wangui-gitahi-817a19152

1. *bit.ly/id-leaves-you-without-identity*
2. *www.unhcr.org/ke/registration*
3. *bit.ly/biometric-purgatory*
4. *bit.ly/kenyan-id-card-sense-belonging*
5. *bit.ly/petition-kenya-repatriating-somalia*
6. *bit.ly/personal-data-protection-unhcr*
7. *bit.ly/kenyans-acquire-citizenship*
8. *bit.ly/kenya-shirika-plan*

The *ejajot* of Rohingya refugees in the age of digital humanitarianism

By **M Sanjeeb Hossain, Tasnuva Ahmad, Mohammad Azizul Hoque** and **Tin Swe**

This article outlines the circumstances that led to the *ejajot* (informed consent) of many Rohingya refugees not being taken during the joint verification exercise, which ultimately led to the biometric registration of almost a million Rohingya people.

In the past few years, we sought to understand at a deeper level how the forcibly displaced Rohingya people living in Bangladesh participated in the biometric registration processes at the core of a *joint verification exercise* launched by the Bangladesh government and UNHCR in 2018. We were particularly drawn to this topic after Human Rights Watch[1] (HRW) claimed in 2021 that the Bangladesh Government had shared the collected biometric data with the Myanmar Government without the informed consent of Rohingya refugees. UNHCR disputed this claim almost immediately.

To unearth whether informed consent had been taken, we organised seven focus group discussions (FGDs), which allowed us to have candid conversations with Rohingya refugees and representatives of several local NGOs that partnered with UNHCR during the joint verification exercise. Through the informal trust network[2] of the Centre for Peace and Justice, we also collaborated with six Rohingya refugee volunteers who conducted key informant interviews with 12 Rohingya refugees whose testimonies were subsequently transcribed and analysed by the authors of this article.

As we reflected on our conversations, we realised that while informed consent as a concept within the context of data protection was not something that many Rohingya people were familiar with, the underlying principles of this concept did indeed exist in the form of *ejajot*, a word from the Rohingya language. This is the story of the circumstances that led to the *ejajot* of many Rohingya refugees not being taken by the Bangladesh government and UNHCR during the joint verification exercise, which began in 2018 and ultimately led to the biometric registration of almost a million Rohingya people by the end of 2023.

The biometric registration drive in the Rohingya refugee response

Immediately after the mass displacement of Rohingya refugees in August 2017, the Bangladesh government's Ministry of Home Affairs, with 'technical assistance' from UNHCR, began the process of biometrically registering Rohingya refugees.[3] Despite criticisms[4] concerning the exploitative aspects of collecting and using the data of the Rohingya people, the biometric registration processes were deployed at full speed over the next few months.

It was in the first Joint Response Plan (JRP)[5] of 2018 that key partners prioritised the need to "harmonise existing databases" and produce "a unified database" that would have "biometric information [of] the whole refugee population". According to the JRP, securing the identities of refugees "through registration and documentation" would enable refugees to "exercise their rights",

A Rohingya refugee in Ukhiya in Bangladesh heads home carrying a gas cylinder. A biometric ID card is needed to access these cylinders which are used for cooking. Credit: Abdullah Habib (Rohingya refugee)

facilitate the targeted providing of assistance "to people in need", "achieve equity in assistance delivery", "control duplication and manipulation of beneficiary lists", and finally "facilitate solutions".

In early 2018, the Bangladesh government and UNHCR signed a memorandum of understanding relating to data sharing. Although this agreement remains confidential, according to a UNHCR Operational Update,[6] it ensured that the "use of information for purposes other than assistance and identification or transfer to third parties would need to be approved by UNHCR". In June 2018, the Bangladesh Government and UNHCR launched its joint verification exercise[7] as a consequence of which, by the end of December 2023, 971,904 Rohingya people received "credit card-sized plastic IDs" in exchange for their biometric data.

In the course of our fieldwork, we realised that it was not just the scholarly community that expressed reservations over what was more or less an unregulated biometric registration drive. We knew from past literature that the Rohingya community was unhappy because the ID did not, for unfathomable reasons, acknowledge their ethnic 'Rohingya' identity.[8] They felt that the ID card should have recognised their

'Rohingya' identity, for which they were not just marginalised but also persecuted. In protests that ensued, the Rohingya people expressed their dissatisfaction over the lack of transparency surrounding the exercise and for not being engaged at all when the ID was being designed. They were also fearful of UNHCR and the Bangladesh government sharing their data[9] with authorities in Myanmar "which could use the information against them".

As our conversations with our interviewees progressed, it became apparent to us that many belonging to the Rohingya community were sceptical of having their fingerprints taken and their irises scanned. They recalled feeling alienated from and unfamiliar with such digital data collection methods. Many of them told us that while they were assured that they would benefit from being biometrically registered, they felt like 'voiceless subjects' in an overarchingly foggy process. So, in the end, what led to nearly a million Rohingya people participating in a biometric registration drive of such massive proportions?

The *ejajot* of Rohingya refugees on the side-lines

In its 2021 statement[10] responding to Human Rights Watch, UNHCR claimed that before taking their biometric data, each refugee family was "informed of the purpose of the joint registration" and was asked "to consent to their data being shared with partners on the ground" to facilitate receiving assistance. It clarified that the registration exercise was also used "to establish Rohingya refugees' former residence in Myanmar and right to return", and to that end, "refugees were separately and expressly" asked to consent to have "their data shared with the Government of Myanmar by the Government of Bangladesh".

UNHCR assured that "a widespread counselling and information campaign" was set in motion "to explain the exercise" and to "inform refugees that they would all be able to access the same services and entitlements, regardless of their consent to share their data with the Government of Myanmar". Furthermore, UNHCR claimed that individual counselling sessions were held in the language understood by the Rohingya people to make sure that they "fully understood the purpose of the exercise" by "responding to their questions and concerns" and also to help them "make an informed decision". UNHCR also stated that it had been made absolutely clear to the Rohingya people that consenting to have their data shared with local partners to receive assistance as opposed to having their data shared with Myanmar was unconnected to each other. Even if they refused to have their data shared, they "would still access the same assistance and entitlements as all others". This amounted to each Rohingya family's consent being "confirmed at least twice" and signatures confirming consent being "only obtained following this double-confirmation". In essence, UNHCR's position is that it took the informed consent of Rohingya refugees before and also during the biometric registration drive.

While the recollections of our interviewees from the Rohingya community and representatives of local NGOs bear some similarities with UNHCR's claims, they also mark important points of departure. Many of our Rohingya interviewees had never heard of the English words 'informed' and 'consent'. However, as we explained what 'informed consent' meant, they quickly pointed out that what we described was aptly captured by the word *ejajot*. A Rohingya refugee quite poignantly explained:

> "Ejajot *confirms our* mon-er iccha *(the desire of our mind). Suppose an unknown person approaches me and asks about my family details. I will likely feel uncomfortable sharing the desired information with him or her. To share, I need to first be satisfied with this person. I need to agree that I will share my information. This* iccha *(desire) is essential. I need to give you permission, my* ejajot. *Taking my* ejajot *is paramount because this guarantees that you will treat my information correctly.*"

Not a single Rohingya person we spoke to felt that his or her *ejajot* had been taken. They acknowledged receiving explanations from their respective *majhis* (community leaders) and local NGO representatives about the purpose behind the biometric registration process. Some recalled being told that biometric registration would facilitate receiving rations and expedite future repatriation initiatives. However, many also claimed that the organised awareness sessions did not adequately explain what they were a part of. A Rohingya refugee, echoing the views held by many of the other participants of the focus group discussions, said:

> "*The [biometric] registration process began soon after we arrived in Bangladesh. We were in a state of trauma. We just did as we were told and got registered. It was a very rushed process.*"

Alarmingly, echoing past claims, many of our Rohingya interviewees alleged that those who initially resisted or refused to take part in the biometric registration drive were informally told by representatives of the government and UNHCR that if they did not change their minds, they would not receive rations in the future, be able to work inside camps or repatriate to Myanmar. In not so many words, the Rohingya people never had a real option to refuse to participate in the biometric registration process. They were merely presented with an illusion that their informed consent, their *ejajot*, had been taken.

Issues with the concept and practice of taking informed consent

The manner in which the Bangladesh government and UNHCR launched the joint verification exercise in 2018 and subsequently collected large amounts of biometric data, and the analysis presented in this article showing how the *ejajot* of the Rohingya people was not taken, raises important questions concerning the meaning of informed consent in the age of digital humanitarianism.

During our focus group discussions and key informant interviews, we often wondered to what extent our Rohingya interviewees were really concerned or bothered by the fact that their *ejajot* had not *really* been taken. From the tone of their voices and facial expressions, we were left with the impression that while the Rohingya people understood and valued the concept of *ejajot*, it was not a pressing concern to them.

At the expense of sounding provocative, is the bar envisioned by Human Rights Watch in relation to informed consent unrealistically high? After the sudden mass displacement of hundreds of thousands of Rohingya people in 2017, to what extent was it really logistically possible to individually gain the *ejajot* of every single Rohingya refugee before taking biometric data? How can a community that has been marginalised decade after decade be expected to easily understand the value of data and give their informed consent or *ejajot*? By focusing on the absence of *ejajot*, are we diverting attention away from more

pressing matters concerning the plight of Rohingya refugees? Is *ejajot* or informed consent in the digital humanitarian age a concept presented and emphasised upon refugees by benevolent responders to refugee crises and situations? These are questions that bother us. We are unsure of the answers.

Conclusion

August 2024 will mark the seventh anniversary of a refugee situation in Bangladesh, surpassing UNHCR's definition for protracted displacement. These years are a testament to a heroic tale of – Bangladesh – one of the world's poorest countries collaborating with UNHCR and other UN agencies, as well as a host of national and international NGOs, to shelter and save over a million Rohingya people. An overarching global refugee regime marred by a culture of responsibility shifting as opposed to responsibility sharing, where developing countries end up shouldering far more responsibilities towards refugees, continues to prevail. Under these circumstances, we do not hesitate to admit that the biometric smart card has benefits and gives many Rohingya refugees a sense of identity. That does not mean that we can shy away from acknowledging that the failure to take the *ejajot* of Rohingya refugees during the process that resulted in these IDs is reflective of a top-down biometric registration process that pushed to the absolute side-lines the thoughts and needs of its subjects.

Both the Bangladesh government and UNHCR felt that it was okay to deny the Rohingya people the opportunity to even be minimally involved in shaping how the biometric registration process would roll out, what data would get shared and with whom, the risks inherent in biometric registration, and how those risks could be mitigated. The Bangladesh government and UNHCR saw no wrong in signing an MoU concerning the sharing of the data of Rohingya refugees but, at the same time, kept the contents of that MoU confidential from the people it was meant to allegedly protect. These hard truths do not come as a surprise to us or to the Rohingya people we interviewed. After all, with a minimal 'right to have rights', the legal status of the Rohingya people is precarious.[11] Where discussions on data protection and sharing are only beginning to gain traction in Bangladesh, where a national law on such remains unrealised, it is unsurprising that the *ejajot* of Rohingya refugees was ignored when their biometric data was taken from them.[12]

M Sanjeeb Hossain
Director (Research)
sanjeeb.hossain@bracu.ac.bd
X: @SanjeebHossain @cpj_bracu

Tasnuva Ahmad, Research Associate

Mohammad Azizul Hoque, Faculty

Tin Swe, Rohingya refugee and Volunteer of the Refugee Studies Unit (RSU)

Centre for Peace and Justice (CPJ)
BRAC University

1. bit.ly/un-shared-rohingya-data
2. bit.ly/rohingya-refugee-camps-coxsbazar
3. bit.ly/un-rohingya-bangladesh-assistance
4. bit.ly/data-risks-registering-rohingya
5. bit.ly/2018-jrp-rohingya
6. bit.ly/bangladesh-update
7. bit.ly/verification-rohingya-refugees
8. bit.ly/bangladesh-faces-anger-rohingya
9. bit.ly/locked-in-locked-out
10. bit.ly/refugee-data-collection-bangladesh
11. bit.ly/bangladesh-final-country-report
12. *This research was carried out with support from the Stateless in the Bengali Borderlands: New Technologies and Challenges for Identity and Identification project of the Peace Research Institute of Oslo (PRIO), which received funding from the Research Council of Norway; the ASILE project, which received funding from the EU Horizon 2020 programme for research and innovation under grant agreement n° 870787, and Asylum Access. We are grateful to the six Rohingya refugee volunteers who conducted the KIIs, our anonymous interviewees from the Rohingya and local NGO community, and Tamanna Siddika for translation support during the FGDs.*

Digital technology, detention and alternatives to detention

By **Carolina Gottardo, Celia Finch** and **Hannah Cooper**

The use of technology in immigration detention and alternatives to immigration detention could lead to the erosion of migrants and refugees' human rights, or it could enable greater freedom and dignity. This article explores the complexities of this issue.

Whether we like it or not, when it comes to migration governance, digital technology is here to stay. From customer service portals to collection of biometric data, forecasting models to face recognition tools, use of algorithms for decision making to use of technologies in border management, over the past two decades governments across the world have increasingly used such technologies in the conception and design of their migration systems and as a migration governance tool.[1] The COVID-19 pandemic[2] further accelerated this trend.

Yet, these types of technology are never neutral.[3] There is no such thing as a technical 'fix' to complex and multifaceted challenges, and efforts by some to portray digital technology as the solution to human bias are, at best naïve and at worst dangerous. Employing Artificial Intelligence (AI) and digital technology is a political choice. But the people making decisions over these technologies rarely experience their impacts themselves. People on the move, as well as their families and communities, often in vulnerable situations, are finding themselves at the 'sharp edges'[4] of policies and practices over which they have no control and little to no agency in shaping.

Technology and (alternatives to) immigration detention

The use of technology in immigration detention and alternatives to immigration detention (ATD) has been less explored than the use of technologies in border management situations, but there are many examples of technologies being introduced. For instance, 'Smart Prisons'[5] are now being adopted in the context of immigration detention in different regions of the world.[6] Meanwhile, technologies such as electronic tagging and monitoring, and facial and voice recognition, are being used or explored by a growing number of governments, ostensibly as part of their efforts to move away from the widespread use of immigration detention. While this may seem like progress, these trends raise serious concerns for the International Detention Coalition (IDC) and other organisations advocating for an end to immigration detention.

Information surrounding the use of tech in ATD – and its impacts on people – is largely confined to data from a few key countries (namely Canada,[7] the UK[8] and the USA[9]). However, we know that an increasing number of governments are contemplating employing such tech, if not already actively using it. In the European Union, for instance, Denmark, Hungary, Luxembourg and Portugal have all established the use of electronic tagging in law or administrative regulations. Türkiye,[10] meanwhile, has included electronic monitoring on a list of authorised ATD included within

amendments to the Law on Foreigners and International Protection made in 2019 (but yet to be implemented). At the end of 2023, Australia passed laws that will place strict curfews and ankle monitoring devices on dozens of people seeking asylum who were released from immigration detention following a High Court ruling that indefinite detention was unlawful.

IDC members across the world, working with communities and people affected by detention or at risk of detention, are increasingly expressing concerns about the use of such technologies in the immigration detention space. People at risk of immigration detention are particularly vulnerable to the misuse of digital technology, and they have little ability to assert their rights or to access justice if technology is abused.

In response to these growing concerns and trends, International Detention Coalition (IDC)[11] has launched a new work stream focused specifically on the use of digital technology in immigration detention and ATD. Currently, we aim to examine the multifaceted impact of these technologies on individuals' lives, well-being and futures to ensure our advocacy is driven by the experiences and insights of IDC members, particularly leaders with lived experience of detention and community organisers. Through this work stream, we aspire to identify how the indiscriminate use of technology can potentially harm people on the move, and to explore if and how it can contribute to positive and meaningful engagement. This article outlines the components of this work and the themes that have emerged.

Alternative forms of detention and de facto detention

Research to date has focused on how states have used digital technology to further restrict people's liberties, undermine their human rights and increase surveillance and enforcement.[12] This has been labelled 'techno-carcerality' in the context of the Canadian government's ATD programme, and represents "the shift from traditional modes of confinement to less traditional ones, grounded in mobile, electronic, and digital technology." A report on the Intensive Supervision Appearance Programme (ISAP) in the USA stated that its electronic monitoring components amount to "digital detention."

IDC considers the use of electronic tagging and monitoring as an alternative *form* of detention rather than an alternative *to* detention (ATD). Alternative forms of detention – which are de facto deprivation of liberty, are simply detention by another name – there is potential for the term ATD to be co-opted and used as a smokescreen for such initiatives. Regarding electronic tagging, a recent IDC report states:

"[electronic tagging] substantially curtails (and sometimes completely denies) liberty and freedom of movement, leading to de facto detention. It is often used in the context of criminal law and has been shown to have considerable negative impacts on people's mental and physical health, leading to discrimination and stigmatisation."

More broadly, electronic monitoring devices pose a threat to personal liberty because of heightened surveillance and indiscriminate data collection. They have connotations of criminalisation, both for the individual mandated to wear the device and for the community that sees the device. We know, too, from research and accounts from our members, that voice and facial recognition technologies have questionable accuracy, especially for communities that experience racial discrimination. This can lead to mistakes that have serious and irreversible

consequences – including detention, deportation, and the separation of families and loved ones.

The applications of new technologies are emerging at an alarming rate, with limited analysis available on the ethical, logistical and broader social and individual impacts. Questions around privacy, human rights, dignity, bias, and whether existing legal frameworks apply to decisions taken by AI need to be addressed to manage potential risks. Alongside risks, there may also be opportunities for migrants to use digital technology in a way that benefits them or to use digital technology to advance their rights.

Tech as a way to improve engagement?

IDC has noted anecdotal reports that the use of digital technology in ATD can have some benefits for people on the move. One example is the shift in the UK[13] from in-person reporting to telephone reporting. This approach was originally tested during the COVID 19 pandemic and then adopted on a more permanent basis following sustained advocacy from campaign groups.[14] Those affected have told IDC that this shift has helped ease in-person reporting requirements that were onerous, expensive and disruptive to their livelihoods and schooling. Moreover, places such as police stations and reporting centres often cause people increased anxiety that they will be re-detained. Limited physical contact with such places is likely to have a positive impact on mental health and wellbeing.

Of course, as one of the groups campaigning for this change stated, "Telephone reporting itself could be equally burdensome if implemented without care." It is essential that people are provided with the means to report in this way (for instance, with support to buy a telephone and credit), and that the consequences for missing a call are not harsh. Otherwise, this type of reporting can have negative impacts on people. Moreover, whilst the use of phones is a relatively rudimentary form of technology, it is important that tools such as voice or face recognition are avoided for the reliability reasons mentioned above.

Lived experience of tech-based 'ATD'

IDC's main impetus for launching its new work stream on technology, immigration detention and ATD has come from our members across the world and, in particular, the experiences and insights of leaders with lived experience of displacement and community organisers on the ground. Through this work stream, we hope to explore the impact that this technology is having on people's lives, wellbeing and futures. Since our founding almost 15 years ago, IDC has been advocating for rights-based alternatives to detention. Crucially, we want to ensure that people on the move have the agency and the ability to meaningfully engage with migration governance systems and that their rights and dignity are upheld.

We hope to understand not only how tech can be harmful to people on the move, but also if and how it can help to increase positive, dignified and meaningful engagement. This will help IDC to better assess how to partner with others to push back on certain types of technologies and also where innovations might open up opportunities for people with lived experience of detention, or at risk of detention, in terms of improvements to services, information provision, communication and more effective implementation of community-based ATD. This will include looking at the impact of digital technology through an intersectional lens and in a gender responsive manner, understanding that people's diverse and intersecting identities mean that their

experiences of such technologies vary greatly.

Accountability and due process

The question of accountability – and the distinct but related issue of due process – is one that we are hoping to explore through this programme of work. Where restrictions are imposed, including those linked to digital technology, these should be subject to rigorous review and include the right to appeal.

When technology is used to increase people's freedom of movement and ability to access information, as well as to increase their agency and support their empowerment, it has the potential to uphold key human rights and standards and to increase wellbeing. However, when the primary purpose of digital technology is to expand surveillance and enforcement-based monitoring, it has the opposite effect and leads to the curtailment of rights and freedoms. Unfortunately, given the increasing tendency of many states across the world to adopt migration governance systems based on criminalisation, coercion, control and deterrence, their growing use of technologies without a rights-based risk assessment could exacerbate the already restrictive, harmful and opaque nature of these systems.

Conclusion and next steps

As we navigate the intricate landscape of technology's role in immigration detention and Alternatives to Detention (ATD), the opportunities for positive change and informed decision-making are both evident and pressing. We are exploring the possibility of conducting further collaborative research with partners like the University of New South Wales Kaldor Center. Opportunities like this will allow for further insights and case studies to be examined, ensuring an evidence base of promising best practice policy recommendations. Our ambition is that, by getting to grips with this issue, we can support the growing movement to ensure that the use of technology in the immigration detention and ATD space does not lead to further criminalisation and the erosion of human rights and dignity for communities of migrants, refugees and people seeking asylum.

More research is needed to build a comprehensive understanding of the impact of digital technology in immigration governance. By exploring the experiences and perspectives of individuals across different regions, we can ensure that our insights are nuanced and reflective of the diverse intersections of identity that shape these experiences.

While international and regional legal frameworks and safeguards are imperative, the most meaningful and impactful change often takes place at the national level. Establishing robust national legal frameworks is therefore essential to safeguard the rights of those affected and at risk of detention and ensure accountability in the implementation of technology in immigration detention and ATD.

Looking forward, the potential positive outcomes of digital technology in ATD can be realised through a conscientious and rights-focused approach. By incorporating technology into migration governance systems with a steadfast commitment to justice, fairness, intersectional approaches and the protection of human rights, we can pave the way for more compassionate and effective practices.

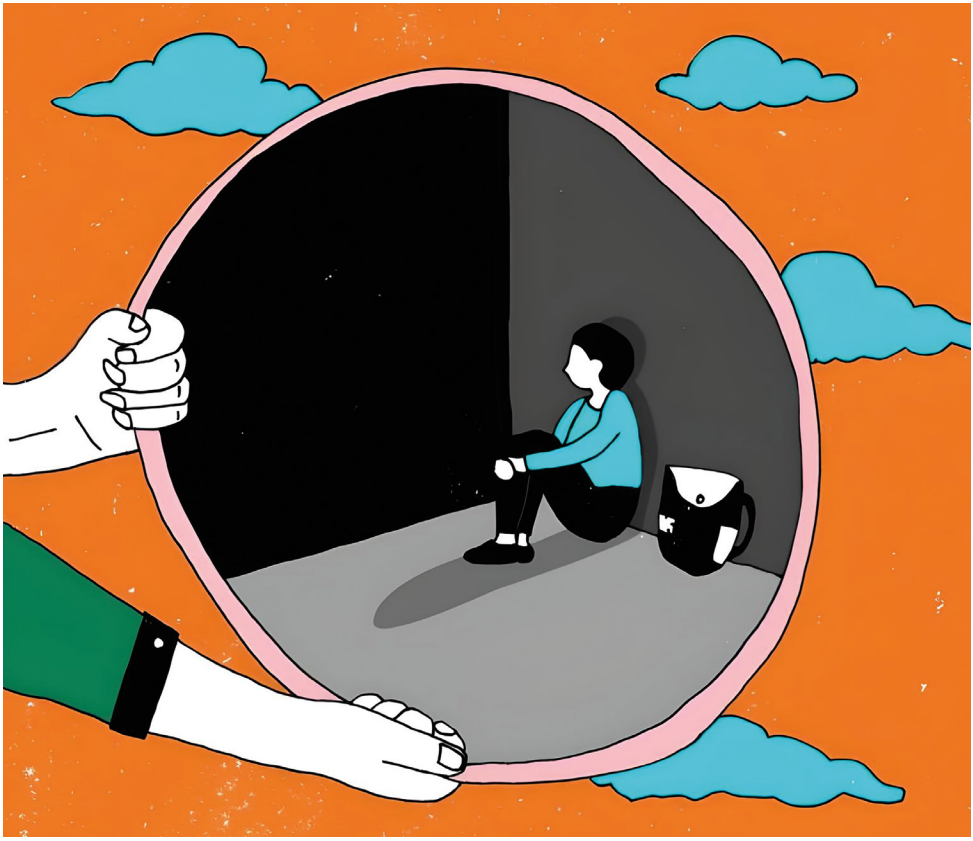
Carolina Gottardo
IDC Executive Director
cgottardo@idcoalition.org
X: @idcmonitor
linkedin.com/company/international-detention-coalition/

Celia Finch
IDC Asia Pacific Regional Manager
cfinch@idcoalition.org

Hannah Cooper
former IDC Europe Regional Manager

IDC would encourage anyone interested in collaborating on this work stream to get in touch with us; we look forward to connecting with others on this crucial issue.

1. *bit.ly/technological-testing-grounds*
2. *bit.ly/digitalisation-ai-migration-manage*
3. *bit.ly/automating-decision-making-migration*
4. *bit.ly/artificial-borders*
5. *bit.ly/digitalisation-prisons-finland*
6. *bit.ly/immigration-detention-east-asia*
7. *bit.ly/confinement-canada-atd-program*
8. *bit.ly/home-office-gps-track-migrants*
9. *bit.ly/ice-digital-prisons*
10. *bit.ly/reduce-end-immigration-detention*
11. *www.idcoalition.org/*
12. *bit.ly/gps-tagging-migrants-uk*
13. *bit.ly/tele-reporting-immigration-bail*
14. *bit.ly/abolish-reporting-campaign-update*



Artwork by Nani Puspasari for the Global Campaign. Credit: International Detention Coalition

Contesting automation: the NewTech Litigation Database

By **Francesca Palmiotto** and **Derya Ozkul**

Informed litigation is vital to uphold the rights of migrants subject to automated decision-making. This article introduces the NewTech Litigation Database, a tool for anyone seeking to contest the use of automated systems in migration and asylum processes.[1]

The use of automated tools in the public domain to identify, categorise and evaluate individuals raises important legal issues concerning fundamental rights. In recent years, legal challenges related to automation in the public sector have emerged under international and national human rights law.

Courts are currently tackling critical questions, such as how to ensure compliance with fundamental rights and what safeguards automated systems require when used in public decision-making. Civil society is also working to understand how these systems work and contest their use. However, there has been little systematic analysis of how these contestations take place, who is involved in their formulation, and on which grounds they are based.

This article provides an overview of the various methods of contestation occurring in this space. It also presents a new tool, the NewTech Litigation Database, which we have developed as part of the Algorithmic Fairness for Asylum Seekers and Refugees[2] (AFAR) project.[3] This tool – launching in May 2024 – facilitates access to existing case law and associated contestation strategies, helping civil society organisations to make searches, learn from others and find inspiration for their work.

Contestation methods

Automated tools are increasingly being used in public decision-making related to migration and asylum, but information about the existence, details and workings of these algorithms is not always available to the public. This lack of transparency makes it difficult for those affected by new technologies to understand how they work and how to contest them. Our research has revealed that individuals impacted by these technologies are seldom able to contest them. Nonetheless, civil society organisations, activists and political party members have employed various methods to understand and challenge these technologies. These methods include demanding transparency through information requests and parliamentary inquiries, filing complaints with data protection authorities and taking legal action in courts.

Demanding transparency through information requests

To obtain information about automated systems, civil society organisations, specifically non-government and non-profit organisations working on digital rights and technology's impact on communities, have used Freedom of Information (FOI) requests to seek information from their respective governments. FoxGlove,[4] a UK-based NGO that aims to promote fair use of technology, supported efforts to obtain information about the Home Office's automated

categorisation and risk assessment tool used for processing short-term visa applications in the UK. Similarly, the Public Law Project (PLP) worked to obtain information on the Home Office's automated categorisation and risk assessment tool to determine sham marriages. In both cases, the Home Office did not disclose all the information, and the basis on which applicants were classified remained unclear. However, at least in the first example, the information helped FoxGlove to file a judicial review, challenging the use of the algorithm under UK equality laws.

In Germany, Gesellschaft für Freiheitsrechte[5] (GFF, The Society for Civil Rights), a non-profit human rights organisation, also made significant efforts to uncover the details of the use of automated mobile phone data extraction by the German asylum authority (BAMF). Prior to these efforts, there was little publicly available information about the details of this practice. To gather information, GFF[6] collaborated with journalist and computer scientist Anna Biselli and carried out extensive research. The information gathered from this research helped GFF take the practice to administrative courts and file a complaint with the Federal Commissioner for Data Protection.

Opposition political parties have used parliamentary inquiries to obtain information about automated tools. For instance, in Germany, members of the Left Party, Die Linke, made multiple attempts to acquire details about the automated mobile phone data extraction and automated dialect recognition tools used in the German asylum procedure. At the EU level, Patrick Breyer, a member of the European Parliament, sought more information about a controversial tool developed in the context of an EU-funded research project called iBorderCtrl. This project aimed to develop an AI-based lie detector to be used on people travelling to the EU borders. However, the Research Executive Agency of the European Commission denied access to documents related to this project on the grounds that the disclosure would undermine the protection of the commercial interests of the consortium of companies involved in developing the technology for the project.

Filing complaints with data protection authorities

Another method used to contest automation is filing complaints with data protection authorities. In the EU, the General Data Protection Regulation (GDPR) allows for complaints to be made to the data protection authorities (DPAs). DPAs are independent authorities with specific powers. Once a complaint is filed, the DPA must investigate the facts, assess the case's merits and issue a legally binding decision. If violations are found, DPAs can impose administrative fines and disciplinary measures to rectify the violation and award the data subject damages for violations. They also hold the power to halt or prohibit certain technologies. For example, in 2019, the European Data Protection Supervisor[7] found that the European Asylum Support Office's (EASO) social media monitoring of asylum seekers and refugees was carried out without a legal basis and temporarily suspended it. They concluded that EASO must have a clear legal basis for the practice in the future and be subject to appropriate safeguards.

Complaint procedures with DPAs are beneficial as they are less formal, less complex, and generally quicker than judicial proceedings. Additionally, a complaint before a DPA is less costly as legal representation is not required. Moreover, DPAs have investigative powers and expertise in data protection law and IT matters. Civil

society organisations have also used this remedial track to stop or limit the use of new technologies. For instance, in Germany, the GFF filed a complaint with the Federal Commissioner for Data Protection in March 2021. The complaint was about the German asylum authority's automated extraction of asylum seekers' mobile phone data, arguing that the phone data analysis disregarded European data protection law. Alongside this complaint, they also successfully took legal action in administrative courts (see the section below).

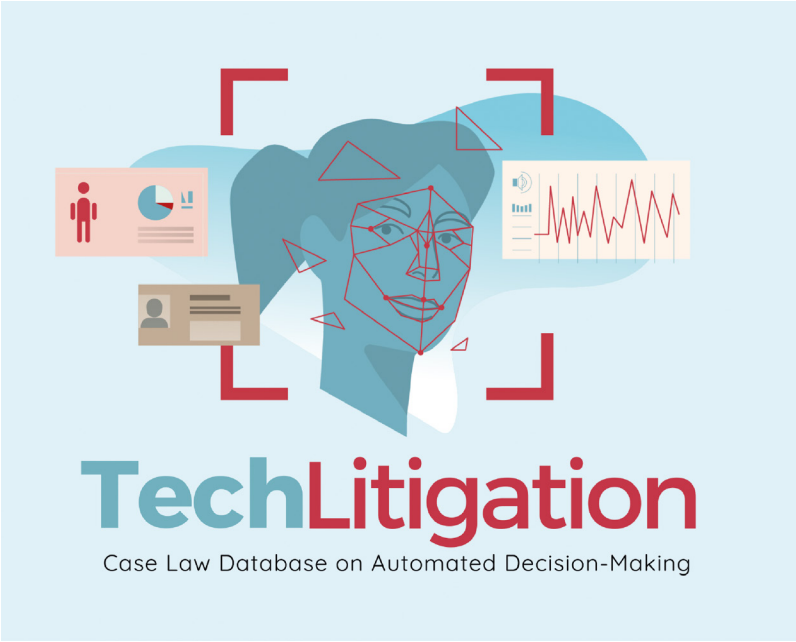
Taking legal action in courts

Civil society organisations and individuals have also challenged the legality of automated tools before courts. In most cases, legal challenges have been brought on human rights grounds, arguing that the use of new technologies was incompatible with the right to privacy, data protection and non-discrimination. Framing cases under human rights law allowed courts to strike down certain governmental uses of automated tools or set specific requirements for their use. One example is the landmark 'System Risk Indication (SyRI)'[8] case in the Netherlands. SyRI was used to profile individuals based on a large amount of personal and sensitive data collected from public bodies to detect potential welfare and tax fraud. Contestants argued that this practice violated the European Convention on Human Rights (ECHR). In February 2020, the European Court of Human Rights ruled that the practice was unlawful as it violated the right to privacy.

In the UK, the High Court of Justice[9] declared the Government's policy of searching, seizing and extracting data from migrants' mobile phones illegal under domestic law and Article 8 of the ECHR. Similar practices involving the acquisition and automated extraction of mobile phones in asylum processes in Germany were challenged in court by the GFF. However, unlike in the UK, this practice was made possible in Germany when amendments to the Asylum Act were introduced to allow mobile phone data analysis to identify asylum applicants without documentation. Nonetheless, in practice, BAMF was operating in violation of the proportionality principle required by the right to privacy. In 2023, the Federal Administrative Court[10] in Germany ruled that the regular evaluation of mobile phone data by the BAMF during the registration of asylum seekers, without considering available information and documents, was unlawful. In this case, the court did not halt the use of the technology but set strict requirements for its use, with important repercussions beyond the individual case.

Another important legal challenge relates to examining the accuracy and biases of automated systems and, in relation to that, the right to non-discrimination. Two refugees in Canada contested the use of a facial recognition system for its lack of accuracy and misclassification with respect to black women and other women of colour. The court allowed the application for judicial review and accordingly returned the matter for redetermination by a differently constituted panel of the asylum authority. GFF also highlighted inaccuracies and errors in automated systems in the German mobile phone data analysis case. According to the government's statistics[11] from 2022, mobile phone data analysis reports provided unusable findings in more than half (67.6%) of the cases, which makes it imperative to reassess the reliability of such technologies in the context of asylum procedures.

Finally, applicants also complained about the lack of transparency, which would impair individuals' procedural rights. In two landmark cases before the Court of Justice



NewTech Litigation Database, the first freely available online resource collating and publishing litigation against the use of new technologies worldwide. Credit: Hertie School & bitteschön

of the European Union, two civil society organisations (Ligue de Droit Humains and La Quadrature du Net) challenged the use of passengers' data in extra-EU flights to prevent and detect terrorism. EU law allowed automated risk assessments to identify travellers that would require further examinations by the authorities. This was, according to the applicants, incompatible with the EU Charter of Fundamental Rights. In the judgments, the court demanded several safeguards for risk assessment technology to ensure compliance with the right to privacy, data protection and effective remedy. In particular, they highlighted the need for reliable technological tools, the obligation of individual review by non-automated means and derived transparency rights for individuals, such as the right to understand how the program works. The court also considered the use of self-learning algorithms incompatible with the right to an effective remedy, as they do not provide sufficient certainty for the human reviewer and individuals.

In summary, by framing contestation on human rights grounds, courts can halt unlawful practices, set specific standards for the use of technology, or derive high transparency standards for automated systems with beneficial effects beyond the individual case.

The AFAR NewTech Litigation Database

As the use of automated tools is still relatively new, methods of contesting them are also emerging and changing slowly. We have developed the NewTech Litigation Database to capture the broad range of contestation methods and their outcomes. It is the first freely available online resource that specialises in litigation against the use of new technologies worldwide. Currently, case law related to contested uses of new technologies is stored in single national databases, often not translated into English.

Our database aims to overcome these access and language barriers through a user-friendly interface, visuals and advanced search tools. The database includes the key details and a summary of all decisions. It includes judgments, decisions, or opinions from national and international courts and Data Protection Authorities with a broad geographical scope (thanks to the work of national rapporteurs worldwide).

At the time of writing (February 2024), the database includes records of fifty litigation cases pertaining to contested uses of new technologies in the public sector. These cases include several public law areas, such as education, administration of justice, law enforcement, migration and asylum governance, admission to public offices and tax enforcement. Of the recorded cases, fifteen specifically deal with migration-related issues, including asylum. The database provides a detailed summary of all decisions in English, categorised according to the sector, country and authority. It also indexes each decision or judgement according to the type of contested technology (e.g. facial recognition), the emerging legal requirements (e.g. transparency), the ownership of the concerned tool (private or public) and the rights impacted. The database is a valuable resource for researchers, practitioners and policy-makers working across all aspects of new technologies and human rights. It also aims to raise awareness and provide transparency about the extent and impact of new technologies, informing and supporting the work of legal actors and civil society organisations.

Conclusion

Our research into the existing contestation methods reveals that civil society organisations and activists have taken most of the actions, while little has been initiated by individuals affected by automated tools, possibly due to a lack of knowledge and resources. Our analysis also found that actors have attempted to challenge automated tools through various means. Due to the lack of transparency, they may need to start their contestation by seeking details about the workings of the concerned tools via information requests. Once they have obtained enough information and evidence, they can take legal action in court. Alternatively, filing complaints with DPAs can provide fast and easy remedies for data protection violations. We strongly encourage anyone interested in challenging the harmful uses of new technologies to stay informed and take action by using the NewTech Litigation Database. This database provides valuable information on existing legal strategies and case law, which can help individuals protect their rights against those in power.

Francesca Palmiotto
Post-Doctoral Researcher, Centre for Fundamental Rights, Hertie School
f.palmiotto@hertie-school.org
X: @FPalmiotto

Derya Ozkul
Assistant Professor, Department of Sociology, University of Warwick
derya.ozkul@warwick.ac.uk
X: @DeryaOzkul

1. *The information presented in this article, including data from the NewTech Litigation Database, has been collected as part of the AFAR Project, funded by the Volkswagen Foundation.*
2. *bit.ly/afar-volkswagen*
3. *If you are interested in the project, follow our countdown to the launch on X: @AFARproject and visit the AFAR project website to access the database.*
4. *bit.ly/home-office-racist-algorithm*
5. *freiheitsrechte.org/en/*
6. *bit.ly/refugee-phone-search*
7. *bit.ly/redacted-easo*
8. *bit.ly/syri-update*
9. *bit.ly/judgment-ewhc*
10. *bit.ly/handing-whole-life-over*
11. *bit.ly/asylum-stats-2022*

Migration forecasting: expectations, limitations and political functions

By **Steffen Angenendt** and **Anne Koch**

Predictive analytics to forecast future migration and displacement are receiving increasing attention, despite their limited practical utility to date. This is because they serve a number of political functions, including strengthening policy coherence and creating an impression of control.

The desire to anticipate and prepare for future developments is ubiquitous in politics. That is especially true for German and European refugee and migration policy. The recent increases in refugee arrivals via the Balkan route and the Mediterranean, and above all from the war in Ukraine, have boosted the wish not to be surprised by future migration movements. The broad interest in predictive approaches – with a strong focus on irregular border crossings and forced displacement – is reflected in a dynamic research landscape and a proliferation of competing approaches.

Quantitative forecasting tools promise better orientation and greater planning security, with instruments based on machine learning and agent-based modelling generating particularly high expectations in terms of precision and reliability. However, to date their practical utility falls short of the hopes placed in them. Considering the apparent gap between what is expected of predictive analytics and what it has to date delivered in the field of migration forecasting, why do efforts to develop related tools still attract political interest and financial resources?

The agencies involved in migration forecasting and tools used

Broadly speaking, there are three fields of application for predictions of forced displacement and irregular migration:

1. boosting national reception capacity when rising numbers of refugees are expected;
2. adapting border security and management to meet predicted challenges; and
3. anticipatory planning of humanitarian aid (and increasingly also development cooperation) in the context of crisis-driven migration.

In all three areas, the efficient use of scarce resources is a central challenge.

A growing number of actors are involved in quantitative modelling for migration forecasting. In Europe, efforts to forecast migration tend to be concerned with refugee reception and border security and focus on those moving towards the European Union and its member States. The central actors are the European Border and Coast Guard Agency (Frontex) and the European Union Agency for Asylum (EUAA), both of which are in the process of developing machine-learning models to forecast new arrivals in EU member states in line with their respective mandates – Frontex focusing on irregular border crossings, EUAA on the number of asylum claims.

For the past few years, the EU Commission has also been investigating the potential for an EU-wide migration forecasting instrument.

Apart from funding various related research consortia, it also commissioned a feasibility study[1] on an AI-based tool to forecast the direction and intensity of irregular migration into and within the EU with a time horizon of one to three months. The results of this study have yet to be translated into practical steps; however, an instrument limited to predicting irregular migration on a single route is to be trialled in a pilot project.

The fact that none of these various tools under development is yet ready for application points to the existence of challenges that resist even the methods of machine learning. The ambition of developing a comprehensive forecasting and early warning system for irregular migration into the EU encounters technical limits in two respects. First, even the most advanced AI-based instruments currently available cannot yet adequately grasp the complex interaction of the numerous factors that influence migration decisions (especially when the respective instrument is required to be universally applicable to all countries and all migration routes to Europe). Secondly, the reliability of any forecast is limited by the inherent uncertainty of migration processes. Many of the most relevant recent migration movements towards Europe were caused by disruptive events that influenced forced displacement and migration in unpredictable ways.

Parallel to these efforts at the European level, various international organisations are developing forecasting tools for improved humanitarian and development planning, the third field of application. UNHCR's Project Jetson,[2] launched in 2017 to forecast displacements in Somalia, is considered the first machine-learning-based application for forecasting internal and cross-border displacement. A second initiative[3] was launched after the Covid-related border closures of 2020 interrupted migration between Venezuela and Brazil. In order to generate viable predictions of the number of Venezuelan arrivals in Brazil after the border was reopened, and the scale of humanitarian needs this would involve, UNHCR collaborated with UN Global Pulse to create a machine-learning-based forecasting instrument and an interactive simulation tool on housing and other needs under different scenarios.

In the NGO sector, the Danish Refugee Council (DRC) and Save the Children are at the forefront of efforts to harness the potential of predictive analytics for improving aid delivery. The DRC's Foresight Model[4] is an AI-based tool designed to predict conflict-related internal and cross-border displacement, currently in twenty-six countries with a time horizon of one to three years. The DRC's Anticipatory Humanitarian Action for Displacement (AHEAD[5]) model forecasts internal displacement in Burkina Faso, Mali, Niger, South Sudan and Somalia, producing regular reports to support the operational work of humanitarian actors. Save the Children developed a machine-learning-based instrument[6] to predict the scope and duration of displacement that has been continuously improved since its introduction in 2018. Central lessons from this process include the realisation that localised, context-specific models are more useful than a generalised global model and that certain missing data can be interpolated using agent-based modelling.

Overall, the practical use of migration forecasting in humanitarian settings seems to be more advanced than efforts to predict irregular arrivals in the EU. One reason may be that the prediction objectives are spatially and temporally more limited because of the concrete operational needs, and the learning curve more tangible

than in the more Eurocentric approaches. Additionally, refugee movements caused by sudden events like natural disasters or outbreaks of armed conflict tend to be easier to model using machine learning than migration movements that are influenced by a much larger number of factors. Nevertheless, developing context-specific prediction instruments is time-consuming, requiring about one year according to the UNHCR Innovation Unit. Tools forecasting displacement may therefore be especially suitable for the longer-term observation of fragile contexts, e.g. in the context of development cooperation.

Even if the practical benefit of quantitative migration predictions varies strongly from one policy field to another, similar obstacles to feeding them into political decision-making processes exist in all areas. Despite the strong need for more forward-looking planning at all levels, national administrations lack the resources and structures required to fully exploit the findings of quantitative prediction instruments. One reason for this is a shortage of personnel and time in the relevant ministries. Another reason is that the inevitable uncertainty of predictions diminishes their value for the political process, which is best suited to dealing with clear and simple facts. And finally, there is a lack of established processes to feed forecasts into political decision-making.

Political functions of migration forecasting

So, what are the uses of quantitative migration predictions in the political process? Apart from hopes of improving inter-departmental cooperation, these include individual ministries gaining a competitive edge through the additional knowledge gained from predictions, legitimation of decisions already made, and the use of forecasts to advance political interests and to acquire funding.

Improving governmental coherence and cooperation

Decision-makers in Germany and at the European level report that the exchange of data on forced displacement and migration between different actors remains relatively unstructured and unsystematic. The patchiness of the information on forced displacement and migration hinders joint decision-making, especially in crisis situations where there is little time for coordination.

AI-based migration forecasting could contribute to a system for preparing a shared situational picture, which clearly assigns responsibilities and is accepted as a basis for decision-making by all relevant actors, and it could mitigate the time pressure that is inherent to crises by enabling discussion and consensus-building early on. The same applies at the European level, where structures for joining up the diverse migration data from different countries are notably lacking. Reliable migration forecasting could expedite coordination between the countries of first arrival, the Commission and EU agencies in the event of a rapid increase in numbers along individual migration routes.

Knowledge as a competitive advantage

Alongside the shared goal of improving predictions, there is also competition for influence over asylum and migration decisions. The fact that additional knowledge can represent a significant competitive advantage can lead to non-cooperation between different actors pursuing migration forecasting. Frontex and EUAA, for instance, both aim to leverage their predictive abilities for their own benefit: While Frontex primarily collects information about trends in irregular migration and the EUAA focuses on building

reception capacity for asylum-seekers, both use their respective forecasts to garner support for institutional expansion. Ultimately, work on developing quantitative migration predictions often serves the organisation's own political goals. This kind of 'silo mentality' also creates obstacles to the development of a quantitative prediction tool by the EU Commission.

Political communication and legitimisation of political choices

In the field of migration and asylum, calls for more evidence-based politics and more investment in data gathering and analysis are ubiquitous. The argument is that presenting decision-makers with evidence-based options would help objectify the frequently emotionally charged and highly polarised debates, and thus help to counteract populist rhetoric. At the same time, figures and statistics fulfil important communicative and legitimising functions in politics. Instead of serving an impartial exploration of different policy options, their primary purpose is often to legitimise or substantiate decisions that have already been taken. Quantitative predictions have yet another function: investments in migration forecasting can create an impression of control in a policy area characterised by uncertainty and periodic shocks and therefore signal efforts to realise forward planning. If forecasting efforts are primarily motivated by these considerations, they are likely to amount to a selective and largely self-serving collection and analysis of data.

Political lobbying and funding acquisition

In the humanitarian sector, quantitative predictions of forced displacement fulfil the important additional function of generating political attention for emerging crises and mobilising the required funding. The Danish Refugee Council and Save the Children explicitly name funding as one of their motives for developing forecasting tools, while at the same time trying to avoid perpetuating the narrative of a growing threat to affluent states through large-scale refugee movements from the so-called Global South. Migration forecasting can also assist state actors in allocating funding and resources. Funding invested before a crisis has broken out is a great deal more efficient than emergency relief after the event. This has long been recognised in humanitarian aid and would warrant greater use of forecast-based financing instruments. Greater efficacy of employed funds is an important argument in the competition for public resources.

Finally, humanitarian aid practitioners also emphasise that reliable predictions of refugee movements could encourage donors to allocate more unrestricted and 'soft earmarked' aid funding, opening up greater manoeuvring space for aid organisations to respond to needs on the ground.

Conclusion

The political functions of quantitative migration prediction outlined here underline the diverse, sometimes contradictory, motives that drive interest in forecasting migration and displacement and thus supplement their practical applications in adapting reception capacities, adjusting border protection and improving the planning and implementation of humanitarian aid and development-oriented projects. While a focus on gaining knowledge steers actors towards coordination and exploitation of synergies, the wish for competitive advantage and the legitimisation of existing policies mitigate towards unilateralism.

A discussion of the potential and pitfalls of novel forecasting tools would be incomplete without engaging with the potential negative effects of these new technical developments on migrants and refugees. While forecasting tools based on machine learning typically

Refugees from Ukraine head to a transport hub after arriving in Moldova. Credit: UNHCR/Andrew McConnell

gather group-based rather than individual data, this still entails considerable human rights risks. In the context of the overheated and polarised debate about forced displacement and migration, quantitative predictions are inherently political and there is a risk they could be used to conjure threat scenarios and to stoke fears. This may lead to the closure of border crossings to asylum seekers, or an increase of racist attacks against particular nationalities or ethnicities. In addition, there is a lack of clarity about the rights of displaced persons and refugees to prevent their data being used in training sets for modelling migration or to receive redress if they suffer unintentional harm through the use of prediction models or if their data is misused for other purposes.

The effects of migration forecasting on forcibly displaced people can be positive (e.g. by improving humanitarian aid planning) or negative (e.g. by redirecting humanitarian funds to border security). This means that even if predictive tools gradually improve, forced displacement and migration will remain areas where difficult political decisions have to be made and defended. Where quantitative migration predictions are used in practice, the risks to those directly affected must be considered and addressed. On the one hand, it must be ensured that predictions are not used as a political tool or used to present migration as primarily a security risk. On the other, data protection must cover group-based data as well as personal data. In the area of humanitarian aid and development cooperation, the principles of the responsible data movement should be developed and adapted to keep pace with the technological progress of the predictive models.

Steffen Angenendt
Partner, Migration Experts Groups
angenendt@migrationexperts.ch

Anne Koch
Associate, Stiftung Wissenschaft und Politik (German Institute for International and Security Affairs)
anne.koch@swp-berlin.org

1. *bit.ly/forecasting-early-warning-ai*
2. *https://jetson.unhcr.org/*
3. *bit.ly/predicting-unpredictable-scenarios*
4. *bit.ly/foresight-displacement-forecasts*
5. *bit.ly/predictive-analysis-ahead*
6. *bit.ly/predictive-displacement*

Keep up-to-date with FMR

To receive FMR updates, including newly-released issues and calls for articles, please sign up to our mailing list: **www.fmreview.org/fmr-alerts.**

Follow us on social media

- @FMReview
- linkedin.com/company/forced-migration-review
- facebook.com/FMReview
- @fmreview.bsky.social

FMR Programmes

FMR prioritises inclusion and impact.

Our **Inclusion Programme** makes FMR accessible to authors and readers around the world. This includes editorial support, mentoring and language accessibility at all stages of the publication cycle.

Our **Impact Programme** ensures FMR reaches decision makers in all areas of forced displacement response, all over the world. This includes multi-format engagement, audience testing, accessibility improvements and impact monitoring.

Artists from 9 countries create a mural in Sofia, Bulgaria together with refugee children. Credit: UNHCR/Dobrin Kashavelov

Get involved

Support FMR

At FMR, we believe forcibly displaced people should have a central voice in displacement response – and that displacement response policies and programmes should reflect evidence from research, practice and lived experience.

FMR relies on the generous support of donors who share our beliefs. Together, we create opportunities for forcibly displaced people and their allies to share learning and engage in dialogue that reaches decision makers in all areas of displacement response.

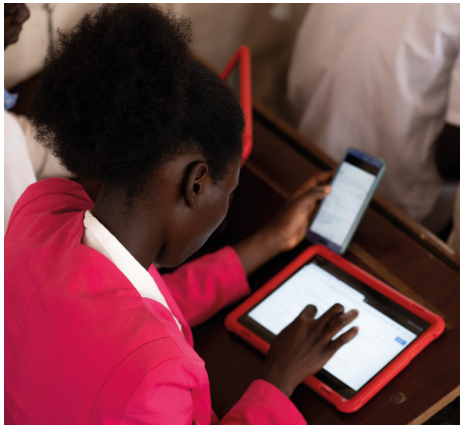
We invite you to consider making a gift at **tinyurl.com/FMRdonate**.
(To arrange institutional contributions, please contact us at **fmr@qeh.ox.ac.uk**.)

Write for FMR

FMR issues a call for article proposals approximately 8 months before each forthcoming issue:
www.fmreview.org/#forthcoming-issues

You do not need any specific qualifications to write. We ask you to draw on your experience – whether of research, practice or lived experience of displacement. If your topic fits the call, please send us a proposal that follows our guidance, detailed here:
www.fmreview.org/write-for-us

We are happy to receive both proposals and full articles in Arabic, English, French and Spanish.



Mozambique. Empowered by digital education: Asylum seeker Izere studies hard to become a doctor. Credit: UNHCR/Lara Bommers

Other ways to get involved

FMR's Inclusion and Impact Programmes are only possible with the help of dedicated volunteers:

- Our mentors offer writing support to new authors with lived experience of forced displacement.
- Our translators ensure FMR's content is accessible and accurate.
- Our advisors, experts in forced displacement and related issues, provide insight and advice on FMR's strategic direction and editorial content.

Join us or learn more at **www.fmreview.org/support-fmr**

Forced Migration Review's free flagship magazine is accessible to a global audience in English, Arabic, French and Spanish, online and in print. Related audio/visual content is available online.

Visit **www.fmreview.org** to sign up for emails, request print copies, browse our archive of content and submit proposals for forthcoming issues.

Solidarity Initiative for Refugees provides ICT training for women in Kakuma refugee camp, Kenya. Credit: UNHCR/Charity Nzomo

www.fmreview.org/digital-disruption

Refugee Studies Centre

UNIVERSITY OF OXFORD