HPG working paper

Digital identity, biometrics and inclusion in humanitarian responses to refugee crises

Kerrie Holloway, Reem Al Masri and Afnan Abu Yahia

October 2021

HPG Humanitarian Policy Group

ODI

How to cite: Holloway, K., Al Masri, R. and Abu Yahia, A. (2021) *Digital identity, biometrics and inclusion in humanitarian responses to refugee crises*. HPG working paper. London: ODI (https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises).

This PDF has been prepared in accordance with good practice on accessibility.

Cover graphic: Fingerprint. Muhammad Ridho/Noun Project

Acknowledgements

The authors would like to thank the refugees and contacts in Jordan and key informants who gave their valuable time to participate in this study, including the many informants who also peer reviewed this publication and gave invaluable comments. Thanks to Barnaby Willitts-King for his guidance during the study and to Sorcha O'Callaghan, Oliver Lough and John Bryant who also provided comments on an early draft. The study could not have been completed without the support of Cat Langdon (Project Manager), Laura Mertsching (Project Manager), Katie Forsythe (Editor) and Hannah Bass (Senior Publications Officer).

About the authors

Kerrie Holloway is a Senior Research Officer at ODI's Humanitarian Policy Group (HPG).

Reem Al Masri is a Senior Researcher at 7iber Magazine in Jordan.

Afnan Abu Yahia is an independent consultant.

Contents

List of boxes and tables

Boxes

Tables

Acronyms

AI	artificial intelligence
AML	anti-money laundering
ATF	anti-terrorist financing
ATM	automated teller machine
CaLP	Cash Learning Partnership
CCF	Common Cash Facility
CO	country office
CVA	cash and voucher assistance
DIGID	Dignified ID
DRC	Democratic Republic of Congo
FSP	financial service provider
GDPR	General Data Protection Regulation
IASC	Inter-Agency Standing Committee
ICRC	International Committee of the Red Cross
ID	identity document
INGO	international non-governmental organisation
IOM	International Organization for Migration
JD	Jordanian Dinar
KYC	know-your-customer
OCHA	Office for the Coordination of Humanitarian Affairs
OIOS	Office of Internal Oversight Services
PIN	personal identification number
SDG	Sustainable Development Goal
UN	United Nations
UNHCR	UN Refugee Agency
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
WFP	World Food Programme

1 Introduction

Digital identity and biometrics have long been divisive topics in the humanitarian sector. On the one hand, they have the potential to be more inclusive and reach people in need at scale due to perceived efficiency gains. A legal identity for everyone as part of the Sustainable Development Goals (SDGs) has spurred the drive to innovation and registration, particularly in the aid and development sectors. On the other hand, serious questions have been raised around their potential for harm, particularly related to data privacy.

As the use of digital identity and biometrics continues to grow, the humanitarian sector must find ways to improve the systems that are in place and mitigate potential risks. These risks go beyond technical failure and relate to broader issues. The addition of technology has often deepened, rather than solved, long-standing structural issues, such as the unequal power dynamics between aid giver and aid receiver, and questions of inclusion and exclusion, such as who gets to decide who is included and how these decisions are made. Due to their immutable nature, the use of biometrics has thrown up several human rights issues around choice, informed consent, privacy and data protection for those who need humanitarian assistance, as well as highlighting wider issues around ethics and data responsibility in the sector.

Biometrics have been used to create digital identities in the humanitarian space since the early 2000s, though little research has been conducted on how end users – in this case, those who register for humanitarian assistance – understand and experience using this technology to receive aid.[1] This report seeks to work towards filling this gap by sharing the perspectives of (mostly Syrian) refugees in Jordan on their experiences with biometrics alongside information and analysis on the larger issues of digital identity (for terminology, see Box 1).

[1] Some notable exceptions include Casswell (2019); Baker and Rahman (2020); Schoemaker et al. (2020) and Iazzolino (2021).

Box 1 Terminology

For the purposes of this paper, **digital identity** refers to 'a set of electronically captured and stored attributes and credentials that can uniquely identify a person' (Casswell, 2019: 64). It can be used as either a **foundational identity** (a legal or personal identity, such as a birth certificate or passport) or a **functional identity** (an identity used to access services, such as a library card or an automated teller machine (ATM) card).[i] An identity document (ID) provides proof of one's identity. Occasionally, the use of biometrics negates the need for a physical ID, when the capture of biometrics links directly to records stored in central databases, rather than on paper (Ucciferri et al., 2017). Often, however, biometrics are used in conjunction with a physical ID.

Biometrics are the biological or physiological characteristics (fingerprints, facial structures, iris or retinal patterns, voice recognition, gait, etc.) measured and assessed for either identification – who are you? – or verification – are you who you say you are? – of an individual through comparison with a database of previously collected samples. Biometrics are sometimes used to facilitate digital identity for service delivery, but this use rises significantly with cash and voucher assistance (CVA), which has become a key component of humanitarian responses, due to the higher level of assurance required by donors when giving cash. Identification by biometrics is typically viewed as more invasive than other means of identification, such as personal details like names and addresses, because of their immutability. By contrast, biometrics have also been promoted as a way to prevent identity theft because it is tied to a unique identifier.

[i] See Gelb and Clark (2013), Kuner and Marelli (2020) and Manby (2021) for more on this distinction.

1.1 Methodology

This study used a qualitative approach based on in-depth interviews with global stakeholders and refugees in Syria. Thirty-three interviews with key stakeholders globally were conducted in English by a researcher in the UK between December 2019 and March 2021. Two interviews with key stakeholders in Jordan were conducted by researchers in Jordan (see Table 1). The location of these interviews will not be used throughout the report to ensure all respondents' anonymity.

Interviews with 45 refugees living outside camps in Jordan took place remotely – due to Covid-19 restrictions – between February and April 2021. These interviews were conducted in Arabic by researchers located in Jordan. All of the interviewees had had their biometric data, including iris scans, collected during the registration process, and all of the interviewees were receiving or had previously received assistance via the iris authentication modality. Some were also receiving or had previously received assistance via a pre-paid ATM card. As of 30 April 2021, 88.3% of refugees under the mandate of the United Nations Refugee Agency (UNHCR) in Jordan were Syrian.[2] Likewise, 40 of 45 interviewees (88.9%) were from Syria. The age and gender of respondents varied, as did place of residence (see Table 2).

Table 1 Stakeholder interviews conducted

Type of organisation	Number
Advocacy organisation	3
International non-governmental organisation (INGO)	8
Red Cross/Red Crescent movement	3
Private sector	6
Research institution	7
UN agency	8
Total	**35**

[2] This figure does not include Palestinian refugees, of which there are more than 2.2 million registered in Jordan, under the mandate of the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) (www.unrwa.org/where-we-work/jordan).

Table 2 Number of refugees interviewed, by geographic region

Governorate	Refugee population	% of total refugee population[i]	Number interviewed
Amman	272,236	36.1	24
Irbid	137,728	18.3	4
Mafraq	87,544	11.6	11
Zarqa	51,419	6.8	5
Other	205,523	27.2	1
Total	**754,450**	**100**	**45**

i See footnote 2.
Source: UNHCR, 2021b

Refugees in Jordan were self-selected by responding to a post on a Facebook group for refugees receiving aid through iris scans, which described the research, the research team and the aims of the research. Within this post, there was a link to a form where they added their information, and the research team in Jordan called them for further verification, such as the date from which they started to receive assistance and the method through which they collect it. Once this had been completed, a time was set for the interviews, which were carried out remotely. Some of the interviewees were found through snowballing, where interviewees from the Facebook group suggested further contacts. To accompany the publication of this report, a link to the Arabic version will be posted in the same Facebook group and sent directly to all interviewees via WhatsApp.

Conducting remote interviews allowed for a broader geographical range, although people's answers remained remarkably consistent across locations. For this reason, age, gender and location are not used throughout the report to ensure respondents' anonymity.

For more on why Jordan was chosen, see Box 2.

Box 2 Why Jordan was chosen for this study

Jordan was selected for this working paper because it has a relatively stable refugee population, which has been using biometrics for registration and to access CVA for several years without any major documented issues. As of 30 April 2021, 85.4% of the refugee population under UNHCR's mandate had been registered using biometrics, with 14.6% awaiting biometric processing (UNHCR, 2021b). Urban refugees were chosen as interviewees because they make up the majority of refugees in Jordan under UNHCR's mandate – 83% as of 30 April 2021 (UNHCR, 2021b). The Jordanian government has shown a willingness to act on progressive policies for refugees, such as access to the labour market through the Jordan Compact, and Jordan is already equipped to use iris scan equipment for refugees and citizens alike at the border and in the banking industry (see section 2.2). Working with other refugee populations who are undergoing biometric registration at a large scale, such as the Rohingya in Bangladesh, would have posed a much bigger possibility for harm (particularly emotional and social), and interviews or questions around the use of biometrics would have been more likely to reignite pre-existing concerns around data protection and identity (see Islam, 2018; Baker and Rahman, 2020). By doing the interviews with a more settled population, the experiences and recommendations can inform other programmes, without sparking rumours or increasing fear in a system that refugees often must agree to use to survive.

1.2 Limitations

The research underpinning this paper took place over the course of 18 months – from December 2019 to May 2021 – due to the challenges of Covid-19. Interviews in Jordan were set to take place, in person in March 2020, but were limited to phone interviews, conducted in early 2021. The population sampled was not representative of the refugee population in Jordan. It was limited by the recruitment method, which saw respondents self-selected by volunteering to participate and through those respondents' contacts. This excluded people who do not have social media from participating in the interviews, though 82% of urban refugees in Jordan have used mobile internet and 73% own a smartphone (Casswell, 2019). There was also an uneven gender split among refugees interviewed, with more women agreeing to be interviewed than men, though responses across the entire sample remained consistent and did not vary based on gender.

This paper largely focuses on the use of biometrics and digital identity in refugee contexts, rather than providing a comprehensive and global assessment, in order to give more detail of a situation where it is used often, rather than to provide a shallower overview. Moreover, the focus on iris scans as the biometric modality in the refugee context in Jordan also limits the study's potential applicability to other biometric modalities, each of which has its own risk and protection profiles. Deployment styles – whether the biometric is stored in a database or not, whether there is a single mode of access or multiple – also vary and impact the amount of risk involved. It is the authors' hope that this deep dive spurs further conversation around different types of biometric modalities and how they are experienced by those who use them on a daily basis.

2 Digital identity and biometrics in the humanitarian sector

Over the past decade, governments around the world have turned to foundational digital identities, often with biometric verification, to register citizens and non-citizens alike. Foundational identities are legal or personal identities, such as civil registries or national ID cards (Gelb and Clark, 2013). In part, the digitisation of foundational IDs is supported by SDG 16.9, which calls for legal identities for everyone in a push to safeguard rights such as access to education, healthcare and financial inclusion, among others. However, this SDG does not stipulate that these identities be digital or include biometrics, and its only indicator is focused on birth registration. Nevertheless, governments and biometric companies have used SDG 16.9 as justification to implement biometric identity systems, due to a perceived reliability of these systems to determine unique identity as well as the increasing availability of this technology (Privacy International, 2018; Manby, 2021). According to one interviewee, however, people in crisis contexts rarely make a distinction between a physical foundational ID, such as a birth certificate, and a biometric ID, such as a national identity card that is tied to a fingerprint; and most are 'willing to give up their fingerprint if they think it will make life easier for them'.[3] With little distinction – and little say in which systems are used (see section 4.1) – it is important that those implementing identity systems mitigate potential risks as much as possible.

Foundational digital IDs with biometrics have been used in numerous cases throughout the world, most notably India's Aadhaar national registration system. In the humanitarian sector, UNHCR is the only organisation mandated to give stateless and displaced people foundational IDs (UNHCR, 2013). The 2018 *Strategy on digital identity and inclusion* notes:

> Integrated national identity systems providing a foundational identity to everybody, including refugees and asylum seekers, stateless persons, and other forcibly displaced, will receive UNHCR's full support. Hence, the UN Refugee Agency will focus on refugee registration as a functional subset of a multi-sector and multi-purpose ID infrastructure and assist States to register and document all individuals living on the State's territory, incl. those under the organization's mandate (UNHCR, 2018: 2).

Digitisation, then, has extended the long-standing process by which states have delegated some powers to UNHCR, leading UNHCR's registration process to become 'something comparable to citizenship' between UNHCR and 'quasi state-citizens' (Hilhorst and Jansen, 2010: 1124; cited in Lemberg-Pedersen and Haioty, 2020: 609). This responsibility means they 'need to have assurances that they know who they are dealing with, and that that person stays the same throughout the service provisioning process. They are therefore more likely to employ advanced biometrics' (Schoemaker et al., 2018: 33).

[3] The same could likely be said of people in high-income countries, although they normally have more choice in what types of system they consent to than those in crises.

The use of biometrics by UNHCR, then, can be for both foundational and functional IDs (i.e. IDs that are used for a specific service provision, are typically proprietary to a single agency/consortium and are not universally issued), leading to confusion among those who register with UNHCR as to why they do not automatically receive aid. According to Schoemaker et al. (2020:8), 'refugees register with UNHCR and other organizations for two primary reasons': first, they register 'to obtain legal status as a refugee', or for a foundational ID; and second, 'to be able to access critical services', or for a functional ID. Functional IDs are less likely to incorporate biometrics unless they are providing CVA (see Box 3).[4]

Several organisations including UNHCR and the International Organization for Migration (IOM), as well as governments around the world, are exploring the use of self-sovereign IDs – digital IDs that are controlled by the end user and decentralised from a specific organisation. The use of self-sovereign ID, however, remains rare, and despite the growing discourse around its disruptive effects on asymmetrical power structures, it is unlikely to circumvent or challenge the role of governments in providing foundational IDs due to state sovereignty (Cheesman, 2020). Self-sovereign IDs can be used for either foundational or functional identities.

Although this study recognises that the field of digital identity is large and there are many examples of digital identity systems that do not include biometrics – such as the digitisation of paper records (Manby, 2021) – the use of these non-biometric programmes is less contested, in part because they are so ubiquitous. By contrast, biometrics goes beyond information typically captured in records – such as name, age, address, etc. – to include a data point that is 'singularly unique to the individual involved and cannot be changed' and that is increasingly used for surveillance and monitoring in a way that names and ages cannot be (Rahman, 2018: 5). For beneficiaries in vulnerable situations, for example because they have been forcibly displaced or are in conflict situations, this type of information presents potential risks that can outweigh the potential benefits (see section 4). Thus, the bulk of this paper focuses on the use and experience of biometrics in digital identity systems, how to mitigate their risks and how to make these systems safer and more efficient for those receiving aid.

[4] Other INGOs providing CVA that do not use biometrics require digital registration due to country restrictions and know-your-customer (KYC) requirements.

Box 3 Why use biometrics for cash and voucher assistance?

Biometrics are often used in cash and voucher assistance (CVA) because of a perceived need[i] for a higher level of assurance of the beneficiary's identity than if the assistance was in-kind. They may be required by the donor, the financial service provider (FSP) or both. The use of cash – particularly when delivered digitally – exposes organisations, FSPs and private sector partners to international regulations such as know-your-customer (KYC), anti-money laundering (AML) and anti-terrorist financing (ATF) regulations. Because most refugees do not have sufficient identification to meet KYC requirements, many humanitarian organisations – including UNHCR – establish a bank account, with recipients holding sub-accounts (Schoemaker et al., 2018).

[i] One key informant disclosed that studies had been done showing how the implementation of biometrics had cut the amount of fraud by 20% of the distributed value, but these studies are not publicly available. The authors were therefore unable to assess or cite them.

2.1 How we got here: the history of biometrics

Digitised biometrics made their entrance in the humanitarian sector in the early 2000s when UNHCR introduced iris scans in the repatriation process of Afghan refugees in Pakistan, mainly to eliminate aid fraud caused by 'recyclers', i.e. people who registered as a refugee, returned home and then came back to register again in order to receive more aid (Jacobsen, 2015). Although biometric registration to reduce aid duplication may have been initially conceived as a one-off event among a highly mobile refugee population, as an INGO worker remarked, 'decisions about technology and systems are made hastily, but then they end up lasting and end up being the channels and infrastructure for a long time'.

Indeed, in the 2003 *Handbook for registration*, UNHCR notes that it is 'likely to use biometrics sparingly because of their technical complexity and their costs, both initial and long-term. The use of biometrics may be recommended in only a few situations and only after a rigorous analysis of the complexities involved in, and the potential alternatives to, using biometrics' (UNHCR, 2003: 141). Less than a decade later, however, biometrics was an official policy in UNHCR refugee registration (UNHCR, 2010). This was largely due to the ability of biometrics to uniquely identify individuals and satisfy the high levels of assurance of verification mentioned previously. By the end of 2019, UNHCR aimed to have all refugee biometric data in a single population database (Madianou, 2019b) – confirming what one academic referred to as 'the use of biometrics more generally has become a goal in itself'.

Since its first use in the early 2000s, the main role of biometrics for UNHCR has come as part of the registration process for people newly arrived in host countries, rather than for service delivery. However, once biometrics are registered, they are often used for CVA and in-kind distributions where feasible and necessary. According to one informant, 'Biometrics are very much a part of our registration and identity management process and that is why we capture biometrics; it helps us to anchor identities. [Distributing cash] is secondary … We don't collect biometrics for assistance or other programming, we capture biometrics as part of our registration procedures'.

Other UN agencies and humanitarian organisations have used biometrics more sporadically. The 'underpinning principle' of the World Food Programme (WFP), for example, 'is to do biometrics [for functional IDs] as a last resort when there's no foundational ID in place, or when it's very weak', according to one informant, and they often rely on other UN agencies, such as UNHCR, to provide verified ID and the associated checks. Yet, the increase in biometric-specific policies from NGOs and the International Committee of the Red Cross (ICRC) may suggest that the use of biometrics outside of the UN system is on the rise. In 2015, Oxfam self-imposed a moratorium on using biometrics (Rahman, 2018). In 2021, however, it published a *Biometric and foundational identity policy*, which committed to responsible biometric practice based on specific principles for data use that minimises harm, since biometrics are 'more tightly bound to individuals in ways which remove individuals' abilities to avert harm to themselves or avoid harmful consequences in the future' (Oxfam, 2021: 8). The ICRC likewise has a policy specific to biometrics, which sets out the limited-use cases and conditions required for processing this type of data due to the specific risks posed by its sensitivity (ICRC, 2019a).

Although fingerprints and iris scans for registration and assistance are the most well-known uses of biometrics in the humanitarian sector, they are not the only ones. Other modes include facial and voice recognition technology, and biometrics have also been used to track health records. The ICRC is developing new capabilities, leveraging artificial intelligence (AI) and facial recognition in its Restoring Family Links Programme (including the 'Trace the Face' website). In this programme, family members looking for their loved ones ask the ICRC for help. Families provide photos of the person they are looking for, and these photos are run through a database of photos of people looking for lost relatives. The facial recognition algorithm is completed with fuzzy searches (that search for a close rather than exact match) on biographical data (ICRC, 2019b).

Voice recognition to confirm identity prior to the disbursement of mobile money payments has also been used by INGOs seeking to increase their accountability and reduce the logistical processes, particularly with hard-to-reach communities. In one example, an INGO uses voice recognition to disburse payments to pastoral communities in Somaliland (Mebur, 2021). According to a key informant, this organisation previously travelled to communities and collected signatures or thumbprints before payments could be released. Now, the SIM card is inserted into a mobile phone, the recipient says a phrase and, if the voice matches, the money is released without teams having to travel to collect signatures. If a voice does not match, that person receives a phone call, and they have another chance to say the phrase correctly. In his opinion, the voice identity project 'has transformed systems, saved time and resources and improved accountability'.

Digital health records have been beneficial, for example in transient populations such as migrants and refugees in Europe who often need medical care along their journey. In this instance, a migrant who registers in one location would be able to take their medical history with them digitally and access the information at another location by providing their fingerprint or iris scan rather than repeating the registration process. According to one medical NGO, this type of system increases patient privacy as doctors are not able to access a record without the patient being present and offering their biometric as consent. Vaccine records are another area in which digital identity has shown real benefits, according to one INGO worker, by speeding up delivery, authenticating data and increasing the quality of data. According to him, the successful use of biometrics for a vaccine programme in which it was important that the same person received a second dose was due to its being rolled out slowly, over 3–5 years, and in consultation with field workers. It remains to be seen whether Covid-19 vaccine records – and the highly debated immunity or vaccination passport (Privacy International, 2020; BBC, 2021; Cooke and Muller, 2021) – will have similar success (see Box 4).

Box 4 Biometrics, digital identity and Covid-19

How the humanitarian sector adapts over the next few years will be dictated in many ways by changes brought on by Covid-19. Tech can be ‘sticky’, and it is likely that new tech introduced during the pandemic will persist for years to come (Bryant et al., 2020). According to the Cash Learning Partnership (CaLP) (2020: 1), for biometrics specifically, the pandemic was found to be ‘driving a rapid shift to remote and digital channels for registration, delivery and monitoring of CVA. These shifts may become the “new normal”, bringing opportunities and requiring careful consideration of risks around safe programming and data management’.

According to one private sector actor, Covid-19 ‘sped up the drive towards contactless technology … particularly palm biometrics because of its high social acceptability and it can be done at a distance’. Similarly, iris scan equipment was adapted for the pandemic by removing the eye hoods and placing scanners further away, making the process contactless. Another INGO worker noted, however, that while they were able to easily shift to remote working since implementing voice recognition technology to authorise cash disbursements, he preferred working in the communities and found remote working ‘challenging because we don’t have a rapport with respondents and don’t have access to the same type of background information’.

2.1.1 The case for (and against) biometrics

Organisations are turning to biometrics now for the same reasons as when they initially implemented them in the early 2000s: to eliminate fraud, reduce duplication, meet the assurance requirements of donors and encourage confidence in States receiving vulnerable refugees for resettlement. Since then, other benefits have been noted: organisations see it as more reliable, and it is often required by FSPs for CVA due to the higher level of assurance required to identify recipients (see Box 3). Indeed, the use of biometrics and CVA have increased in parallel over the past two decades. For those who are registered, organisations argue that using biometrics results in more secure IDs, prevents against identity theft and can streamline processes by eliminating the need for multiple registrations by various organisations (Walkey et al., 2019).

Public evidence of the benefits of biometrics for fraud reduction, however, remains scant (OIOS, 2016; Rahman, 2018; Kaurin, 2019). In a rare published example, fewer than 500 out of more than 500,000 refugees registered with UNHCR in Ethiopia (less than 0.1%) were registered twice (Baker and Rahman, 2020). A key problem in finding this type of data, according to one informant, is that organisations often have no baseline for their level of fraud to determine if it has improved.

Refugees in Uganda welcomed verification, according to one informant in the research sector, because they knew refugees were exaggerating their family size to get more aid. They believed that if fraud were reduced, the amount of aid they received would increase and assistance would spread to more people. In reality, however, verification exercises using biometrics have been used to reduce the overall amount of aid given, not extend it further (WFP and UNHCR, 2015; Tekle, 2020). Similarly, according to Alston (2020), though state digital welfare systems have been presented as altruistic and as an attempt to ensure citizens benefit from technological gains, in reality, they have led to deep budget cuts, fewer beneficiaries, elimination of services, intrusive forms of conditionality and a complete reversal of the idea that the state is accountability to the individual. Indeed, the use of digital systems by states has made rights holders into applicants, where people are required to prove they are deserving of assistance (Alston, 2020). A similar shift can be identified in the digitisation of humanitarian assistance; biometrics can serve to reinforce this change.

Moreover, the majority of fraud – in value, if not in numbers – in humanitarian assistance occurs upstream, at the organisational level of procurement, rather than downstream, at the recipient level of double registration (Rahman, 2018; Schoemaker et al., 2018). As one INGO worker recalled when asked about fraud, 'most admit the fraud that happens by beneficiaries is miniscule compared to the fraud that happens in the rest of the organisation, but we justify biometrics because of the fraud risk', in an attempt to be seen to be taking action. Biometrics have yet to be used to solve the problem of upstream fraud, though Kuner and Marelli (2020) suggest that another type of technology – blockchain – 'may offer a way to introduce transparency into these operations', with transactions throughout the supply chain entered into an immutable record (see also Coppi and Fast, 2019). Blockchain's transparency benefits, however, may not outweigh its potential for surveillance and privacy invasions (Cheesman, 2020).

Other justifications for biometrics centre on their being more efficient than previous methods of data collection. While this may be true for meeting donor requirements because of their high level of assurance and streamlining processes following system set-up, financial efficiency is less certain. Any gains here are often limited by the cost of implementing and running biometric systems (Magnet, 2011; Walkey et al., 2019). In Kenya, for example, biometric registration is reported to have cost $5.14 million (Capgemini Consulting, 2019), whereas UNHCR contracts with IrisGuard between 2014 and 2018 totalled $3.3 million (Lemberg-Pedersen and Haioty, 2020). In these cases, the implementation of biometrics may have been based in part on what one interviewee described as 'something we can do rather than something we should do'.

2.2 Where are we now: biometrics, cash and refugees in Jordan

Jordan has hosted Syrian refugees since the popular uprising and subsequent war broke out in Syria in March 2011, with biometric registration and iris scans to access cash for Syrians in Jordan beginning the following year (Gilert and Austin, 2017). Ten years later, Jordan remains home to more than 750,000 refugees (excluding Palestinian refugees) – almost all of whom are Syrian (88.3%), live outside of camps (83%) and have been biometrically registered using iris-scan technology (85.4%) (UNHCR, 2021b). All refugees from Syria are required to register for a security card with the Ministry of Interior when they enter the country before registering with UNHCR if they need assistance – both registration processes include giving basic personal data and iris scans and result in receiving a biometric security card from the Ministry of Interior and a 'proof of registration' document or asylum seeker/refugee certificate from UNHCR – though some Syrians may have settled in urban areas without registering (Wilson and Casswell, 2018).

The iris-scan technology used in Jordan is provided by IrisGuard, which captures a greyscale image of the iris at registration and converts it to a unique verifiable identity. The iris scanners connect with the EyeCloud®, a server run by UNHCR, which securely stores the iris template as well as other personal data (Baah, 2020). Neither IrisGuard nor the FSP have access to the personal or biometric record.

Although much has been written about the use of iris scans to access cash-based assistance in refugee camps in Jordan (Daniels, 2018; Juskalian, 2018), they are also used on ATMs outside of the camps, in part because iris scanning equipment has been part of Cairo Amman Bank ATMs in Jordan since 2008 (O'Carroll, 2008). Indeed, in many ways, Jordan is unique. Rather than biometrics being pushed by a donor or agency in order to fulfil requirements, a biometric system was adopted because it was already part of the country's infrastructure. Attempts to replicate similar systems in other countries have proved much harder due to a lack of existing machinery. Lebanon, for example, has a similar population with a similar system of cash transfers, but does not use iris scans because the country is not set up for it, and, according to one informant, the government was not interested.

Most CVA in Jordan is distributed by two UN agencies – WFP and UNHCR. In May 2021, WFP supported more than 525,000 individuals through cash transfers (WFP, 2021b) and UNHCR distributed cash to 33,000 families (UNHCR, 2021a). The Common Cash Facility (CCF) – a consortium of UN agencies, NGOs and the Jordanian Government[5] – distributes more than 90% of the cash assistance to refugees outside of camps using UNHCR's iris database and a single FSP – Cairo Amman Bank (Gilert and Austin, 2017; UNHCR, 2017; Baah, 2020).

Of the 45 refugees interviewed for this study, two-thirds (29) preferred to receive cash assistance on an ATM card, 10 preferred iris scans and six declined to state a preference because they felt they had no choice in which one they received. The most common reasons for preferring the ATM card were that another family member could access the assistance for them if they were unable to go to the ATM, the iris scanning equipment often did not work correctly and – at least for the refugees interviewed – the card seemed just as safe as the iris scans since the card's personal identification number (PIN) was known only to the card holder. The 10 interviewees who preferred the iris scans did so because either they did not understand how to use the card or were scared that they would lose their card or their PIN number or that the card would be kept by the machine if they entered an incorrect PIN three times.

While not representative, the fact that a large proportion of the people consulted for this study did not prefer using iris scans to receive their assistance should give pause when compared to the 2016 study by UNHCR, which found that 95.5% of those receiving cash assistance were 'satisfied with the method by which the money is disbursed' (Gilert and Austin, 2017: 14). A majority of the interviewees for this study who stated they did not have trouble collecting money using iris scans still preferred the ATM card. However, many said they were also happy with the iris scan if it meant continuing to receive aid – a comment that highlights the power imbalance between the givers and receivers of aid. There was also a perception among respondents that cash delivered through the iris scan was more guaranteed than that delivered through the card, which may be partly due to the 3–4-month wait to switch modalities reported by refugees.

According to a UN worker, biometrics are particularly useful in cash programming because 'cash needs a stronger level of assurance' that the money is going to the right recipient – a level that is much higher than for something like school feeding programmes. Indeed, many interviewees in Jordan acknowledged this as the purpose of biometrics. As one interviewee explained:

> They say that the purpose of taking the eye's biometrics is to make sure that the people taking the aid are the people who are supposed to receive it, meaning that when someone goes back to Syria, they leave their card here and another family starts taking the aid.

[5] As of June 2019, the CCF included five UN agencies (ILO, IOM, UNOPS, UNHCR and UNICEF); 16 NGOs (Action contre la Faim, Care International, Collateral Repair Project, Danish Refugee Council, Finn Church Aid, GIZ, Intersos, Medair, Mercy Corps, Nippon International Cooperation for Community Development, Première Urgence-Internationale, Save the Children, Terre des Hommes, Vento di Terra, World Relief Deutschland and World Vision); and seven municipal governments in Jordan (Karak, Mafraq, Al-Wasattya, Ramtha, Madaba, Dair Alla and Al-Taybeh) (UNHCR and CaLP, 2020). WFP – one of the main UN agencies providing CVA in Jordan – is not a part of the CCF because they deliver their assistance via vouchers (Gilert and Austin, 2017).

Yet, as one rights advocate explained, the jump to implement biometrics has been premature 'because there could have been other solutions, but these were not explored because biometrics seemed to fix all of these problems'. Indeed, according to another informant, biometrics are increasingly being used in new situations where there is no justification; and, as another researcher noted, questions should be asked prior to any new implementation, such as 'To distribute aid or cash, are biometrics necessary? Could you do it in a less risky way? With less resistance?'

2.3 Where we are going: the future of biometrics

Although biometrics have raised numerous red flags over the past two decades, it is unhelpful 'to take a Luddite view of the technology', as it is not likely to be phased out anytime soon, if ever (Sandvik et al., 2014: 221). Instead, many interviewees agreed that biometrics are likely to become 'ubiquitous' and 'more standardised', 'underpinning all sorts of other applications and interventions' – in humanitarian aid, as well as in the world at large. It is also unhelpful to assume that 'technology is neutral' and that its benefits outweigh the concerns (Gelb and Clark, 2013: 17). Instead, a depolarised approach should be embraced,[6] and those working on humanitarian issues should find ways to improve existing systems of digital identity and biometric technology while mitigating their risks.

Some interviewees felt that the future of biometrics is moving towards more interoperability – with other systems and other technologies. Several noted that governments in the future are unlikely to accept numerous proprietary systems – one for each agency – and will push for things to be consolidated. Others spoke about the combination of biometrics with AI. One private sector actor noted that AI was already gaining interest in the biometric space, particularly in analysing patterns in earlobes, which were mentioned in one interview as the best way to register the biometrics of infants. Another worker in the humanitarian sector, however, cautioned against the use of AI: 'When people try to sell solutions with AI, and there are outliers[7] that don't work well, the thing is, we only work with outliers'.

By contrast, other interviewees felt the goal of future digital identity systems should be to give power back to end users through pushing functional identity towards a self-sovereign ID. One project that is working towards this is Dignified ID, or DIGID – an open-source digital identity platform that works across databases used by UN agencies and INGOs, where the default is a system without biometrics. With DIGID, the end user would give consent for an organisation to access the pieces of information they have requested rather than all information held in the database. Any additional information not already held in the database, including biometric credentials, if necessary, would then be taken by that organisation and accessed only by the organisations that require it.

[6] According to Weitzberg et al. (2021: 2), a depolarised approach is 'equally wary of techno-apologetics and naïve empiricism as it is of reflex technophobic rhetoric'.

[7] 'Outlier' is originally a term used in statistics to describe data points that differ substantially from the average.

Other Red Cross and INGO workers went further, speaking of the desire for anonymised ID, or even to move away from identity completely and provide aid on the basis of unique tokens or hardware not linked to biological data. As this worker put it, ‘In the end, all the obsession about people’s names and things are just a fiction. It’s a utopia that we’re chasing to try to frame an identity of people’. The fact that there is currently a proliferation of digital ID systems being touted is likely to be a challenge in itself, and one that is unlikely to be easily resolved.

3 Digital identity and inclusion

People working on humanitarian issues often speak of foundational digital identities that use biometrics in terms of 'giving people an identity'. This description appeared only recently, roughly 15 years after biometrics were introduced to the sector, to provide them with what Madianou (2019a: 594) calls 'a cloak of legitimacy' . SDG 16.9 perpetuates this notion by tying foundational digital identity to 'a means of enabling inclusive societies in which everyone has portable, sustained access to legal status and rights, including social and medical services, police protection and economic inclusion' (Cheesman, 2020: 4). Several informants for this study noted the need to nuance SDG 16.9 so as to give a legal identity to those who need it while continuing to protect those for whom a foundational digital identity would make them vulnerable. Additionally, not all digital identity systems should be equated with the legal identity aimed at through SDG 16.9. For most refugees, having a digital ID does not enhance their rights, which are still restricted by host country policies, and thus does not match the aspirations of SDG 16.9.

Moreover, this narrative of 'giving people an identity' (rather than an identity *document*) promotes digital identity as a method of inclusion – particularly for those who have been forcibly displaced or who are stateless – without acknowledging existing self-identity. Exclusion from a digital identity programme does not mean that someone does not have an identity any more than inclusion in a digital identity programme means that they do. As Rahman (2018) notes, organisations cannot give an individual an identity, and attempting to do so risks dehumanising them. Others suggest that the reduction of a human being's unique identity to numbers through biometric data is already dehumanising (Capgemini Consulting, 2019).

Based on the interviews in Jordan, refugees do not think of their biometrics as part of their self-identity, but merely a means to receive aid – an identifier both detached from their identity yet simultaneously an integral part of them. Many remarked that the purpose of the iris scan was to confirm they were eligible for aid because iris scans do not change. Yet as will be discussed in section 4, most did not question why their biometrics were being taken because, as they remarked, 'I am in need of every penny, so I didn't ask' and 'When one is running from a war, torture and broken bodies, we didn't care what they will do [with our irises], we wouldn't have asked about anything'. Thus, giving up one's biometrics is not an issue of privacy so much as not having to give biometrics is an issue of privilege – a privilege refugees in Jordan who are struggling to make ends meet do not feel that they have.

Box 5 Biometrics and financial inclusion

Inclusion in a biometric system for cash assistance has yet to translate into wider financial inclusion for end users. In many places, including Jordan, refugees are not allowed bank accounts for saving money and making payments, but rather have sub-accounts under the main UNHCR or WFP account (Baah, 2020). (However, in Jordan, UNHCR is undertaking a pilot project with the Central Bank of Jordan to promote mobile wallets to refugees as part of the financial inclusion plan (Ammourah and Carlisle, 2019).) This type of workaround can help in situations where there are concerns around data privacy because the due diligence is done only on the main account holder, rather than on individual beneficiaries (Raftree, 2021b). However, the set-up does prohibit further financial inclusion, hindering self-reliance and agency of refugees. Similar arrangements have been made for SIM card registration, but as Martin (2019: 29) notes, while 'such formal workarounds may not be ideal from an inclusion perspective, they do provide an effective and, importantly, legal means to facilitate access in certain contexts where other means are not open'.

3.1 Reasons for and implications of exclusion from digital identity systems

Some interviewees claimed that biometric registration systems for foundational identities 'don't exclude anyone'. In their opinion, a system such as UNHCR's registration allows refugees who would have been excluded from the foundational ID registration system of their host state to be included. Even those who do not want their biometrics captured during the process of registration for refugee status can still register for a foundational ID.

Increasingly, however, exclusion from digital identity systems means exclusion from aid, as biometrics are often implicitly required for service provision in protracted displacement settings, particularly for reoccurring cash transfers (see Box 5). Biometrics, like all technology, are not unbiased, and many studies have shown that these biases reproduce existing prejudices and discrimination. As one interviewee explained:

> Any ID requirement is going to be exclusive in some form or another. The reason you have it is to show you're eligible or so people can screen you out as not being eligible. Every time there's something you need to have, or a technology you need to access something, it will be exclusionary … There are inevitably increasing patterns of exclusion because each technology has layers of exclusion built in, and the structure [of exclusion] will depend on the context and population group.

In digital identity systems, as in paper-based registration systems, exclusion can occur before the technology comes into the process. For example, barriers to entry include registration processes that do not match people's situations, such as registration centres that are not conveniently located or inaccessible to those with disabilities; low levels of literacy, including digital literacy; people's cultural and social norms, such as having to remove headscarves for photographs or both genders waiting in the same queue; or for religious reasons (Baker and Rahman, 2020; Tekle, 2020; Khoury, 2021). People who are already marginalised in society, such as those with diverse sexual orientations, gender identities and expressions or persecuted ethnic minorities, can be less willing to participate in registration processes, which they may see as intrusive and high risk. In Kenya, some populations were concerned that biometric data gathered for HIV research 'could be used by the police to target criminalized key populations for arrest' (KELIN and the Kenya Key Populations Consortium, 2018: 10). While some NGOs give people the option to register anonymously, this option is almost never extended to CVA.

Other reasons for exclusions are harder to foresee. According to one private sector worker, in Ethiopia there was a rumour that the red light on the top of the iris scanner was associated with the Illuminati. In his view, 'you can't think of these things beforehand because you won't know [what they will be], so you need to allocate resources for this when biometrics is deployed'. These and similar stories have appeared in other studies. Refugees in Ethiopia and Bangladesh believed the iris scanner tested for eye disease – a claim that some suggested was also promoted by those doing the scanning (Baker and Rahman, 2020). When such missteps and false narratives are perpetuated, people are less willing to engage with the technology, leading to a form of self-exclusion that is harder to rectify than to prevent in the first place.

Failures in technology can also cause exclusion from digital identity systems. For example, fingerprint scans do not work well for those who have spent a lifetime doing manual labour, the elderly or those whose fingerprints are very faint. Iris scans do not work well for those with vision impairments and work better on those with light-coloured eyes, while facial recognition works better on those with lighter coloured skin (Magnet, 2011). One INGO worker using these technologies said that when they fail (e.g., in the case of a deaf person using a voice recognition system or someone who has lost their limbs using fingerprint biometrics), workarounds are typically found by using the biometrics of a family member. In his words, 'When the strategy doesn't work, we find another way'. Similarly, another INGO worker noted that if the iris scan for CVA does not work, the applicant is given an ATM card or a SIM card and a mobile wallet instead.

Not all organisations, however, have been so accommodating. When failures in technology happen, for any reason, end users are typically accused of acting fraudulently before the technology is questioned (Hosein and Nyst, 2013; Jacobsen, 2017; Sepúlveda Carmona, 2019). Lack of trust in people's stories and their own confirmation that they are who they say they are can be demoralising, whereas machines are seen as infallible. An illustrative example of this is when a National Geographic photographer returned to Afghanistan to find the Afghan girl who had appeared on the magazine's cover in 1985; he did not believe her or her family when they confirmed she was the same girl. Instead, he used iris scans – helped by her light-coloured eyes – to prove she was who she, and her family, said she was (Magnet, 2011).

In other cases, exclusion has resulted from previous inclusion. In Kenya, for example, Kenyans who registered themselves as Somali refugees in the early 1990s in order to receive aid during periods of drought now find themselves unable to register for the Kenyan national ID card – a situation that is as political as it is technical. Few redress mechanisms with the Kenyan government speaks to 'longstanding patterns of discrimination against northerners and Somalis' while 'the problem of double registration in Kenya serves as a cautionary tale about the rush towards centralized biometric systems and growing interoperability in the humanitarian sector', where 'incessant proof of legitimate identity' has raised 'the stakes of exclusion' (Weitzberg, 2021: n.p.). Rather than inclusion by default, digital identity and biometrics have shifted the paradigm to exclusion by default.

3.2 Experiences of exclusion from refugees in Jordan

Although all the refugees in Jordan who were interviewed for this study were receiving or had previously received aid through iris scans, they are still subject to exclusionary practices for many of the reasons outlined in the previous section, as well as demographic characteristics such as age and health, inconvenient locations and technological failures. Inclusion, then, is not just being counted as a beneficiary, but rather, 'benefit[ing] from humanitarian action on an equal basis with others' (Searle et al., 2016: 7). As Barbelet and Wake (2020: 12) argue, 'an inclusive humanitarian response … invests in systematically understanding barriers to accessing information on protection and assistance and the barriers to participation for different individuals'. While none of these barriers were insurmountable for the interviewees we spoke with, they must still be overcome. Similar barriers to accessing information on assistance – and in particular on how their biometrics are used and who has access to their data – are discussed in sections 4.1 and 4.2.

Age and health were two factors that were consistently mentioned by interviewees as challenges to receiving assistance through iris scan-enabled ATMs. Older people or those with certain health conditions can struggle to keep their eyes open for the scanning equipment. As one interviewee explained:

> I started having issues in my eyes three months ago. This makes me repeat my eye scans multiple times until it works, and the money is dispensed. Sometimes I stand in line four or five times until it works. One time I had to come back the day after to relieve my eye overnight. I ask someone to come with me to focus my eyes at the camera. For three months now, I couldn't focus on my own, no matter how I tried, and they start watering.

Similarly, another interviewee commented that since the machine struggles to read his eyes, 'sometimes a volunteer will assist me by holding my head at the right position until it works'. Another refugee shared a similar experience from his mother:

> My wife doesn't face any obstacles. But I see that most elderlies, anyone between 50 to 60 years old, needs half an hour to an hour until it recognises their iris. My mother is one of those people. The problem is in the iris not in the machine. When my mother got winter assistance, she had to use an eye drop in order for the machine to recognise it.

Being young, however, does not guarantee that the process is quick. 'Since my wife is young, it [is] usually quick', he continued,

> but it depends on the machine. There are many problems at the ATM machine as some people try to cut in line and stand in front of those who have been waiting two hours in line. It takes my wife around two to three hours to get her turn and obtain assistance.

Those who are older or who have health conditions are also often unable to wait in these long queues, which are worst on the day money is disbursed. Some resort to bringing along chairs because 'they can't stand on their feet for that long', according to one interviewee – negating the common argument that CVA released through ATMs keeps beneficiaries from waiting in queues to receive aid – while others go at night or several days after it has been released to avoid the crowds – an option that may not be available for those who need cash quickly. As one remarked, 'I can't wait for it to be less crowded – impossible – because the owner of the house knocks our door every day asking us for rent'.

For these reasons, many interviewees wondered why ATM cards (which work quicker and can be used at many ATMs) were not the preferred method beyond a certain age. Even those with poor eye health claimed they needed a medical report attesting to their condition before they could be switched from iris scans to the ATM card. Gilert and Austin (2017) note that 7% of UNHCR's caseload of 32,000 families are unable to use the iris scans for reasons such as cataracts or diabetes, and they are provided with an ATM card instead. A more recent report puts the number of recipients not using iris scans at 17%, and these are now split between ATM cards (11%) and mobile wallets (6%) (Samuel Hall, 2021).

Some UN workers see the flexibility for refugees to get aid 'whenever they want' as a positive of the biometric system (quoted in Lemberg-Pedersen and Haioty, 2020: 614). However, refugees interviewed for this study repeatedly noted that they would prefer a flexible system as to who is allowed to collect aid for them. Because biometrics are personal, it is also inherently unshareable. If the person to whom the aid distribution is registered is unable to collect it – if they are sick, need to work or run other errands – the card cannot just be passed to another family member. In the words of one respondent, 'The card is easier to be honest. For example, my husband is ill and can't go. I could go and get it, but with biometrics [I can't]; sometimes he's too tired because he had a heart surgery, so he's always sick'. In some UN programmes, there can be more than one person (i.e. mother and father) registered in the biometric token, allowing any of them to receive the distribution. This, however, is not the case in Jordan, where 'each beneficiary household selects one "cash collector", who is placed on the master cash list as the monthly recipient' (Gilert and Austin, 2017: 10). Although one key informant stated that refugees could change the cash collector (but not add another one), none of the refugees interviewed mentioned this.

Place of residence was also seen to be exclusionary, with some refugees living far from the nearest Cairo Amman Bank ATM. According to Baah (2020), there are 89 iris scanner-enabled Cairo Amman ATMs throughout Jordan; yet for the refugees interviewed for this study, that is not nearly enough. Interviewees mentioned spending up to an hour on a bus or travelling to different governorates to get to a dedicated (and working) ATM. One noted there was only one dedicated ATM in the main commercial street in Irbid, the city with the second largest refugee population in Jordan, while others said there was only one Cairo Amman Bank with iris-scan equipment in Mafraq, the city with the third largest refugee population (see Table 2). According to the post distribution monitoring report, in 2020, 28% of refugees could reach the bank in fewer than 15 minutes, 36% took between 15 and 30 minutes and the remaining 36% needed more than 30 minutes, and 'close to half of the respondents required two or more trips to withdraw the assistance' (Samuel Hall 2021: 27).

Moreover, many queried why assistance was only released through one FSP. When asked what could be done to make the process better, one interviewee remarked, 'I suggest having multiple banks where we can retrieve our assistance, not only Cairo Amman Bank. The problem is that it gets very crowded, and they release our assistance with the military salaries. It becomes crowded for both the military and us'.

Technological failures were commonly cited by all interviewees. For iris scans in particular, many interviewees stated that they had to spend hours and even days travelling from ATM to ATM until they found one that was working or that would accept their iris scan.

> The iris scan depends on the internet. When the internet is weak, the machine doesn't identify you. The machine also has to be in the shade so it can identify you. So we face some issues until your iris clicks with the machine. You also have to arrive at a certain time during the day when the ATM is in the shade so it can correctly click … Sometimes it clicks from the first time; other times I will need to try four or five times. Sometimes I return another day, and others I change the bank … Even the bank employees tell us that we have to come back when the ATM is in the shade.

Another interviewee commented that it can take up to two hours for the machine to read his eyes, and 'even if 20 people are standing in line, and someone with a card comes in, we let him skip the line because it doesn't require much time'. This corresponds with Gilert and Austin (2017: 16), who reported that 'there continue to be technological issues which occasionally prevent beneficiaries from accessing their cash smoothly, including: over-sensitivity of cameras at the ATMs which cannot read all iris scans; interference due to direct sunlight; and maintenance issues'. The most recent post distribution monitoring report noted that 50% of respondents in October 2020 needed an average of 4–7 attempts to scan their iris and withdraw cash (Samuel Hall, 2021).

According to the interviewees, there seems to be a lack of accountability in terms of who should fix the systems when they do not work – either the bank or UNHCR. As one interview remarked:

> We suffer receiving our assistance through biometrics because of ATMs. Either you get errors like your account is insufficient or that your eye scan is not compatible. You try 20 times until it works, so you take the 100 or 150 JDs [Jordanian Dinars].[8] It's not only me; everyone has these issues. When we report it to the bank manager, they tell us that it's UNHCR's problem, not the bank. They say the internet is weak.

Other interviewees commented that they will not complain to UNHCR because 'if we communicate our issues with biometric IDs, they will disconnect it, I know … so no, I will wait two hours instead of losing it'. No refugees interviewed for this study mentioned the role of the technology provider during any part of the interview.

[8] The JD is pegged to the United States Dollar at an exchange rate of 1JD = $1.41.

Yet, according to a member of the CCF in Jordan, many problems are not due to technological issues, but rather because refugees try to access their CVA outside of the allotted times and dates so their account balance is insufficient, and by moving around to find ATMs that work, they quickly deplete the cash from those that do.

4 Three areas of concern for employing biometrics for digital identity

Using biometrics for digital identity in humanitarian programming leads to three areas of concern for end users and those working on humanitarian issues. First, end users should have a free choice in whether or not their biometrics are captured and used. For humanitarians, this choice is institutionalised in the form of 'informed consent'. Second, end users desire privacy for their own protection, which corresponds to how organisations implement data protection and with whom data is shared. Third, end users need biometrics to be employed ethically. Humanitarians must therefore act both ethically and responsibly in terms of how much data is collected and with whom they collaborate. These areas all build on one another and are interconnected. Therefore, those employing biometrics should not only mitigate risks associated with each area, but also address the risks of a biometrically based digital identity system more holistically.

4.1 Choice and informed consent

Having one's biometrics captured and used to prove one's identity should be a choice that is freely given and based on an adequate understanding of what is happening – two elements that, together, are known as 'informed consent'. Kaurin (2019: 10) defines informed consent as 'granting permission with the full knowledge of possible consequences around the using, accessing or sharing of one's data, digital identities and online interactions'. As technologies become more complex, the concept of 'full knowledge' grows increasingly unrealistic – or, according to Schoemaker et al. (2018: 19), 'largely aspirational, seldom meaningful, and frequently problematic'. When digital identities are stored on blockchain, for example, it is unlikely that even the agencies using the technologies understand them fully (Coppi and Fast, 2019), much less those individuals whose data is stored. Instead, informed consent should neither be overly demanding, requiring full disclosure and complete understanding, nor under demanding, requiring only a signed consent form based on scant information (Beauchamp, 2011).

Using biometrics to access aid raises two main issues around informed consent: whether the end user understands the technology and the extent to which their data will be used, protected and shared (see also section 4.2); and whether they have been given a choice between participation and non-participation that does not affect the level of aid they will receive. In literature and in the interviews in Jordan, little time (if any) seems to be spent explaining what biometrics are, why they are collected, how the technology works and how it is used, protected and shared. In an audit of UNHCR's biometric system, the Office of Internal Oversight Services (OIOS) (2016: 10) noted:

> In four out of the five country operations reviewed, OIOS observed that the level of information provided to persons of concern during the biometric registration was below the standards required by the Policy [on the Protection of Personal Data of Persons of Concern to UNHCR] … There was no evidence that the persons of concern were informed of their rights and obligations, for example through the distribution of leaflets or posting of visibility materials in registration sites.

Although UNHCR accepted the recommendations of the audit and committed to mainstreaming data protection into their training programmes (OIOS, 2016), more recent reports show that little has changed. In Bangladesh, the Rohingya interviewed by Baker and Rahman (2020) reported sparse and inconsistent information around the scope and purpose of the digital identity system, with several believing that the iris scan was checking for eye disease. Rather than asking for consent at the individual level, 'community leaders indirectly gave group consent', while some refugees were told 'that registering with the system was a requirement for receiving aid' (Baker and Rahman, 2020: 83). Similarly, in Ethiopia, only one in 25 refugees was informed about how their data would be used and just one in 16 was asked for consent, according to Baker and Rahman (2020).

Indeed, consent for registration (foundational ID) or services (functional ID) is likely to be taken as blanket consent for service provision via biometrics. In Jordan for example, none of the 45 interviewees in this study said they were given information at the time of having their biometrics taken for registration beyond being told it was part of the standard procedure. Most claimed, 'they didn't tell us, and we didn't ask'. One interviewee did question directly why they were taking iris scans and was told 'we don't have information'. When interviewees were asked what they thought the purpose of biometrics was, the majority guessed that it was to ensure the aid reached the intended beneficiary. As one explained it, 'I concluded myself that such procedures are taken to limit cheating and identity theft, like when they take your iris scan at the borders'. Although there are important differences between iris scans taken for registration and those for CVA, most refugees – as with the previous remark – conflated the two purposes due to their using the same modality.

As to the second issue, in theory, informed consent means that the provision of aid is not affected if someone chooses not to register their biometrics for a functional ID. For true informed consent, an alternative way of registering is required so there is a meaningful choice; otherwise, it is informed coercion. In practice, however, biometrics are often a requirement, not an option, with the assumption (correct or incorrect) that those who do not provide their information are excluded from aid. A common sentiment among interviewees in Jordan is expressed in this example: 'I don't resist giving my biometrics. I will give my information if it means assistance … What I care about is that I can get a monthly allowance'. Others said that if they refused, they would be seen as suspicious, so they consented to avoid any trouble.

In the UNHCR *Handbook for registration*, protection officers are instructed on how to handle situations when people refuse to register their fingerprints due to religious or cultural reasons: hold a meeting with men and women in the community, explain why registration is important for UNHCR and its partners and explain the consequences of not registering (UNHCR, 2003; see also Farraj, 2011). The option of an alternative form of registration is not mentioned. Indeed, in Ethiopia, UNHCR stopped aiding refugees who did not register their biometrics, which led to coerced registrations for those who wanted to stay, while others chose to leave the camps and return to South Sudan (Baker and Rahman, 2020; Tekle, 2020). In Jordan, while official UNHCR policy is that refugees can be registered without having their biometrics captured, none of the refugees interviewed for this study were aware of that right.

Increasingly, organisations are turning away from informed consent and towards other legal bases or legal justifications for data processing, such as duty of care and legitimate interest. Duty of care allows organisations to handle data without explicit consent when deemed necessary, as long as it is handled carefully, used reasonably and in the best interest of the individual to whom the data belongs. Legitimate interest allows organisations to process data for activities that are within their mission, as long as this does not compromise the rights and freedoms of the individual to whom the data belongs (Kuner and Marelli, 2020). While these new justifications may go some way towards redressing the problems brought about by informed consent, they also may inadvertently ignore the original motives behind it – that giving people a choice (and perhaps even a false choice) is a sign of respect and upholds their dignity as people with agency. According to one interviewee: 'We try to avoid legitimate interest if we can … as it may be seen as an easy way out of proper accountability and also a weak basis that would be difficult to prove if challenged'. By contrast, Raftree (2021b) argues that legitimate interest may shift the onus of understanding complex risks and how to handle them onto organisations, rather than participants, whereas traditional consent often transfers liability to those least likely to understand such risks.

4.2 Privacy and data protection

Privacy is often a key concern for people affected by crisis who are trying to ensure protection for themselves and their families. Focus groups of refugees in Jordan, Rwanda and Uganda, for example, found that privacy concerns and an unwillingness to allow companies access to personal information were significant barriers to mobile use. In Uganda, refugees were significantly more concerned about sharing data with UN agencies and NGOs than on social media (Casswell, 2019). In Kenya, Somali refugees feared the use of biometrics for tighter control over their movements by police, particularly since the introduction of biometrics in Kakuma coincided with the government's efforts to repatriate them (Iazzolino, 2021).

In several cases, for instance Eritrean refugees in Ethiopia (Tekle, 2020) and Rohingya refugees in Bangladesh (Baker and Rahman, 2020), refugees were concerned that their data would be shared with their country of origin. According to someone working in Bangladesh at this time, the registration process was more anxiety-inducing than necessary 'because it coincided with negotiations with Myanmar, so many communities thought registration meant being prepped for return … and what it would mean if they all signed up for registration. Would they be sending the wrong signal, that they were ready for return?'. Indeed, a recent exposé by Human Rights Watch (2021: n.p.) claimed that UNHCR 'improperly collected and shared personal information … with Myanmar to verify people for possible repatriation', by sharing data without consent. In interviews with 24 Rohingya, they found that sharing data with Myanmar was not mentioned, and all interviewees but one were told they had to register to receive aid. The person who was asked felt he could not refuse because he needed the aid. In his words, 'I did not think that I could say no to the data-sharing question and still get the card'. Three interviewees were told their data might be used for repatriation only after they had already given it, and one noticed that a box on his registration receipt asking (in English) if they were willing to share their data with Myanmar had been ticked 'yes' even though he had never been asked (ibid.).

For Syrians, an academic remarked that questions remained: 'If Assad remains in power, is he going to want to find out who left the country? Who received assistance from Western agencies?' Yet, among Syrian refugees in Iraq, when organisations asked how aid recipients felt about the potential of their data being shared with the government, one interviewee noted they were indifferent, either because the risks were unknown or because they did not see an alternative.

Interviewees in Jordan answered the question 'Who do you think has access to your data?' consistently across interviews. All assumed that UNHCR had access to and stored their data, and most – though not all – believed Cairo Amman Bank and perhaps other implementing partners of UNHCR, such as Care International or Caritas, also had access.[9] Others mentioned that donor countries must have their data since the text message they receive telling them their disbursement is ready mentions the countries providing the funding: 'When I get a message announcing that I am listed to receive assistance through my eye scan, it mentions the donor state like England, Italy or the European Union'. None of the refugees interviewed assumed the technology company itself had access to their data. Many also stated that UNHCR would delete their data when they left Jordan, and none mentioned the possibility of data being shared with the Syrian government.

End users have entrusted organisations and agencies with their private identification information and thus protecting that data should be paramount. According to Capgemini Consulting (2019: 58), 'In case of an incident, such as for example data privacy breaches, with digital ID, individuals will have a lot to lose. They need control over how their identity-related information is used and by whom. Their data needs to be secured and protected at all costs'. Yet, Karl Steinacker, the former Head of UNHCR Global Service Centre, admitted at the World Humanitarian Congress in 2018 that UNHCR built their system by 'introducing the technology first and doing the impact assessment second'.[10]

Weitzberg et al. (2021: 4) note that data protection legislation is vital for identification information, but 'the reality of realising data protection goals in humanitarian contexts is a complex negotiation between governments, emergency management and humanitarian professionals'. Indeed, humanitarian agencies that collect data have been found to be lacking proper data protection, even when guidelines exist, and often operate in countries that lack data protection legislation and/or enforcement tools to protect data. The audit of UNHCR in 2016 found several incidents of poor data protection, including the keeping of a local server in an open cupboard accessible to everyone in the camp in the Democratic Republic of Congo (DRC), unlocked workstations when registration assistants left the room in Thailand and limited knowledge of the Policy on the Protection of Personal Data of Persons of Concern to UNHCR in all five country contexts reviewed (OIOS, 2016).

[9] According to one informant, neither Cairo Amman Bank nor other implementing partners have direct access to data, but rather they send information/data to the UNHCR servers for verification. UNHCR can side-step the KYC requirements because the bank accounts are owned by UNHCR, as sub-accounts of the main UNHCR account, which allows them to retrieve any disbursements that are not collected within the timeframe given.

[10] A video of this panel can be found at www.youtube.com/watch?v=PPVDPGm64MQ.

WFP also notably got caught out during an internal audit and were accused of 'sloppy handling of sensitive data' and failing 'to follow rules it has set for itself' (Parker, 2018). They fared little better in a more recent internal audit: 'In most cases, COs [country offices] did not have operational plans for beneficiary information management, including data privacy and protection, with the majority of Privacy Impact Assessments completed after SCOPE [WFP's beneficiary information and transfers management system] had been implemented, confirming previous audits results' (WFP, 2021a: 12).

While each organisation has their own data protection policies, their organisational interests are likely to influence their priorities for protection. As Clark and Albris (2020: 427) note, 'IOM, for instance, may be more concerned with the monitoring of locational data than the World Health Organization, which sees the protection of information related to personal health indicators as a greater priority'. To help with this, the ICRC has published an industry-wide set of data protection guidelines (Kuner and Marelli, 2017; 2020); the UN Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data (2019) circulated a working draft of its data responsibility guidelines; and the Inter-Agency Standing Committee (IASC) (2021) published its *Operational guidance: data responsibility in humanitarian action*. All of these guidelines could help mitigate the risks posed by collecting and storing data, but only if they are understood and followed. According to one researcher, 'There's been a lot of work around GDPR [General Data Protection Regulation of the European Union], but there needs to be further work to translate that and develop that kind of regulatory regime for the sector'. Nevertheless, these documents remain at the headquarters/institutional level and are often not accessible to frontline staff. There are few documents specifically for practitioners, although Raftree (2021b) and the Centre for Humanitarian Data's guidance[11] are notable exceptions.

Beyond what data is held and who has access to it, another issue with data protection is 'function creep', or how data collected for one purpose can be used for something else. What could start off as a functional collection of data (i.e. for a food distribution programme) can easily transform into a database underpinning a foundational collection of data (i.e. blanket refugee registration) if not guarded carefully (Gelb and Clark, 2013; Rahman, 2018). This often occurs within programmes in the same organisation, or when programmes from one organisation collect more data than necessary, which is later used by other programmes, or other partners, without regaining consent to use the same data for a new purpose. WFP's internal audit, for example, found that 'in a few cases' WFP and its partners gathered more information than necessary, including religious affiliation, 'without a specified or legitimate purpose' (WFP, 2017: 17). WFP has since endeavoured to include data protection in the design of their activities and holds discussions with NGO partners on what personal data is necessary for delivering food assistance. This type of 'information creep' is particularly dangerous where people have fled persecution due to their political views, religious beliefs, ethnicity or sexuality (Cheesman, 2020). The extent to which this type of function creep exists is unclear, and although humanitarian organisations are taking steps to minimise it and understand how it can occur, greater efforts must be made.

[11] Notes on responsible approaches to data sharing, sharing with donors, CVA, data impact assessments, humanitarian data ethics, public–private partnerships, data incident management and statistical disclosure control can be found at https://centre.humdata.org/tag/guidance-note.

In other cases, 'function creep' can extend beyond the organisation that originally collected the data. Behnam and Crabtree (2019: 4) found that 'in some locations, donors' very broad interpretations of confidentiality and consent have diluted accepted standards, for example by arguing that once consent has been given to one organisation, that consent extends to the sharing of data with any other related party'. Like information creep, this type of function creep is particularly dangerous in refugee settings, if (and when) UNHCR is asked to share biometric information by host, origin or donor governments (Jacobsen, 2015). Because they work at the behest of host states, UNHCR's data protection policy reserves the right to share data with the host country and other 'third parties' that comply with the policy (Walkey et al., 2019), following a Data Protection Impact Assessment and Data Sharing Agreement. This has already occurred with Central African Republic refugees in the DRC, refugees in India and Thailand and Rohingya refugees in Bangladesh[12] (OIOS, 2016; Thomas, 2018). In Kenya, the biometric refugee registration system was purposefully designed to crossmatch data between national and humanitarian databases (Sandvik et al., 2017). According to a key informant in Jordan, UNHCR's data is '100% accessible by the Government of Jordan, which squares data with their other data on counter-terrorism. Jordan won't give their data, but they will accept UNHCR's data and see if it matches in their databases'. According to UNHCR, only 'basic biodata', such as a name, is shared, not biometric data.

While similar instances of IDs being used for harm occurred prior to the introduction of biometrics systems – most notably the genocide in Rwanda where mandatory identity cards were used to identify and kill Tutsis on the spot (see Longman, 2002) – technology makes it easier and more efficient to discriminate than previous methods, and for data to be stolen or even sold (Rahman, 2018). With biometric data, its immutability means that once a person is linked with a fingerprint or an iris scan, it is difficult to become decoupled, whereas basic biodata can be changed relatively easily. When it comes to sharing data with governments, the initial assumption should be that governments will change – though the current government may be using the data responsibly, the next government may use it to do harm (Raftree, 2021a).

4.3 Ethics and data responsibility

Data collection for digital identity should be done ethically, particularly regarding what data is collected (and how) and who is responsible for it. UNHCR's biometric database, because of its role as a foundational as well as a functional ID, includes 'ten fingerprints, two iris images and a face photo for most individuals' (Accenture, 2015: 2). However, according to one of the mobile cash providers for UNHCR, the only data that is passed on to them as part of the functional ID for CVA is the person's name, iris code, UNHCR case number and the amount of money to transfer.

For organisations that use biometrics for functional IDs, the primary aim should be data minimisation. As one rights advocate noted, 'once data exists, there's a temptation to see what else it can be used for. The main way to mitigate this is to make sure only the data needed is collected', as well as deleted once

[12] In Bangladesh, the government and UNHCR both register Rohingya, with no option to give data to only one or the other. Between 2018 and 2021, Bangladesh turned over personal and biometric data for 830,000 refugees to Myanmar for repatriation eligibility assessments (Human Rights Watch, 2021).

it has served its purpose. Information that is used to discriminate – whether regarding ethnicity, gender, religion or sexual orientation – should not be collected unless absolutely necessary, as the only way to mitigate risk is to not gather the data in the first place (ELAN, 2016; USAID, 2017; Kuner and Marelli, 2020; Raftree, 2021a). As one Red Cross worker explained: 'You don't need to collect gender or religion to provide food assistance, or marriage status to provide health care. We may have double dipping and some donors don't like that. I think that's the price to pay'.

Accountability to affected people should include good data collection and data protection, but definitions of data responsibility in the humanitarian sector are only recently formulated. The working draft of OCHA's *Data responsibility guidelines* defines data responsibility as 'a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response' (OCHA Centre for Humanitarian Data, 2019: 7). The IASC guidance, which drew on the work of the Centre for Humanitarian Data, defines data responsibility as 'the safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection' (IASC, 2021: 7). CaLP's *Data responsibility toolkit* for cash and voucher practitioners builds on these definitions and looks at data responsibility throughout the data lifecycle, from the initial assessment and design, to collection, storage, analysis, sharing and retention/destruction (Raftree, 2021b).

Collaboration with the private sector – as makers and gatekeepers of technology, FSPs and other third parties – should also be subjected to data responsibility guidelines. According to one INGO worker, 'tech partners are conscious and interested in making responsible choices. They may not do it because they subscribe to humanitarian principles, but because of the reputational risks involved'. Yet, as Raftree (2021b: 23) points out, 'their fundamental motive is profit … In some cases, the private sector will take data privacy and security very seriously in order to maintain customer trust. In other cases, private sector actors might have an interest in monetizing data or reusing customer data to develop commercial products or services'. Although this has yet to result in a serious problem, there are still valid concerns and potential for harm when private sector actors who do not adhere to humanitarian principles are involved in crisis responses. Humanitarians have a responsibility not to outsource the risks of affected populations – to whom they are accountable – to the private sector.

Finally, self-sovereign ID (previously mentioned in section 2) is an attempt to give people more power over their own data and solve some of the problems raised by data responsibility. One advocate for self-sovereign ID noted that it would minimise the hurdle of informed consent, allow the person to know what data was held about them and allow them to share that data when they wanted to. Yet, as another informant warned, 'Self-sovereign identities are interesting, but they're also problematic in the assumption that individuals will start taking responsibility. It delegates responsibility from the organisation to the individual'. Moreover, it does not overcome the hurdle of voluntariness. As Cheesman (2020: 20) points out, 'In some scenarios, data sharing could be coercive rather than voluntary if refugee groups are not in a position to turn down the economic value offered for their personal information'. Like alternative frameworks to informed consent, passing responsibility for how data is handled and shared on to the individual may be one more way of organisations absolving themselves of accountability.

5 Conclusion and recommendations

Biometrics have been used in the humanitarian sector for almost two decades, yet expectations around their efficiency are not met in reality, particularly for end users, in this study's sample in Jordan. Moreover, although the sector has only recently published robust data responsibility policies, organisations continually fail to live up to such policies. While it is likely that the use of biometrics, particularly for CVA, will persist, and even increase, in the future, more work needs to be done. Barriers to access must be removed, alternative options should be made available and data protection and data responsibility need to be taken seriously to ensure those receiving assistance can do so with dignity and that their basic rights are respected. This may prove particularly difficult – but is no less important – considering that biometrics and other forms of technology have brought new stakeholders into the mix. The introduction of technology infrastructure for service provision means that humanitarian agencies may no longer have full control over responses; yet they are ultimately responsible for and accountable to affected people.

This report has highlighted four key disconnects between the current discourse surrounding biometrics and CVA in the humanitarian sector and the lived experiences of refugees in Jordan. First, only 10 of the refugees interviewed prefer receiving aid via iris scans, versus 29 who prefer cash via an ATM card. Most refugee interviewees understand why biometrics have a higher level of assurance and mentioned some of the benefits of iris scans. Yet, their reasons for not wanting to use them were not the same as those given by academics and advocates who are against the use of biometrics in humanitarian action. Rather than describing biometrics in terms of surveillance, data protection or having ownership of their data, interviewees talked about them on a very practical level. Indeed, the challenges wrought by broken machines and weak internet connections, a single FSP and the inability to have another family member pick up aid raise serious questions around whether the benefits to aid organisations are worth the trade-off of a more difficult experience for affected communities. While some humanitarian actors interviewed for this study felt biometrics helped simplify affected people's lives – and indeed OCHA asserts that biometrics should be used to improve lives, rather than add complexity or burden them (Arendt-Cassetta, 2021) – this was not borne out by the interviews with refugees. To this end, organisations employing biometrics over other secure modalities of CVA must weigh up how much risk they are willing to accept in terms of payments being cashed out by someone other than the intended recipient, such as other family members, with the hardships facing refugees due to following stringent procedures.

Second, rather than being a vehicle for inclusion, biometrics and digital identity have resulted in exclusion by default, where users must opt-in to the service, rather than opt-out. The responsibility for receiving aid has shifted: instead of being provided by humanitarian actors, affected people must now prove their eligibility for aid. There is great potential for this type of system to exclude anyone who does not consent to their biometrics being used, while all users are exposed to specific and documented risks through weak data protection. Other barriers to inclusion, which are greater for some, depending, for example, on age, health and geography (as was the case in Jordan), do not allow for equal access by all.

Third, the absence of discussion of the practical concerns among refugees (such as the technological challenges, drawbacks to having only one FSP and one account holder) in the context of larger debates around risks and ethics shows a general lack of awareness of how the process works on the ground. This indicates a challenge of complexity, where higher-level discussions (e.g., about informed consent) may consider some of the power dynamics between the aid giver and the aid receiver but ignore the realities that anyone who needs aid is not in a position to withhold consent. Similarly, the expectation of privacy and data protection is a privilege that is not afforded to those who have few other options. For the refugees, consent and data protection were secondary concerns to needing a system that functions and provides them with assistance.

Finally, much of the language of threats in the humanitarian space – particularly in the data security space – stems from the role of third-party providers, such as technology companies. Yet, technology providers were not mentioned by a single interviewee, even when discussing who is responsible for ensuring the machinery is working correctly. On the one hand, it is likely they were not sufficiently aware of the situation to understand the role these providers play. On the other hand, however, perhaps the humanitarian community places too much emphasis on the role of technology companies and, in doing so, shifts some of the responsibility for service delivery onto them, even though they are not accountable to affected people in the same way. If the humanitarian sector is to continue to use these technologies, they must ensure the technologies work for the people using them.

5.1 Recommendations

So, how can the humanitarian sector address the risks of a biometrically based digital identity system more holistically and inclusively? (For recommendations specific to Jordan, see Box 6.)

1. Ask if biometrics are the right fit for the context and use case. How can you ensure biometrics benefit both the organisation and end user? In many cases, older methods of identification, registration and verification are good enough, and while the addition of biometrics may increase the level of assurance for humanitarian organisations, it may also increase the cost of the programme, leaving less money to go towards assistance, while also increasing data protection risks for affected people in situations where there are no legal tools to ensure their right to privacy.
    a. Complete independent risk assessments for both data security and data protection of biometrics during programmes' design phase to evaluate whether the risk to affected people is greater than the anticipated value of the addition of biometrics.
    b. Rather than assume biometrics will reduce fraud, study the current level of fraud to understand the full extent of how biometrics will (or will not) solve this problem. Where studies have already been done, they should be published so they can be scrutinised. Explore other solutions and evaluate them for similar levels of fraud reduction, balancing these benefits with the data protection risks for affected people.

2. Where biometrics are used, co-design systems alongside affected people. Listen to communities and modify systems to address their concerns. Continue community meetings during the first year of use to address any issues raised while the technology is being implemented and learned, and continually monitor feedback throughout the programme's lifecycle to ensure issues are dealt with as soon as they arise. Emphasis should be placed on creating systems that work for both the humanitarian organisation and the affected population, without adding extra burdens to their lives.
3. Assess any system with an inclusion lens to ensure that there is equal access for all. This may mean altering programmes and modalities based on age and health conditions, and confirming that the chosen FSP does not disadvantage any recipients based on location.
4. Offer a meaningful alternative to service provision via biometrics, rather than biometrics as default, so that biometrics are always optional. Provide information about the options in simplified and transparent language that explains where data is stored, who has access and with whom it is shared. Consent should not be taken at face value if end users believe that assistance will be revoked if they do not consent or if they complain.
5. Practice data minimisation during registration and for service delivery. Do not collect data that is unnecessary for the provision of aid and could potentially pose harm to individuals by someone wishing to target specific population groups, and do not hold data longer than is necessary. Conduct continuous risk audits so that if a situation changes, data protection policies can also change.
6. View data protection as more than just compliance or a tick box. View it through the lens of 'do no harm' and as an opportunity to not expose people to additional and unnecessary risks.
7. Provide transparency reports to end users on data sharing, including any requests received from other entities to access the data and what type of data was provided in response.

Box 6 Jordan-specific procedural recommendations, based on interviews

1. Offer the ATM card as an alternative without a delay in shifting modalities and without asking questions.
2. Allow families to register two members to collect the assistance, rather than only one, as is done in other countries. This would accommodate those who have conflicts or are ill when disbursements are released.
3. Stagger payments according to refugee choices of dates, based on their regular financial commitments such as rent or debt re-payments. Cash distributions are currently staggered, but those receiving aid do not necessarily understand why. Offer refugees a choice of dates so they can decide which one best fits their circumstances.
4. Expand the number of iris scan-enabled ATMs or the number of FSPs so that there are reduced queues during disbursement times and reduced travel times for those who do not live near a Cairo Amman Bank.
5. Decide who is accountable for ensuring technical equipment is working, whether this is IrisGuard, Cairo Amman Bank or UNHCR. Ensure those receiving aid know who to contact when things are not working, and offer anonymous forms of feedback so they do not fear their aid being cut if they make a complaint.

References

Accenture (2015) 'UNHCR: innovative identity management system uses biometrics to better serve refugees'. Dublin: Accenture.

Alston, P. (2020) 'What the "digital welfare state" really means for human rights' *Open Global Rights*, 8 January (www.openglobalrights.org/digital-welfare-state-and-what-it-means-for-human-rights).

Ammourah, M. and Carlisle, L. (2019) 'The digital lives of refugees: what's next?' Amman: UNHCR (www.unhcr.org/jo/12182-the-digital-lives-of-refugees-whats-next.html).

Arendt-Cassetta, L. (2021) *From digital promise to frontline practice: new and emerging technologies in humanitarian action*. New York: OCHA (www.unocha.org/story/ocha-launches-report-new-and-emerging-technologies-humanitarian-action).

Baah, B. (2020) *Humanitarian cash and voucher assistance in Jordan: a gateway to mobile financial services*. London: GSMA (www.gsma.com/mobilefordevelopment/blog/the-versatility-of-mobile-money-insights-from-jordan-and-uganda).

Baker, S. and Rahman, Z. (2020) *Understanding the lived effects of digital ID: a multi-country study*. The Engine Room (www.theengineroom.org/understanding-the-lived-effects-of-digital-id-systems).

Barbelet, V. and Wake, C. (2020) *Inclusion and exclusion in humanitarian action: the state of play*. HPG Working Paper. London: ODI (https://odi.org/en/publications/inclusion-and-exclusion-in-humanitarian-action-the-state-of-play).

BBC (2021) 'Could Covid-19 vaccine passports use biometric data?' BBC, 27 April (www.bbc.co.uk/news/av/technology-56818006).

Beauchamp, T.L. (2011) 'Informed consent: its history, meaning, and present challenges' *Cambridge Quarterly of Healthcare Ethics* 20(4): 515–523 (www.cambridge.org/core/journals/cambridge-quarterly-of-healthcare-ethics/article/abs/informed-consent-its-history-meaning-and-present-challenges/27E8171706F09D53D5702137B3DEA168).

Behnam, N. and Crabtree, K. (2019) 'Big data, little ethics: confidentiality and consent' *Forced Migration Review* 61: 4–6 (www.fmreview.org/ethics/behnam-crabtree).

Bryant, J., Holloway, K., Lough, O. and Willitts-King, B. (2020) 'Bridging humanitarian digital divides during Covid-19'. HPG Briefing Note. London: ODI (www.odi.org/publications/17580-bridging-humanitarian-digital-divides-during-covid-19).

CaLP – Cash Learning Partnership (2020) 'Chapter 9 summary. Covid-19 and CVA: impacts and implications of the crisis and response'. Oxford: CaLP (www.calpnetwork.org/publication/state-of-the-worlds-cash-2020-chapter-9-summary-covid-19-and-cva-impacts-and-implications-of-the-crisis-and-response).

Capgemini Consulting (2019) *Technological innovation for humanitarian aid and assistance*. Brussels: European Parliament (www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634411).

Casswell, J. (2019) *The digital lives of refugees: how displaced populations use mobile phones and what gets in the way*. London: GSMA (www.gsma.com/mobilefordevelopment/blog/the-digital-lives-of-refugees-how-displaced-populations-use-mobile-phones-and-what-gets-in-the-way).

Cheesman, M. (2020) 'Self-sovereignty for refugees? The contested horizons of digital identity' *Geopolitics* 1–26 (www.tandfonline.com/doi/full/10.1080/14650045.2020.1823836).

Clark, N. and Albris, K. (2020) 'In the interest(s) of many: governing data in crises' *Politics and Governance* 8(4): 421–431 (http://dx.doi.org/10.17645/pag.v8i4.3110).

Cooke, T. and Muller, B. (2021) 'Why we need to seriously reconsider Covid-19 vaccination passports'. The Conversation, 19 May (https://theconversation.com/why-we-need-to-seriously-reconsider-covid-19-vaccination-passports-159405).

Coppi, G. and Fast, L. (2019) *Blockchain and distributed ledger technologies in the humanitarian sector*. HPG Report. London: ODI (www.odi.org/publications/11284-blockchain-and-distributed-ledger-technologies-humanitarian-sector).

Daniels, R. (2018) 'How blockchain technology is distributing aid to Jordan' (https://socialprotection.org/discover/blog/how-blockchain-technology-distributing-aid-jordan).

ELAN – The Electronic Cash Transfer Learning Action Network (2016) 'Tip sheet 2: data minimization'. Portland, OR: MercyCorps (http://elan.cashlearning.org/wp-content/uploads/2016/05/Data-minimization-tip-sheet.pdf).

Farraj, A. (2011) 'Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers' *Columbia Human Rights Law Review* 42(3): 891–942 (https://iow.eui.eu/wp-content/uploads/sites/18/2013/04/07-Rijpma-Background4-Refugees-and-Biometrics.pdf).

Gelb, A. and Clark, J. (2013) *Identification for development: the biometrics revolution*. Working Paper 315. Washington, DC: CDG (www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315).

Gilert, H. and Austin, L. (2017) *Review of the common cash facility in Jordan*. Oxford: CaLP (www.unhcr.org/uk/protection/operations/59fc362e7/calpunhcr-review-common-cash-facility-jordan.html).

Hilhorst, D. and Jansen, B.J. (2010) 'Humanitarian space as arena: a perspective on the everyday politics of aid' *Development and Change* 41(6): 1117–1139 (https://doi.org/10.4324/9780203082461).

Hosein, G. and Nyst, C. (2013) *Aiding surveillance: an exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*. London: Privacy International (https://privacyinternational.org/report/841/aiding-surveillance).

Human Rights Watch (2021) 'UN shared Rohingya data without informed consent'. New York: Human Rights Watch (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

IASC – Inter-Agency Standing Committee (2021) *Operational guidance: data responsibility in humanitarian action*. Geneva: IASC (https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action).

Iazzolino, G. (2021) 'Infrastructure of compassionate repression: making sense of biometrics in Kakuma refugee camp' *Information Technology for Development* 27(1): 111–128 (https://doi.org/10.1080/02681102.2020.1816881).

ICRC – International Committee of the Red Cross (2019a) *Policy on the processing of biometric data by the ICRC*. Geneva: ICRC (www.icrc.org/en/document/icrc-biometrics-policy).

ICRC (2019b) ‘Rewards and risks in humanitarian AI: an example’. ICRC Blog, 6 September (https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence).

Islam, M.N. (2018) ‘Bangladesh faces refugee anger over term “Rohingya”, data collection’. Reuters, 26 November (www.reuters.com/article/us-myanmar-rohingya-bangladesh-idUSKCN1NV1EN).

Jacobsen, K.L. (2015) ‘Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees’ *Security Dialogue* 46(2): 144–164 (https://journals.sagepub.com/doi/abs/10.1177/0967010614552545).

Jacobsen, K.L. (2017) ‘On humanitarian refugee biometrics and new forms of intervention’ *Journal of Intervention and Statebuilding* 11(4): 529–551 (www.tandfonline.com/doi/abs/10.1080/17502977.2017.1347856).

Juskalian, R. (2018) ‘Inside the Jordan refugee camp that runs on blockchain’. MIT Technology Review, 12 April (www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain).

Kaurin, D. (2019) *Data protection and digital agency for refugees*. WRC Research Paper 12. Waterloo, Canada: Centre for International Governance Innovation (www.cigionline.org/publications/data-protection-and-digital-agency-refugees).

KELIN and the Kenya Key Populations Consortium (2018) *‘Everyone said no’: biometrics, HIV and human rights: a Kenya case study*. Nairobi: KELIN (www.kelinkenya.org/wp-content/uploads/2018/07/“Everyone-said-no”.pdf).

Khoury, N. (2021) *Digital identity: enabling dignified access to humanitarian services in migration*. Geneva: IFRC (https://preparecenter.org/resource/digital-identity-enabling-dignified-access-to-humanitarian-services-in-migration).

Kuner, C. and Marelli, M. (2017) *Handbook on data protection in humanitarian action*. Geneva: ICRC (www.alnap.org/help-library/handbook-on-data-protection-in-humanitarian-action-0).

Kuner, C. and Marelli, M. (2020) *Handbook on data protection in humanitarian action*, 2nd edn. Geneva: ICRC (www.icrc.org/en/data-protection-humanitarian-action-handbook).

Lemberg-Pedersen, M. and Haioty, E. (2020) ‘Re-assembling the surveillable refugee body in the era of data-craving’ *Citizenship Studies* 24(5): 1–18 (https://doi.org/10.1080/13621025.2020.1784641).

Longman, T. (2002) ‘Identity cards, ethnic self-perception, and genocide in Rwanda’ in J. Caplan and J. Torpey (eds) *Documenting individual identity: the development of state practices in the modern world*. Princeton, NJ: Princeton University Press, pp. 345–357 (www.degruyter.com/document/doi/10.1515/9780691186856-021/html).

Madianou, M. (2019a) ‘The biometric assemblage: surveillance, experimentation, profit, and the measuring of refugee bodies’ *Television & New Media* 20(6): 581–599 (https://journals.sagepub.com/doi/pdf/10.1177/1527476419857682).

Madianou, M. (2019b) ‘Technocolonialism: theorizing digital innovation and data practices in humanitarian response’ *Social Media + Society*: 1–13 (https://journals.sagepub.com/doi/full/10.1177/2056305119863146).

Magnet, S.A. (2011) *When biometrics fail: gender, race, and the technology of identity*. Durham, NC: Duke University Press.

Manby, B. (2021) ‘The Sustainable Development Goals and “legal identity for all”: “first, do no harm”’ *World Development* 139: 105343 (https://doi.org/10.1016/j.worlddev.2020.105343).

Martin, A. (2019) *Displaced and disconnected: connectivity for refugees*. Geneva: UNHCR (www.unhcr.org/innovation/displaced-and-disconnected).

Mebur, J. (2021) 'The Voice ID Project: verifying recipients of mobile money supported humanitarian cash transfers in Somaliland'. London: GSMA (www.gsma.com/mobilefordevelopment/blog/the-voice-id-project-verifying-beneficiaries-of-mobile-money-supported-humanitarian-cash-transfers-in-somaliland).

O'Carroll, J. (2008) 'Banking on iris biometrics in Jordan' *Card Technology Today* 20(4): 6 (www.sciencedirect.com/science/article/abs/pii/S0965259008700896).

OCHA Centre for Humanitarian Data (2019) *Data responsibility guidelines. Working draft*. The Hague: Centre for Humanitarian Data (https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf).

OIOS – Office of Internal Oversight Services (2016) *Audit of Biometric Identity Management System at the Office of the United the Nations High Commissioner for Refugees*. New York: OIOS (https://oios.un.org/file/6506/download?token=h8ejKFap).

Oxfam (2021) *Oxfam biometric and foundational identity policy*. Oxford: Oxfam (https://oxfam.app.box.com/file/819408637805?s=bin2029flc736j9ngskhtqqf90gews05).

Parker, B. (2018) 'Audit exposes UN food agency's poor data-handling'. The New Humanitarian, 18 January (www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling).

Privacy International (2018) 'The Sustainable Development Goals, identity, and privacy: does their implementation risk human rights?' Privacy International, 29 August (https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk).

Privacy International (2019) 'Palantir and the UN's World Food Programme are partnering for a reported $45 million'. Privacy International, 6 February (https://privacyinternational.org/news-analysis/3405/palantir-and-uns-world-food-programme-are-partnering-reported-45-million).

Privacy International (2020) 'Immunity passports and Covid-19: an explainer'. Privacy International, 21 July (https://privacyinternational.org/explainer/4075/immunity-passports-and-covid-19-explainer).

Raftree, L. (2021a) *Case study: responsible data sharing with governments*. Oxford: CaLP (www.calpnetwork.org/publication/case-study-responsible-data-sharing-with-governments).

Raftree, L. (2021b) *Data responsibility toolkit: a guide for cash and voucher practitioners*. Oxford: CaLP (www.calpnetwork.org/publication/data-responsibility-toolkit-a-guide-for-cva-practitioners).

Rahman, Z. (2018) *Biometrics in the humanitarian sector*. Oxford: The Engine Room and Oxfam (www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf).

Samuel Hall (2021) *Multi-purpose cash assistance 2020: post distribution monitoring report*. Amman: UNHCR Jordan (https://data2.unhcr.org/en/documents/details/86576).

Sandvik, K.B., Jumbert, M.G., Karlsrud, J. and Kaufmann, M. (2014) 'Humanitarian technology: a critical research agenda' *International Review of the Red Cross* 96(893): 219–242 (https://international-review.icrc.org/articles/humanitarian-technology-critical-research-agenda).

Sandvik, K.B., Jacobsen, K.L. and McDonald, S.M. (2017) 'Do no harm: a taxonomy of the challenges of humanitarian experimentation' *International Review of the Red Cross* 99(904): 319–344 (https://international-review.icrc.org/articles/do-no-harm-taxonomy-challenges-humanitarian-experimentation).

Schoemaker, E., Currion, P. and Pon, B. (2018) *Identity at the margins: identification systems for refugees*. Farnham, UK: Caribou Digital Publishing (www.gov.uk/research-for-development-outputs/identity-at-the-margins-identification-systems-for-refugees).

Schoemaker, E., Baslan, D., Pon, B., et al. (2020) 'Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda' *Information Technology for Development* 27(1): 13–36 (https://doi.org/10.1080/02681102.2020.1785826).

Searle, L., Flint, J., Munyeki, M., et al. (2016) *Inclusive humanitarian action: a study into Humanitarian Partnership Agreement (HPA) agency practice in the Nepal earthquake response*. Melbourne: Humanitarian Advisory Group (https://humanitarianadvisorygroup.org/wp-content/uploads/2016/06/HAG-CBM_May-2016_email.pdf).

Sepúlveda Carmona, M. (2019) 'Biometric technology and beneficiary rights in social protection programmes' *International Social Security Review* 72(4): 3–28 (https://onlinelibrary.wiley.com/doi/abs/10.1111/issr.12219).

Tekle, T.-A. (2020) 'Refugees in Ethiopia's camps raise privacy and exclusion concerns over UNHCR's new digital registration'. Global Voices Advox, 19 March (https://advox.globalvoices.org/2020/03/19/refugees-in-ethiopias-camps-raise-privacy-and-exclusion-concerns-over-unhcrs-new-digital-registration).

Thomas, R. (2005) 'Biometrics, international migrants and human rights' *European Journal of Migration and Law* 7(4): 377–411 (https://doi.org/10.1163/157181605776293255).

Thomas, E. (2018) 'Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database'. Wired, 12 March (www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh).

Ucciferri, L., Milanes, V., Ferreyra, E. and Segarra, A. (2017) *The identity we can't change: how biometrics undermine our human rights*. Buenos Aires: Asociación por los Derechos Civilies (https://adc.org.ar/en/reports/the-identity-we-cant-change-how-biometrics-undermine-our-human-rights/).

UNHCR – UN Refugee Agency (2003) *UNHCR handbook for registration: procedures and standards for registration, population data management and documentation*. Geneva: UNHCR (www.unhcr.org/afr/3f8e93e9a.pdf).

UNHCR (2010) *Policy on biometrics in refugee registration and verification*. Geneva: UNHCR.

UNHCR (2013) 'Note on the mandate of the High Commissioner for Refugees and his office'. Geneva: UNHCR (www.unhcr.org/uk/526a22cb6.pdf).

UNHCR (2017) 'The Common Cash Facility: partnering for better cash assistance to refugees in Jordan'. Geneva: UNHCR (https://reliefweb.int/report/jordan/common-cash-facility-partnering-better-cash-assistance-refugees-jordan).

UNHCR (2018) *UNHCR strategy on digital identity and inclusion*. Geneva: UNHCR (www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf).

UNHCR (2021a) 'Jordan operational update. May 2021'. Geneva: UNHCR (https://reliefweb.int/report/jordan/jordan-unhcr-operational-update-may-2021).

UNHCR (2021b) 'Registered persons of concern, refugees and asylum seekers in Jordan as of 30 April 2021'. Geneva: UNHCR (https://reliefweb.int/report/jordan/registered-persons-concern-refugees-and-asylum-seekers-jordan-30-april-2021).

UNHCR and CaLP (2020) 'Common Cash Facility factsheet: a partnership for coordinated cash assistance'. Geneva: UNHCR (https://data2.unhcr.org/en/documents/download/75834).

USAID – United States Agency for International Development (2017) *Identity in a digital age: infrastructure for inclusive development*. Washington, DC: USAID (www.usaid.gov/digital-development/digital-id/report).

Walkey, C., Procter, C. and Bardelli, N. (2019) 'Biometric refugee registration: between benefits, risks and ethics'. International Development LSE Blog, 18 July. London: London School of Economics (https://blogs.lse.ac.uk/internationaldevelopment/2019/07/18/biometric-refugee-registration-between-benefits-risks-and-ethics/).

Weitzberg, K. (2021) 'Gateway or barrier? The contested politics of humanitarian biometrics'. Network Blog, Data Rights Africa, 11 January (https://citizenshiprightsafrica.org/gateway-or-barrier-the-contested-politics-of-humanitarian-biometrics-data-rights-africa/).

Weitzberg, K., Cheesman, M., Martin, A. et al. (2021) 'Between surveillance and recognition: rethinking digital identity in aid' *Big Data and Society*, January (www.doi.org/10.1177/20539517211006744).

WFP – World Food Programme (2017) *Internal audit of beneficiary management*. Rome: WFP (https://docs.wfp.org/api/documents/WFP-0000040084/download/?_ga=2.18686585.1326768420.1516256388-1682848339.1511261484).

WFP (2021a) *Internal audit of SCOPE WFP's digital management of beneficiaries*. Rome: WFP (https://docs.wfp.org/api/documents/WFP-0000128891/download).

WFP (2021b) 'Jordan country brief. May 2021'. Rome: WFP (https://reliefweb.int/report/jordan/wfp-jordan-country-brief-may-2021).

WFP and UNHCR (2015) *Joint inspection of the biometrics identification system for food distribution in Kenya*. Rome: WFP (https://documents.wfp.org/stellent/groups/public/documents/reports/wfp277842.pdf).

Wilson, M. and Casswell, J. (2018) *Recognising urban refugees in Jordan: opportunities for mobile-enabled identity solutions*. London: GSMA (www.gsma.com/mobilefordevelopment/resources/recognising-urban-refugees-in-jordan-opportunities-for-mobile-enabled-identity-solutions).

HPG
Humanitarian
Policy Group

ODI

The Humanitarian Policy Group (HPG) is one of the world's leading teams of independent researchers and communications professionals working on humanitarian issues. It is dedicated to improving humanitarian policy and practice through a combination of high-quality analysis, dialogue and debate.

Humanitarian Policy Group
ODI
203 Blackfriars Road
London SE1 8NJ
United Kingdom

Tel: +44 (0) 20 7922 0300
Fax: +44 (0) 20 7922 0399
Email: hpgadmin@odi.org
Website: odi.org/hpg