doi:10.1111/disa.12612

‘I know you like the back of my hand’: biometric practices of humanitarian organisations in international aid

Çağlar Açıkyıldız PhD Candidate, Pompeu Fabra University, and FI Predoctoral Fellow, Institut Barcelona d’Estudis Internacionals, Spain

Humanitarian organisations are increasingly utilising biometric data. However, we know little about the extent and scope of this practice, as its benefits and risks have attracted all the attention so far. This paper explores the biometric practices of the United Nations Refugee Agency, the United Nations World Food Programme, the International Committee of the Red Cross, Médecins Sans Frontières, and World Vision International. The study analysed relevant documents published over the past two decades and 17 semi-structured interviews with humanitarian workers conducted between June 2021 and June 2022. The findings reveal that humanitarian organisations use diverse types and functions of biometric data for different services, collaborate with many actors, and employ various data protection measures. Ultimately, challenging the straightforward generalisations about the use of such data, the paper argues that variational applications of biometrics in the humanitarian context require case-by-case analysis, as each instance will likely produce a different outcome.

Keywords: biometrics, data, humanitarian aid, humanitarian organisations, international aid, technology

Introduction

In 2002, the United Nations High Commissioner for Refugees (also known as the United Nations Refugee Agency; UNHCR) used biometrics to facilitate the return of Afghan refugees from Pakistan (UNHCR, 2003). Since then, we have witnessed a gradual increase in the integration of biometrics into humanitarian operations. Biometrics refers to the ‘technology of measuring, analysing and processing the digital representations of unique biological data and behavioural traits’ (Ajana, 2013, p. 3). Indeed, specific body patterns are proven unique and persistent over time, making biometric technology useful to humanitarian organisations (HOs) in supporting aid operations (Rahman, 2018, p. 5). However, even though UNHCR made biometrics an official policy for refugee registration in 2010, Oxfam self-imposed a moratorium on the use of biometrics in 2015. In May 2021, though, Oxfam changed its stance and approved a biometrics policy (Oxfam, 2021). Starting from the point that there are likely several in-between positions, this paper questions how international HOs use biometric technology in humanitarian response.

This question corresponds to a gap in the literature as normative arguments fail to grasp that there is no one-size-fits-all approach. The prevalent debates on using biometrics in

the humanitarian context centre around benefits and risks. Arguments in favour of biometrics primarily highlight fraud prevention, stating that it helps to track multiple aid claims (Jacobsen, 2017, p. 537). Moreover, it provides a high level of assurance in beneficiary numbers and the allocated resources (Rahman, 2018, p. 7). Biometrics also speeds up registration, shortens the waiting time at aid distribution points, and facilitates the issuing of identity documents (Holloway, Al Masri, and Yahia, 2021, p. 16). However, it is also pointed out that biometrics has been used experimentally in humanitarian sites, and that this can expose vulnerable people to unforeseen harm (Jacobsen, 2015). If the governments from which people fled access biometric data, it can be used to identify or locate them and threaten their safety (Madianou, 2019, p. 591). It may also lead to exclusion and denial of humanitarian access as some individuals have hard-to-capture biometric traits, and matching algorithms perform worse for marginalised populations (Kaurin, 2019; Polk, 2020). Similar concerns have been raised over technical errors, such as system failures to recognise targeted beneficiaries (Farraj, 2011, p. 936; Magnet, 2011, p. 150).

Some arguments, though, rely on straightforward assertions and overgeneralisations. A number proceed as if there is a standard or unified biometric practice, overlooking variational data management. Different types of biometrics have different degrees of intrusiveness (Kuner and Marelli, 2017, p. 131), and the risk level of using some biometric types varies depending on the systems in which they are employed. For example, collecting multiple biometric indicators (such as a fingerprint and iris) allows more ways to access humanitarian aid since one can be an alternative to the other for identity verification (Gelb and Clark, 2013, p. 48). Moreover, entering an unknown person's data into a database is technically riskier than verifying their identity against the already stored template (Rahman, 2018, p. 6). Therefore, variational biometric practices undermine or make less relevant or alter some normative arguments.

Filling this gap has real world importance as well. The use of biometrics by states and commercial actors dates back to the nineteenth century, and this technology is now commonly associated with the pursuit of interests tied to contemporary cultures of security and fear (Magnet, 2011, p. 150). It is deemed special category data (EU, 2016, Article 9) and can reveal personal information such as that concerning genetics, ethnic origin, health conditions, and age (Rahman, 2018, p. 11). For instance, biometric data seized by the Taliban in Afghanistan in 2021 has raised concerns that it will be used to target those deemed to be dissidents (Loy, 2021). The use of data belonging to already vulnerable aid beneficiaries is even more troubling. There are 274 million people worldwide in need of humanitarian assistance and protection (UN OCHA, 2022, p. 9), so analysis of biometric data processing, which is becoming a systematic part of humanitarian operations, is significant. Thus, the major aim of this research is to explore specific practices and policies surrounding the use of biometrics in humanitarian response. The novelty of this paper lies in its determination to offer a fresh perspective and up-to-date investigation of the current state of this technology in the humanitarian context and to include new insights and data that were not aggregated or previously unavailable.

This paper establishes a foothold in the broader literature, particularly on the role of HOs in the digitalisation of humanitarian action. Assisting victims of armed conflict,

famines, and natural hazards in many countries, HOs exercise significant governance power and shape the everyday realities of humanitarian action (Barnett and Weiss, 2008, p. 31). Under the shadow of growing humanitarian needs and funding gaps, HOs are using new and emerging technologies such as artificial intelligence and predictive analytics, crisis mapping, mobile applications, drones, blockchain, and biometrics (UN OCHA, 2021). The main argument of this paper is that there are various applications of biometrics, hence measuring the benefits and challenges of using such data in the humanitarian context requires a case-by-case analysis. In this respect, the paper contributes to the ongoing dialogue about responsible practices and ethical guidelines regarding the utilisation of biometric data by HOs to harness the potential of this technology while minimising the risks to vulnerable populations.

The following section examines the academic literature to identify the ways in which we expect the use of biometrics to vary. The next section explains the methodological tools employed. The paper then analyses how five different HOs use this technology in their operations. After that, similar and divergent practices are assessed alongside the implications for humanitarian action. Finally, the conclusion summarises the discussions and points out the limitations of this paper and avenues for future research.

Humanitarian biometrics

This section outlines the different ways that HOs can use biometrics.

Functions and services

Biometrics can offer two functions: identification (who are you?) and verification (are you who you claim to be?) (Gelb and Clark, 2013, p. 1). The former includes one-to-many authentication, which refers to searching a presented sample and contrasting it with multiple biometric profiles often in a centralised database (Rahman, 2018, p. 6). The latter includes one-to-one authentication, which means checking if the presented sample is identical to the stored template (Rahman, 2018, p. 6). These functions can be used for various services, such as registration, food distribution, healthcare, and repatriation assistance (Gelb and Clark, 2013, pp. 73–81). Therefore, with biometrics, HOs can not only run a deduplication to eliminate redundant data and identify targeted beneficiaries, but they can also verify whether beneficiaries are entitled to claim several types of assistance (Rahman, 2018, p. 6).

Types and systems

HOs can use physiological and behavioural biometrics. The former includes height, face, iris, or fingerprint, which are also called 'hard' biometrics, whereas the latter includes signature, heartbeat, and voice, which are also called 'soft' biometrics (European Commission, Joint Research Centre, 2005, p. 11). HOs may also use one type of biometric indicator or collect multimodal biometrics (European Commission, Joint Research Centre,

2005, p. 56). Furthermore, HOs can store the data in a centralised database or use decentralised mediums such as smart cards (European Commission, Joint Research Centre, 2005, p. 11). Lastly, biometric systems can operate online, integrated into the cloud, or offline (Burt, 2020).

Data collaborations

Investigating who collects and processes biometric data and with whom it is shared may lead to another dimension. In addition to HOs, service providers, government institutions, and partner organisations can collect and process biometric data (Kuner and Marelli, 2017, p. 75). Besides, sharing biometric data with non-governmental organisations (NGOs), donors, governments, or commercial service providers can be tempting for operational continuity (Jacobsen, 2017, p. 538). From a technical point of view, data sharing can be done in two ways: data transfer or granting database access. The former defines the situation where data are made available by transmitting a copy of the entire dataset, whereas the latter refers to granting third-party access to the systems (European Commission, Joint Research Centre, 2005, p. 77).

Data protection measures

HOs can also put several measures in place before, during, and after biometric data collection, such as consent-seeking, a Data Protection Impact Assessment (DPIA), password protection, anonymisation, encryption, pseudonymisation, and determination of the data retention period (EU, 2016). Indeed, depending on the measures taken, data protection levels may vary. Table 1 summarises the ways in which biometric practices are expected to vary.

Table 1. Variations in biometric practices

Dimensions	Uses
Functions and services	Identification (one-to-many authentication) and/or verification (one-to-one authentication). Registration, repatriation, healthcare, and distribution of cash, vouchers, and in-kind aid.
Types and systems	Behavioural/soft biometrics (such as signature, heartbeat, voice) and physiological/hard biometrics (such as face, iris, finger). Unimodal or multimodal. Central database and/or decentralised mediums (such as smart cards). Online and/or offline.
Data collaborations	Partner HOs, governments, donors, private companies.
Data protection measures	Consent-seeking, a DPIA, password protection, anonymisation, encryption, pseudonymisation, and determination of the data retention period.

Source: author.

Methods

This section outlines the methods and procedures used to conduct this study, including the research design, data collection techniques, sampling strategy, and data analysis approach. This paper presents multiple case studies and relies on descriptive inferences. The cases were selected from the largest HOs based on the comprehensive ALNAP (Active Learning Network for Accountability and Performance in Humanitarian Action) report on the shape and size of the humanitarian system (Knox Clarke, 2018). Most funds in the humanitarian system are directed to United Nations (UN) agencies, notably the World Food Programme (WFP) and UNHCR (Knox Clarke, 2018, p. 16). In contrast, Médecins Sans Frontières (MSF) is the largest humanitarian NGO in terms of operational expenditure, followed by World Vision International (WVI) (Knox Clarke, 2018, p. 104). Moreover, the International Red Cross and Red Crescent Movement is the largest humanitarian network in the world. The International Committee of the Red Cross (ICRC) works closely with 192 National Societies and their International Federation (ICRC, 2018, p. 4). Total international humanitarian expenditure in 2020 amounted to USD 30.9 billion (Swithern, 2015, p. 13), and these five organisations account for a large portion of this sum. Table 2 illustrates the total expenditure of these five HOs in United States dollars (ICRC, 2021a; MSF, 2021; UNHCR, 2021a; WFP, 2021; WVI, 2021).

It is critical to note that these numbers do not represent cumulative humanitarian spending as UN agencies outsource large percentages of their funds to NGOs. Nevertheless, these HOs form a crucial part of the international humanitarian architecture due to their capacities to operate in various sectors, set the aid agenda, shape policies, and manage large amounts of funds.

The study data were obtained through document analysis and semi-structured interviews. The first stage was to examine relevant literature and public reports. The latter includes partnership and data sharing agreements, audit reports, policy documents, data protection regulations, annual reports, fact sheets, and news items, all covering the past two decades. The second stage involved semi-structured interviews. Participants were selected from among those who were involved in the use of biometrics in humanitarian programmes. In total, 17 staff members participated between June 2021 and June 2022. This sample size was assessed adequate, as the interviews were used as a supplement to obtain information unavailable in the secondary literature. Furthermore, participants provided sufficiently rich and detailed information as they were highly specialised in their fields. Snowball sampling was employed to recruit the interview participants. This technique allowed me to identify better people of interest in organisations and involve them

Table 2. Total humanitarian expenditure in 2020

	UNHCR	WFP	ICRC	MSF	WVI
Total humanitarian expenditure in 2020 (USD)	9.1 billion	7.4 billion	1.9 billion	1.7 billion	961 million

Source: author, based on ICRC, 2021a; MSF, 2021; UNHCR, 2021a; WFP, 2021; WVI, 2021.

Table 3. Interviewees from each organisation

	UNHCR	WFP	ICRC	MSF	WVI	Other
Number of participants	3	2	4	2	1	5
Number of sessions	3	2	5	2	1	4

Source: author.

in my research, as well as helping me to build trust and develop a rapport with them. I contacted participants via e-mail and social media platforms. The interviews took place over video conferencing platforms as participants attended from different parts of the world, and each session lasted 60 minutes on average. Table 3 displays the number of interviewees from each organisation. The 'other' column refers to former employees of the case study organisations and staff of partner organisations.

Next, recurring patterns were identified from the qualitative data and similarities and differences were explored for analysis. Importantly, data collection methods may have limited this study as HOs may not have disclosed all information, and the interview participants may have hesitated to share some inputs. For example, little or no information is available on the contents of the agreements between HOs, donors, and private companies. Moreover, some contacts, especially from WVI, declined to participate in the study. While it is important to acknowledge these limitations to promote transparency and enable future research to address potential weaknesses, it is worth noting that HOs often proudly relate their biometric data activities to demonstrate that they are keeping up with technological innovation. Also, the responses among different interview participants remained consistent. To avert or minimise the limitations, the confidentiality of the interview participants was respected, and only anonymised information is used throughout the paper.

From innovation to the humanitarian field

This section examines how each of the case study HOs uses biometric data.

United Nations Refugee Agency

As of 2022, UNHCR uses biometrics in 79 country operations (UNHCR, 2022). The Population Registration and Identity Management Ecosystem (PRIMES) works as a single platform to consolidate all UNHCR registration and identity management tools and applications, including the Biometric Identity Management System (BIMS) (UNHCR, 2019, p. 170). BIMS captures photographs, 10 fingerprints, and two irises from each individual, pairs these with other records such as an address, profession, and education, and stores the combined data as a template in a centralised database (UNHCR, 2015a). BIMS is a cloud-based system, but it can also work offline as it also comes as a laptop-sized portable field server (UNHCR, 2015a).

UNHCR uses biometrics primarily to identify refugees, returnees, stateless people, the internally displaced, and asylum-seekers aged five and older. Upon first arrival, a one-to-many search ensures that the person is not registered already. Otherwise, a registration process starts. It takes 10 minutes to capture biometric data from a family of five during registration (UNHCR and WFP, 2020, p. 71). Next comes the issuance of an identity card with a unique identification number. These cards, that is, proof of registration, are generally compatible with the systems used in host states, allowing beneficiaries to access services such as healthcare, a SIM (subscriber identity module) card, a bank account, housing, in-kind/cash assistance, resettlement, and international protection. For service delivery, BIMS is capable of using one-to-one and one-to-few authentications. Research involving refugee interviews has shown that UNHCR often presents biometrics as a prerequisite for refugee status determination and assistance distribution (Kaurin, 2019; Baker and Rahman, 2020; Tekle, 2020).

UNHCR frequently collaborates with governments, partner HOs, and financial service providers in biometric data collection and sharing. In fact, states are sometimes provided with tools and devices as well as staff training to gather biometric data. Referring to UNHCR's work in displacement situations, one interviewee said:

> *Where states do not have their own systems, they make use of ours. [. . .] In Kenya, for example, the government has taken a more active interest to manage the situation over the years. [. . .] So, the biometric registration is now exclusively done by the government and food distributions are almost exclusively [provided] by WFP and WFP's implementing partners. But the systems are UNHCR's, and the data is stored by UNHCR.*

Moreover, the Common Cash Facility brings seven UN agencies, 25 international NGOs, eight government departments, and the Cairo Amman Bank together in Jordan. The main aim of this collaboration is to provide cash assistance using UNHCR's biometric registration system in the country. Beneficiaries can withdraw cash by scanning their irises in the devices installed at ATMs (automated teller machines). In response to a question about the data flow in this process, one interviewee confirmed that the bank has no access to biometric data. It receives a simple 'yes' or 'no' response from the system to verify that the presented sample belongs to the registered person, thereby allowing ATM withdrawals. Interviews revealed that IrisGuard scanners are used in Egypt, Lebanon, Iraq, Jordan, and Syria. In other operations, UNHCR works with multiple technology providers, including Accenture, FotoNation, GenKey, Green Bit, IriTech, Microsoft, and Warwick Warp.

UNHCR also has a data sharing agreement with the US Citizenship and Immigration Services, covering the transfer of the biometrics of refugees seeking resettlement in the country (United States Department of Homeland Security, 2019). Moreover, biometric identity cards were distributed to Afghan refugees in Pakistan in a government-led and UNHCR-backed operation in 2021 (UNHCR, 2021b). Interviewees mentioned that biometric data collaborations are formed with host and resettlement rather than origin states.

One interviewee explained that data sharing is not the first choice and alternative methods are often sought, and that the usual practice is to allow partners to access BIMS rather than transferring data. However, it was reported that UNHCR had shared the personal information of Rohingya refugees, including biometric data, with Bangladesh, which shared it with Myanmar, the same government that originally subjected this population to violence (Human Rights Watch, 2021). In this regard, some refugees previously considered data sharing to be beneficial for a smoother repatriation, whereas others expressed fear of being targeted again (Baker and Rahman, 2020; Prasse-Freeman, 2022).

Given the diversity of use cases, UNHCR puts data protection measures in place. Growing recognition of the value of biometrics has led UNHCR to change some approaches over the years. For instance, the agency used to anonymise all of the data, but later preferred to link the encrypted biometric data to the identity of the person. It issued the Policy on Biometrics in Refugee Registration and Verification in 2010, yet it is only available for internal use. Nevertheless, the 2015 Policy on the Protection of Personal Data of Persons of Concern introduces organisational and technical measures to ensure the confidential and secure processing of sensitive data. These measures include proportional data collection, setting passwords, encryption, consent-seeking, establishing standard operating procedures, organising staff training, a DPIA, and ensuring the physical security of premises and equipment (UNHCR, 2015b, p. 26). In fact, a Data Protection Officer (DPO) at UNHCR's headquarters in Geneva, Switzerland, supervises the compliance of data activities with the Policy. However, one issue with which UNHCR struggles is to determine precise data retention periods. One interviewee explained: 'We often see people returning to us due to displacements resulting from ongoing conflicts. So, sometimes there is an advantage to keeping records open for longer periods'. Lastly, UNHCR claims to give its beneficiaries the right to receive information about how their data are used and to request the correction or deletion of incorrect or excessive personal data (UNHCR, 2015b, p. 20). However, elsewhere, interviews with UNHCR beneficiaries have shown that they lack knowledge of why their information is collected and how it is used (Kaurin, 2019; Schoemaker et al., 2021; Holloway, Al Masri, and Yahia, 2021).

World Food Programme

WFP's digital beneficiary and transfer management system, SCOPE, is compatible with fingerprints, photographs, and iris images. WFP uses this platform mainly to increase performance in food and cash distribution (WFP, 2018, p. 45). Similar to BIMS, SCOPE operates online and offline, stores biometric data in a central database, and supports the distribution of ration cards with identity numbers (WFP, 2014). One interviewee remarked:

> *The chips inside these cards have two functions: storing e-vouchers and storing the biometric and biographical information. [. . .] When a beneficiary shows up to receive an entitlement, we scan their fingerprint and perform [a] one-to-one check with the stored template in the card thanks to mobile point-of-sale devices. [. . .] Once the cardholder is verified, the transaction takes place, and [an] e-voucher, cash, or commodity value is topped up into the card to be spent or redeemed at distribution points.*

WFP also registers people and runs a one-to-many authentication to check for duplicates. Moreover, verification of identities does not always require fresh data collection. Sometimes a match is sought between the data on the card and the profiles in the database.

Alongside its food and cash programmes, WFP has used biometrics for its education programme for secondary school girls in Pakistan. The latter included fingerprinting students to keep attendance data, and girls who attended at least 80 per cent of classes each month were rewarded with cash grants (WFP, 2017b). Moreover, in Jordan, refugees scan their irises at local supermarkets to purchase food through entitlements recorded on a blockchain-based computing platform (WFP, 2017a). Here, the verification exercise not only ensures that the intended beneficiaries claim the aid, but it also helps to track purchasing trends. WFP also utilised voice response technology in the response to the Ebola outbreak (2014–16) in the Democratic Republic of the Congo (DRC), Guinea, Liberia, Sierra Leone, and Somalia (WFP, 2015, p. 31). In such operations, the agreement with the state authorities is of great importance. Regardless of institutional determination to use biometrics, it may not be possible unless the government of the country in which WFP operates allows it. For example, in 2019, WFP suspended food aid in Yemen over a dispute about biometric registration with Houthi leaders (WFP, 2019b). Also, the agency was not permitted to collect biometric data in some regions of Afghanistan in 2020 (WFP, 2020a).

WFP works with companies, including IrisGuard and the NEC Corporation, as technology providers. Biometric data are often collected by WFP staff or implementing partners on behalf of the agency. However, WFP also enters into data collaborations with government institutions, other HOs, and the private sector. For instance, a cooperation with Western Union allowed WFP to distribute cash assistance to people affected by Typhoon Goni in the Philippines in 2020 (WFP, 2020b). And its e-voucher programme in Bangladesh is integrated into UNHCR and government databases to maintain up-to-date beneficiary data (WFP, 2015, p. 90). In fact, the global 2018 Data Sharing Addendum ensured the interoperability of BIMS and SCOPE, including biometric data exchange (UNHCR and WFP, 2018). WFP also signed an agreement in 2018 with the International Organization for Migration to exchange biometric data (WFP, 2019a). In some cases, the agency also allows its partners to access SCOPE. Rather than providing direct access to biometric data, it permits partners to confirm the identity of individuals as a result of a one-to-one check. One interviewee explained:

> *We have service agreements in place with a few organisations, which allows them to distribute aid to beneficiaries using SCOPE. But this does not mean that they [have] access to beneficiary data. It is a way of ensuring complementary assistance. Let us say in this scenario, we provide food to people and UNICEF [United Nations Children's Fund] wants to provide water and sanitation supplies. We would want to make sure that we serve the same people. [. . .] So, the beneficiaries take [the] WFP SCOPE card and can use it for different agencies.*

WFP does not have a biometrics policy, but the 2016 Guide to Personal Data Protection and Privacy defines biometric data as sensitive and personal, requiring strict protection

and confidentiality (WFP, 2016, p. 3). It gives beneficiaries the right to request data updates, corrections, and deletions (WFP, 2016, p. 29). The Guide also identifies specific measures to ensure physical, technological, and organisational security, including restricting access to storage facilities and server rooms, utilising anti-virus and anti-malware software, encryption, a Privacy Impact Assessment (PIA), password protection, and staff training (WFP, 2016, p. 42). WFP operations also include a complaint and feedback mechanism for beneficiaries. The interviewees also underlined the importance accorded to consent-seeking mechanisms. As a matter of fact, I was informed that the very first page on the SCOPE screen is the consent text and that no action can be taken without approving this form. WFP has a DPO responsible for compliance with data protection principles. However, the 2017 internal audit found several data protection flaws in SCOPE and recommended 'major improvements', emphasising that the agency was handling huge amounts of personal data without proper safeguards (Parker, 2018). Moreover, similar to UNHCR, one challenge facing WFP is to determine data retention periods. One interviewee stated:

> *Data retention can range from two to five years. But that depends on a case-by-case basis because we have people who are repeatedly our beneficiaries. For example, we have a seasonal support assistance, and we assist the same people every winter. We keep their data for [a] longer period because we do not want to register them each year.*

International Committee of the Red Cross

The ICRC has labelled biometrics as the biggest challenge to data controllers in humanitarian efforts and advocated limited use of this technology (Staehelin, 2020). The ICRC brands its approach as 'less data, more protection' (ICRC, 2021b). This discreet and data protection-based approach can also be observed in the implementation of the Biometrics Policy in 2019. The ICRC uses biometrics mainly as part of the Restoring Family Links programme and for identifying human remains to determine the fate of the missing and dead (ICRC, 2019a, p. 146). Biometrics helps to locate missing persons and reconnect relatives who had to separate due to violence or migration. One interviewee commented:

> *We run facial recognition over pictures that have been provided by family members to match against the photos of people who contacted [a] National Society to manifest themselves as looking for their family members. [. . .] In the very limited scenario of missing persons, we also identify human remains with DNA [(deoxyribonucleic acid)] profiling.*

The Biometrics Policy also authorises other use cases, such as using fingerprints to issue travel documents, accessing servers and control rooms on the premises, and identifying individuals who have committed malicious acts against ICRC personnel (ICRC, 2019b). What they have in common is a tendency to derive information from one type of biometric modality. Furthermore, the ICRC considers the possibility to process biometric data collected by other HOs to continue aid provision (ICRC, 2019b). In response to a question about biometric use cases, particularly for aid distribution, one interviewee

replied: 'We envision the possibility to use biometrics for the registration and management of aid distribution. [. . .] So, it is a use case that is authorised, but it is not actually done at the moment'. Even other use cases that are not covered by the Policy may be implemented with the approval of the ICRC Data Protection Office (ICRC, 2019b). When asked what kind of future uses were envisioned, one interviewee remarked: 'I do not think it is thought-out yet, but the Policy had to be somehow future-proof. [. . .] There is always a possibility to explore what technology brings to our attention and to decide whether and under what framework it can be accepted'.

Keeping this in mind, the ICRC is stricter in some matters. For example, the Policy determines that one-to-many authentication is riskier than one-to-one authentication (ICRC, 2019b). Even though the organisation uses both functions, one-to-many authentication against a centralised database of biometric profiles of living individuals is restricted. Instead, the ICRC advocates for token-based verification for the provision of humanitarian services, such as a card that holds biometric registration data and information about entitlements. This way data subjects can carry the card, and the ICRC preserves no biometric data (ICRC, 2019b). However, there is one exception, namely the Trace the Face website, on which the ICRC uploads facial images of people who are looking for their relatives and loved ones. The organisation compares the facial images of deceased individuals against this database to try to achieve a match with a person reported missing (ICRC, 2019b).

The Policy authorises ICRC staff to collect biometric data, and the Head of Delegation has overall responsibility for data processing in country operations. Occasionally, especially due to logistical, operational, or technical constraints, the ICRC works with other HOs, National Societies, and service providers, such as forensic laboratories. These partners can process biometric data on behalf of the ICRC if they comply with the organisation's standards (ICRC, 2019b). For example, a memorandum of understanding was signed with the NEC Corporation in June 2021. Its contents include image recognition, AI (artificial intelligence)-based predictions of minefields, and protection of personal data (NEC Corporation, 2021). Indeed, the ICRC relies on some partnerships and suppliers in general for any kind of system except for facial recognition. One interviewee mentioned that the ICRC built this system essentially in-house. Moreover, even though interviewees confirmed that there is currently no biometric data sharing, the Policy identifies certain conditions that may make data sharing possible. These encompass the vital interest of the data subject, the fulfilment of the humanitarian obligation, the informed consent of the data subject, the execution of a DPIA, and the recipient's written commitment to use the data for humanitarian purposes only (ICRC, 2019b).

Lastly, the Policy introduced a number of biometric data protection measures, including data minimisation, pseudonymisation, one-way encoding of biometric images, encryption of data at rest and in transit, establishing an audit trail, and a DPIA (ICRC, 2019b). The DPIA assesses data protection and information security risks, as well as the capacity of the ICRC and its partners to resist data sharing requests from authorities. Data subjects have the right to request access to and the correction and deletion of personal data, including biometric data. The ICRC is also rigid about the data retention period.

Accordingly, the images are deleted after template conversion, and templates are subject to a retention period linked to the specific purpose for which personal data were collected (ICRC, 2019b). Finally, the ICRC explains to beneficiaries the basis and purpose of data activities before collecting any information and respects their decisions if they refuse to give their biometric data (Kuner and Marelli, 2017, p. 136). However, informed and freely given consent is considered infeasible in emergency situations, especially when consenting to the processing of personal data is a prerequisite for receiving humanitarian assistance (Kuner and Marelli, 2017, p. 60). The ICRC also has a DPO working independently to supervise all personal data protection matters.

Médecins Sans Frontières

The biometrics story of MSF goes back to 2017, when MSF Canada had planned to offer 'Unique Biometric IDs' to beneficiaries in line with the Transformational Investment Capacity Project. This approach aimed to keep accurate records of those in need of medical intervention located in hard-to-reach areas. With biometrics, MSF had planned to identify quickly potential patients and monitor continuously the conditions of those in need of treatment. Therefore, it had envisioned the use of both identification and verification techniques. In this context, MSF staff were going to collect fingerprint data from people seeking healthcare in a resource-limited setting; Pakistan was selected for a pilot study. One interviewee said:

> *We were not going to test the technology. We knew it worked [. . .] we had heard that other organisations were using it. [. . .] We were testing [. . .] the ability to obtain real consent and community acceptance of a technology that was primarily used for control of populations.*

The international MSF movement is composed of 25 associations worldwide, and these associations are linked to six operational centres. Consequently, it is not easy to talk about a joint MSF policy and regulation, and most MSF documents are available only for internal use. The interviews revealed no knowledge of any biometrics projects in MSF aside from Unique Biometric IDs. However, the technology was going to be employed across MSF associations once proven effective. The planned project successfully passed the PIA as it addressed risks and introduced relevant data protection measures such as data encryption, local storage, and strict data sharing regulations. However, MSF decided not to deploy biometrics, neither in Pakistan nor anywhere else in the world. Interviewees noted that the project was not completed owing to increasing concerns about the need for a global MSF review of the ethical considerations and a framework and protocol to inform the operational use of biometrics within the organisation. One interviewee stated:

> *The challenge in deploying biometrics was ethical and regulatory, not technical. [. . .] The planned project wanted to test biometrics to see if [the] benefits would outweigh some of the concerns. And we were not able to secure enough pilot sites in order to go forward with the project.*

Moreover, it is worth mentioning that MSF uses telecommunication and information technology to overcome political obstacles and a lack of economic resources, thereby providing remote clinical healthcare in war-torn regions (Delaigue et al., 2018, p. 2). The system links healthcare professionals working on MSF projects with specialists worldwide. It entails, inter alia, transmitting non-traditional medical biometric data such as MRI (magnetic resonance imaging), X-ray, and pathology images to specialists (MSF, 2016). The purpose of this is not to identify individuals but to solve the medical problems of patients. MSF has been utilising telemedicine services since 2010 and reports that data exchange is carried out while protecting the data privacy of patients (MSF, 2016). Although there is no publicly available MSF document outlining what data protection measures are implemented, MSF Canada's 2022 Data Officer (Telemedicine) job posting gives a clue. Accordingly, the person sought is expected to conduct a PIA, organise data privacy trainings for other employees, and ensure compliance with data protection regulations, among other duties. These regulations are specifically referred to as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the European Union's 2016 General Data Protection Regulation (GDPR) (MSF, 2022).

MSF issued a Health Data Protection Policy, aiming to ensure the safety of patients and community data by setting out core principles. Although this document is available for internal use only, an infographic summarising the core values of this policy is publicly available. Accordingly, responsible data management practices are shaped within the framework of the best interest of individuals, health ethics, and the do-no-harm principle (MSF, n.d.). The policy highlights the importance of limited and proportional data practices, transparent information sharing, confidentiality, consent-seeking, and secure data storage (MSF, n.d.). Furthermore, it acknowledges that 'data which reveals or implies racial or ethnic origin' are highly sensitive and require special protection. Lastly, the policy outlines several data protection practices, such as routine threat analysis, restricted and audited access, password protection, encryption, and training MSF staff in this matter (MSF, n.d.). MSF also published a Data Sharing Policy in 2012, permitting access to the MSF dataset by other HOs, researchers from academia, and private companies, such as drug businesses. However, it obliges data sharing parties to abide by certain principles, such as medical confidentiality, respecting privacy and dignity, equity, efficiency, and local benefit (MSF, 2013, p. 5). Even though it does not mention biometrics, it defines sensitive data: 'data that can put data subjects at risk of stigma, discrimination and even criminal sanction, data on sicknesses, and data that could indirectly imply racial or ethnic origin'. Therefore, MSF may decide that such data are unsuitable for sharing (MSF, 2013, p. 8). MSF also has a DPO to monitor data protection and supervise the various MSF entities' compliance with and maintenance of the GDPR.

World Vision International

WVI appears to use biometric data in the broadest sense when co-implementing projects with WFP. Indeed, WVI is WFP's biggest implementing partner, and WVI staff are given access to SCOPE in some cases to collect biometric data on behalf of WFP. An example

is the programme in eastern DRC, where WVI staff collected fingerprints from internally displaced persons to provide identity documents and distribute food respectively in June 2014 and April 2015 (Lee, 2015). However, WVI has also used biometric data in its own operations, especially for health programmes, such as the Ebola vaccine trial. In fact, as part of an Ebola Vaccine Deployment, Acceptance and Compliance (EBODAC) consortium, World Vision Ireland used irises and fingerprints to identify participants (Willems, 2018). After a trial period, the approach was changed to capturing iris-only data using a mobile tablet (Willems, 2018). Given that the two injections were 56 days apart, biometrics allowed participants to take the required shots in Sierra Leone and Rwanda (Lutz et al., 2017, p. 12). In this context, biometric data helped to identify those who came for the first dose and verify that those who showed up for the second dose were the same people. One interviewee mentioned that the data are stored in a centralised database. The EBODAC consortium comprises four partners: the Grameen Foundation, Janssen Pharmaceuticals, the London School of Hygiene and Tropical Medicine, and World Vision Ireland (WVI, 2018).

It is also worth mentioning Last Mile Mobile Solutions (LMMS), a technology solution developed by WVI in 2008 to improve beneficiary registration, verification, distribution planning, and management, including cash-based assistance, monitoring, and reporting (WVI, n.d.). Some organisations using LMMS are Action Against Hunger, CARE, Oxfam, Save the Children, and WVI (WVI, n.d.). LMMS involves the collection and storage of data usually linked to food programming (WVI, n.d.). A typical LMMS deployment entails collecting photographs of the beneficiaries complementary to relevant biographical data such as name, location, and particular vulnerability information (Chibafa, 2014, p. 19). The WVI website about LMMS Solutions reports that the system functions online and offline, supports data import and export, and is integrated into UNHCR's BIMS and WFP's SCOPE. It is, however, important to note that LMMS does not utilise automated identity verification. Beneficiaries were able to claim their entitlements by scanning the barcode on their distributed cards, and eligibility is determined by a visual match using photographs stored in the database. Interviews disclosed that LMMS works in partnership with Simprints, a non-profit technology company, as a provider of technological solutions.

Lastly, a discussion paper on the WVI website written by World Vision staff refers to three policies that regulate data protection issues: Partnership Policy on Global Data Protection and Privacy; Partnership Policy on Information Security; and Management Policy on Information Security. Unfortunately, these policy papers are not publicly available. For data protection efforts, however, one interviewee explained that DPIAs are conducted before starting a project and a risk assessment is carried out annually in each country operation. Every WVI device has built-in encryption, and there is also a mandatory online training course on data protection for all staff.

Comparative display of the findings

Table 4 summarises the findings. Information on the biometrics project that MSF planned but did not implement is also included in the table.

Table 4. Comparative display of the findings

	UNHCR	WFP	ICRC	MSF	WVI
Functions and services	One-to-many, one-to-one, and one-to-few authentications. Registration, cash/in-kind aid delivery, repatriation, and identity management.	One-to-many and one-to-one authentications. Food/cash assistance, registration, and education.	One-to-many and one-to-one authentications. Reuniting families, locating missing persons, and identifying the dead.	One-to-many and one-to-one authentications. Health assistance.	One-to-many and one-to-one authentications. Registration, health assistance, and cash/in-kind aid delivery.
Types and systems	Fingerprints, iris, and photographs. Multimodal, centralised database; online/offline.	Fingerprints, iris, photographs, and voice. Multimodal, centralised database and token-based ration cards; online/offline.	Fingerprints, DNA, and photographs. Unimodal, token-based cards; online/offline.	Fingerprints, MRI, X-ray, and pathology images. Unimodal, local storage.	Fingerprints, iris, and photographs. Multimodal, centralised database; online/offline.
Data collaborations	Other UN agencies, partner NGOs, financial service providers, governments, and private companies.	Other UN agencies, partner NGOs, financial service providers, governments, and private companies.	Other HOs, National Societies, and private companies.	Other HOs, researchers, and private companies.	UN agencies, governments, partner NGOs, and private companies.
Data protection measures	Encryption, password protection, staff training, a DPIA, consent-seeking, and standard operating procedures.	Anti-virus and anti-malware software, encryption, consent-seeking, a DPIA, password protection, and staff training.	Data minimisation, pseudonymisation, encryption, one-way encoding, audit trail, a DPIA, deletion of images, template conversion, and data retention period.	A DPIA, consent-seeking, encryption, routine threat analysis, restricted and audited access, password protection, and staff training.	A DPIA, a PIA, encryption, and staff training.

Source: author.

Emerging trends and implications

The findings presented above demonstrate that HOs have variational biometric practices. This section analyses similar and different approaches to reveal trends and draw inferences about how biometrics is used in the humanitarian context.

First, empirical findings demonstrate that the ICRC, UNHCR, WFP, and WVI use both identification and verification techniques. However, the ICRC uses one-to-many authentication only on the decedent. Moreover, one-to-one authentication seems to be the prevailing function in WFP operations, while UNHCR's work primarily requires one-to-many authentication for identifying refugees. Biometric ID cards issued by HOs serve as functional identities for individuals to access humanitarian services such as food, cash, healthcare, and family reunification, whereas UNHCR cards frequently serve as foundational identities that entitle refugees to more rights than merely access to services. However, the narrative of digital identity provision is claimed to undermine a person's existing self-identity and legitimise distrust of self-affirmations (Holloway, Al Masri, and Yahia, 2021, p. 22). The identity of people encompasses more than fixed numbers determined by their unique physical characteristics, and the digital identity is asserted to mask an ulterior motive to increase control over people (Amoore, 2006; Madianou, 2019; Metcalfe and Dencik, 2019). It is also argued that recognised existence of marginalised groups, including refugees, hardly empowers them with sustainable and meaningful political and social rights (Cheesman, 2022). In this case, the varying applications of biometric identification in humanitarian response indicate a trade-off between access to rights and services by beneficiaries to some extent and the reduction of their identities to traceable numbers in a database.

Second, the findings indicate that behavioural traits are not as popular as physical ones. Indeed, face images and fingerprints are the most used biometric traits in the humanitarian context. Nevertheless, the ICRC's DNA capturing stands out as an unconventional practice. DNA collection has raised concerns about the disclosure of health- and genetics-related personal information (Wendehorst and Duller, 2021). However, using DNA to identify human remains refers to a different level of intrusiveness and impacts on personal privacy. At this point, the debate about the neutrality of technology comes to mind. It is famously stated that '[t]echnology is neither good, nor bad; nor is it neutral' (Kranzberg, 1986, p. 545). Building on this aphorism, some have highlighted the algorithmic bias, contending that technological tools systematically reflect human bias and subjectivity (Olwig et al., 2020, p. 161). Yet, others have argued that the technology is neutral (Gelb and Clark, 2013, p. 17). Under the circumstances, the use of different types of biometric data in different humanitarian settings implies that the impact of technology can be either advantageous or hazardous, depending on its political context within the larger system in which it operates. In other words, the same biometric technology can produce disparate outcomes depending on how it is used.

In addition, unlike UNHCR, WFP, and WVI, MSF's planned project and the ICRC's biometric policy envisaged using a unimodal system and decentralised data storage. The collection of multiple biometric modalities is considered beneficial in creating an alternative for those who are unable to give certain data types, while the use of a unimodal system prevents the disclosure of more personal information (Gelb and Clark, 2013). From a practical perspective, centralised data storage allows identification and data deduplication, unlike a tokenised system (Sukaitis, 2021, p. 41). This means that some biometric

systems may not have as much of an impact on fraud prevention as expected. But not creating permanently identifiable records, to some extent, facilitates the prevention of third-party access to data and gives aid beneficiaries more control over the purposes for which their data will be utilised. In this regard, decentralised identity systems are a breath of fresh air in the area of studies linking the data collection activities of HOs with data colonialism, particularly underlining the concerns related to the accountability gap in data ownership (Currion, 2015; Johnson and Campbell, 2020; Hersey, 2021). Therefore, the variational practices of biometric data storage imply a trade-off between improved efficiency of humanitarian programmes and protection of beneficiary data.

Third, HOs rely on partnerships in the use of biometric data. Critics have previously questioned the fact that technology companies and financial and banking institutions do not necessarily share similar ethical principles with humanitarians (Aly, 2013; Malik, Mohr, and Irvin-Erickson, 2018). It is argued that aid beneficiaries represent future market opportunities for profit-oriented companies (Saldinger, 2016) and that personal data can be used with less emphasis on privacy and data protection by private actors. The findings of this paper show that the ever-increasing role of private companies in the humanitarian aid sector is further enhanced by biometric data activities. Yet, biometric data collaborations vary. WVI uses biometric data more frequently in its joint operations with UNHCR and WFP than in its own activities. Indeed, UNHCR and WFP engage in more data collaborations than the ICRC, MSF, and WVI. These two UN agencies claim to refrain from transferring any data to a private actor or state that does not fulfil its responsibility to protect its people or commits human rights violations. The findings, though, exemplify some contrary applications. It is argued that once data are shared, HOs lose control over future use cases (Madianou, 2019, p. 591). Third-party access to biometrics has particularly been associated with increasing government surveillance, where personal data are used to control those who are meant to be assisted (Hosein and Nyst, 2013; Latonero, 2019; Weitzberg et al., 2021). However, despite the ability of biometric data to enable forms of surveillance, not all practices equally contribute to it. Not all HOs share biometric data with public and private actors, and data sharing is not always realised by data transfer, but sometimes by giving controlled access to database. Therefore, the trade-off here is between the use of biometric data for non-humanitarian purposes versus leveraging the private sector, preventing multiple HO datasets floating around, and maintaining good relations with governments.

Lastly, despite addressing similar risks of biometrics, HOs differ in data protection measures implemented. MSF has the strictest data protection measure by not using biometric identification at all. But this also means not leveraging technological innovations for operational benefit. Furthermore, although MSF does not use any automated identification system, 'hidden biometrics' such as knee X-rays and brain prints are increasingly recognised as unique identification methods (Shamir et al., 2009; Bhatnagar and Mishra, 2020). Moreover, UNHCR and WFP retain beneficiary data for a longer time as compared to other HOs. Keeping personal data longer than necessary has raised concerns about the privacy rights of data subjects (Gelb and Clark, 2013; Wendehorst and Duller, 2021),

and determining the data retention period is exemplified as one of the best data protection practices (Hayes and Marelli, 2019; Gazi, 2020). Thus, retaining the data of people who are no longer assisted implies a trade-off between streamlining efforts in recurring humanitarian operations and risking the probability of identity disclosure in the event of a data breach.

The findings also demonstrate differing perspectives and practices in consent-seeking. Although all HOs agree that the collection and use of data should be consent-based, there appear to be some inconsistent UNHCR and WFP practices. What is more, the ICRC considers consenting in exchange for life-saving assistance invalid. In fact, the extent of the ability of data subjects to exercise choice has been a contested subject. The unbalanced power relationship between HOs and aid beneficiaries is argued to put vulnerable people in a situation where they cannot express their reluctance to data collection (de Torrenté, 2013; Rahman, 2018; Kaurin, 2019). Ultimately, variational consent-seeking practices imply a trade-off between disregarding appropriate information sharing or offering alternative registration methods and a meaningful choice in which aid continues to be distributed, even if consent cannot be obtained.

Conclusion

The scholarly debate about the use of biometrics in the humanitarian context revolves around its benefits and risks, and the humanitarian aid literature has so far concentrated on which one outweighs the other. However, there is no one-size-fits-all approach to humanitarian biometrics. Taking UNHCR, WFP, the ICRC, MSF, and WVI as case studies, this paper has examined relevant documents and 17 semi-structured interviews with humanitarian practitioners and demonstrated variational biometric data management in humanitarian response. Four of the five largest HOs use automated biometric systems in their operations. Yet, they use diverse types and functions of biometric data for different services, collaborate with several actors, and use various data protection measures. WVI does not have an official position or view on biometrics, and use cases are quite ad hoc. For UNHCR and WFP, biometric data collection is a regular part of operations for maximum efficiency. The ICRC seems more focused on data protection as it currently allows limited use. And, by contrast, MSF has no operation involving biometrics.

Ultimately, variational practices imply that the advantages and risks of using biometric data in the humanitarian context differ depending on how it is done. Therefore, it is encouraged to mount related arguments on a case-by-case basis. This paper was not intended to evaluate the practices of HOs, nor to determine whether the use of biometric data in the field of humanitarian aid should increase or decrease. However, the results can be an asset for future research to provide a more in-depth analysis of responsible use of this technology. What still needs to be clarified is the role of the other actors in humanitarian action in biometric use cases. In addition, technological development can momentarily open new doors. Consequently, the findings are subject to change, and it is favourable to keep them up to date.

Acknowledgements

I would like to acknowledge the financial support provided by the Agency for Management of University and Research Grants of the Government of Catalonia to carry out this research. I would also like to express my sincere gratitude to Miriam Bradley for her insightful discussions and feedback on the manuscript. Finally, I would like to thank my family for their unwavering support throughout this research.

This paper reports on an analysis of primary data. The ethics of data collection and analysis were approved by the Institutional Committee for the Ethical Review of Projects of the Pompeu Fabra University.

Data availability statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.[1]

Correspondence

Çağlar Açıkyıldız, Pompeu Fabra University and Institut Barcelona d'Estudis Internacionals, Carrer de Ramon Trias Fargas, 25, 27, 08005 Barcelona, Spain.
ORCID: https://orcid.org/0000-0002-7685-8332
E-mail: caglaracikyildiz@gmail.com

Endnotes

[1] This includes the dataset needed to interpret, replicate, and/or build on the methods or findings reported in the paper. However, data availability is subject to fulfilment of any necessary ethical and legal requirements and compliance with the anonymisation agreements I have made with each interview participant.

References

Ajana, B. (2013) *Governing through Biometrics: The Biopolitics of Identity*. Palgrave Macmillan, Basingstoke.

Aly, H. (2013) 'What future for private sector involvement in humanitarianism?'. The New Humanitarian website. 26 August. https://www.thenewhumanitarian.org/analysis/2013/08/26/what-future-private-sector-involvement-humanitarianism (last accessed on 5 October 2023).

Amoore, L. (2006) 'Biometric borders: governing mobilities in the War on Terror'. *Political Geography*. 25(3). pp. 336–351.

Baker, S. and Z. Rahman (2020) *Understanding the Lived Effects of Digital ID: A Multi-Country Study*. January. https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf (last accessed on 5 October 2023).

Barnett, M. and T.G. Weiss (2008) *Humanitarianism in Question: Politics, Power, Ethics*. Cornell University Press, Ithaca, NY.

Bhatnagar, S. and N. Mishra (2020) 'A review of MRI brain print as hidden biometric'. *TEST Engineering and Management*. 83 (May–June). pp. 28,571–28,578.

Burt, C. (2020) 'Iris biometrics from IrisGuard to enable paperless disbursement of refugee cash aid in Egypt'. BiometricUpdate.com website. 24 February. https://www.biometricupdate.com/202002/iris-biometrics-from-irisguard-to-enable-paperless-disbursement-of-refugee-cash-aid-in-egypt (last accessed on 5 October 2023).

Cheesman, M. (2022) 'Self-sovereignty for refugees? The contested horizons of digital identity'. *Geopolitics*. 27(1). pp. 134–159.

Chibafa, K. (2014) 'Why not digital? Technology as an interagency tool in the Central African Republic'. *Humanitarian Exchange*. 62 (September). pp. 19–21.

Currion, P. (2015) 'Eyes wide shut: the challenge of humanitarian biometrics'. The New Humanitarian website. 26 August. https://www.thenewhumanitarian.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics (last accessed on 5 October 2023).

de Torrenté, N. (2013) 'The relevance and effectiveness of humanitarian aid: reflections about the relationship between providers and recipients'. *Social Research*. 80(2). pp. 607–634.

Delaigue, S. et al. (2018) 'Seven years of telemedicine in Médecins Sans Frontières demonstrate that offering direct specialist expertise in the frontline brings clinical and educational value'. *Journal of Global Health*. 8(2). Article number: 020414. https://doi.org/10.7189/jogh.08.020414.

EU (European Union) (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. *Official Journal of the European Union*. 4 May. L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679#:~:text=This%20Regulation%20respects%20all%20fundamental,conscience%20and%20religion%2C%20freedom%20of (last accessed on 5 October 2023).

European Commission, Joint Research Centre (2005) *Biometrics at the Frontiers: Assessing the Impact on Society*. EUR 21585 EN. European Commission, Joint Research Centre, Brussels.

Farraj, A. (2011) 'Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers. *Columbia Human Rights Law Review*. 42(3). pp. 891–941.

Gazi, T. (2020) 'Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR'. *Journal of International Humanitarian Action*. 5 (July). Article number: 9. https://doi.org/10.1186/s41018-020-00078-0

Gelb, A. and J. Clark (2013) *Identification for Development: The Biometrics Revolution*. Working Paper 315. January. Center for Global Development, Washington, DC.

Hayes, B. and M. Marelli (2019) 'Facilitating innovation, ensuring protection: the ICRC Biometrics Policy'. Humanitarian Law & Policy website. 18 October. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/ (last accessed on 5 October 2023).

Hersey, F. (2021) '"You cannot trust a vendor": understanding biometrics in the humanitarian sector'. BiometricUpdate.com website. 4 October. https://www.biometricupdate.com/202110/you-cannot-trust-a-vendor-understanding-biometrics-in-the-humanitarian-sector (last accessed on 5 October 2023).

Holloway, K., R. Al Masri, and A.A. Yahia (2021) *Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises*. HPG Working Paper. October. Overseas Development Institute, London.

Hosein, G. and C. Nyst (2013) *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries*. October. Privacy International, London.

Human Rights Watch (2021) 'UN shared Rohingya data without informed consent'. Website. 15 June. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent (last accessed on 5 October 2023).

ICRC (International Committee of the Red Cross) (2018) 'Statutes of the International Committee of the Red Cross'. 1 January. https://www.icrc.org/en/document/statutes-international-committee-red-cross-0 (last accessed on 5 October 2023).

ICRC (2019a) *Annual Report 2019: Volume I*. https://www.icrc.org/en/document/annual-report-2019 (last accessed on 5 October 2023).

ICRC (2019b) *Policy on the Processing of Biometric Data by the ICRC*. https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf (last accessed on 5 October 2023).

ICRC (2021a). *Annual Report 2021*. https://www.icrc.org/en/document/annual-report-2021 (last accessed on 5 October 2023).

ICRC (2021b) 'The biometrics minefield'. ICRC Inspired website. 26 February. https://blogs.icrc.org/inspired/2021/02/26/the-biometrics-minefield/ (last accessed on 5 October 2023).

Jacobsen, K.L. (2015) 'Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees'. *Security Dialogue*. 46(2). pp. 144–164.

Jacobsen, K.L. (2017) 'On humanitarian refugee biometrics and new forms of intervention'. *Journal of Intervention and Statebuilding*. 11(4). pp. 529–551.

Johnson, M. and E. Campbell (2020) 'Biometrics, refugees, and the Middle East: better data collection for a more just future'. Middle East Institute website. 25 August. https://www.mei.edu/publications/biometrics-refugees-and-middle-east-better-data-collection-more-just-future (last accessed on 5 October 2023).

Kaurin, D. (2019) *Data Protection and Digital Agency for Refugees*. World Refugee Council Research Paper No. 12. May. Centre for International Governance Innovation, Waterloo, ON.

Knox Clarke, P. (2018) *The State of the Humanitarian System*. ALNAP (Active Learning Network for Accountability and Performance in Humanitarian Action), London.

Kranzberg, M. (1986) 'Technology and history: "Kranzberg's Laws"'. *Technology and Culture*. 27(3). pp. 544–560.

Kuner, C. and M. Marelli (2017) *Handbook on Data Protection in Humanitarian Action*. International Committee of the Red Cross, Geneva.

Latonero, M. (2019) 'Stop surveillance humanitarianism'. *The New York Times* website. 11 July. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html (last accessed on 5 October 2023).

Lee, J. (2015) 'IOM deploys biometric verification project to help displaced people in Congo'. Biometric Update.com website. 5 May. https://www.biometricupdate.com/201505/iom-deploys-biometric-verification-project-to-help-displaced-people-in-congo (last accessed on 5 October 2023).

Loy, I. (2021) 'Biometric data and the Taliban: what are the risks?'. The New Humanitarian website. 2 September. https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban (last accessed on 5 October 2023).

Lutz, A., A. Doornbos, A. Kehl, A.E. Ghee, and L. DePauw (2017) *Data Protection, Privacy and Security for Humanitarian & Development Programs*. World Vision International Discussion Paper. https://www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20%26%20Security%20for%20Humanitarian%20%20%26%20Development%20Programs%20-%20FINAL.pdf (last accessed on 5 October 2023).

Madianou, M. (2019) 'The biometric assemblage: surveillance, experimentation, profit, and the measuring of refugee bodies'. *Television and New Media*. 20(6). pp. 581–599.

Magnet, S.A. (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Duke University Press, Durham, NC.

Malik, A.A., E. Mohr, and Y. Irvin-Erickson (2018) *Private-Sector Humanitarians? New Approaches in the Global Refugee Response*. Research Report. September. Urban Institute, Washington, DC.

Metcalfe, P. and L. Dencik (2019) 'The politics of big borders: data (in)justice and the governance of refugees'. *First Monday*. 24(4). Article number: 9934. https://doi.org/https://doi.org/10.5210/fm.v24i4.9934.

MSF (Médecins Sans Frontières) (n.d.) *Health Data Protection Policy*. https://endtb.org/sites/default/files/2019-11/MSF%20Infographics-Health%20Data%20Protection%20Policy_June%202018.pdf (last accessed on 5 October 2023).

MSF (2013) *Data Sharing Policy*. December. https://www.msf.org/sites/default/files/msf_data_sharing_policy_final_061213.pdf (last accessed on 5 October 2023).

MSF (2016) 'Telemedicine helps to bridge the gap between remote areas and large hospitals'. Website. 13 July. https://www.msf.org/telemedicine-280-doctors-little-mohamed (last accessed on 5 October 2023).

MSF (2021) *International Financial Report 2021*. https://www.msf.org/sites/default/files/2022-05/MSF_Financial_Report_2021_FINAL%20provisional.pdf (last accessed on 5 October 2023).

MSF (2022) 'Telemedicine Data Officer'. Website. https://startup.jobs/telemedicine-data-officer-doctors-without-borders-3731900 (last accessed on 9 October 2023).

NEC Corporation (2021) 'NEC and ICRC sign memorandum to utilise Japanese technology to resolve humanitarian issues in conflict areas'. Website. 16 June. https://jpn.nec.com/press/202106/20210616_02.html (last accessed on 5 October 2023).

Olwig, K.F., K. Grünenberg, P. Møhl, and A. Simonsen (2020) *The Biometric Border World: Technologies, Bodies and Identities on the Move*. Routledge, London.

Oxfam (2021) *Oxfam Biometric and Foundational Identity Policy*. 18 May. https://oxfam.app.box.com/v/OxfamBiometricPolicy (last accessed on 5 October 2023).

Parker, B. (2018) 'Exclusive: audit exposes UN food agency's poor data-handling'. The New Humanitarian website. 18 January. https://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling (last accessed on 5 October 2023).

Polk, A. (2020) 'Big brother turns its eye on refugees'. *Foreign Policy* website. 2 September. https://foreignpolicy.com/2020/09/02/big-brother-turns-its-eye-on-refugees/ (last accessed on 5 October 2023).

Prasse-Freeman, E. (2022) 'Nothing to lose but their (block)chains: biometrics, techno-imaginaries, and transformations in Rohingya lives'. *AE: Journal of the American Ethnological Society*. 49(4). pp. 563–579.

Rahman, Z. (2018) *Biometrics in the Humanitarian Sector*. https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf (last accessed on 5 October 2023).

Saldinger, A. (2016) 'Where is the private sector in humanitarian response?'. Devex website. 29 June. https://www.devex.com/news/where-is-the-private-sector-in-humanitarian-response-88328 (last accessed on 5 October 2023).

Schoemaker, E., D. Baslan, B. Pon, and N. Dell (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). pp. 13–36.

Shamir, L., S. Ling, S. Rahimi, L. Ferrucci, and I.G. Goldberg (2009) 'Biometric identification using knee X-rays'. *International Journal of Biometeorology*. 1(2). pp. 365–370.

Staehelin, B. (2020) 'Humanitarian effectiveness through new technology requires standards of control over data, data integrity and data availability'. International Committee of the Red Cross website. 10 June. https://www.icrc.org/en/document/humanitarian-effectiveness-through-new-technology-requires-standards-control-over-data-data (last accessed on 5 October 2023).

Sukaitis, J. (2021) *Building a Path Towards Responsible Use of Biometrics: A Proposal for Security and Data Privacy Evaluation of Biometric Systems*. Master's thesis, École polytechnique fédérale de Lausanne, Switzerland. https://infoscience.epfl.ch/record/285077?ln=en (last accessed on 5 October 2023).

Swithern, S. (2015) *Global Humanitarian Assistance Report 2015*. http://www.globalhumanitarianassistance.org/report/gha-report-2015 (last accessed on 5 October 2023).

Tekle, T.-A. (2020) 'Refugees in Ethiopia's camps raise privacy and exclusion concerns over UNHCR's new digital registration'. Global Voices website. 19 March. https://advox.globalvoices.org/2020/03/19/refugees-in-ethiopias-camps-raise-privacy-and-exclusion-concerns-over-unhcrs-new-digital-registration/ (last accessed on 5 October 2023).

UN OCHA (United Nations Office for the Coordination of Humanitarian Affairs) (2021) *From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action*. April. https://www.unocha.org/publication/policy-briefs-studies/digital-promise-frontline-practice-new-and-emerging-technologies (last accessed on 5 October 2023).

UN OCHA (2022) *Global Humanitarian Overview 2022*. https://reliefweb.int/report/world/global-humanitarian-overview-2022 (last accessed on 5 October 2023).

UNHCR (United Nations High Commissioner for Refugees) (2003) 'Afghanistan: Iris-testing proves successful'. Briefing Notes. 10 October. https://www.unhcr.org/news/briefing/2003/10/3f86a3ac1/afghanistan-iris-testing-proves-successful.html (last accessed on 5 October 2023).

UNHCR (2015a) 'Biometric Identity Management System'. Brochure. http://www.unhcr.org/protection/basic/550c304c9/biometric-identity-management-system.html (last accessed on 5 October 2023).

UNHCR (2015b) *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*. May. https://www.refworld.org/docid/55643c1d4.html (last accessed on 5 October 2023).

UNHCR (2019). *Global Report 2019*. https://www.unhcr.org/globalreport2019/ (last accessed on 5 October 2023).

UNHCR (2021a) *Update on Budgets and Funding (2020-2021)*. Executive Committee of the High Commissioner's Programme. EC/72/SC/CRP.7. 4 March. https://www.unhcr.org/uk/media/update-budgets-and-funding-ec-72-sc-crp-7 (last accessed on 5 October 2023).

UNHCR (2021b) 'Government of Pakistan delivers first new biometric identity smartcards to Afghan refugees'. Website. 25 May. https://www.unhcr.org/asia/news/press/2021/5/60ae48424/government-of-pakistan-delivers-first-new-biometric-identity-smartcards.html (last accessed on 5 October 2023).

UNHCR (2022) *Biometrics*. https://help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN_Final_April2022.pdf (last accessed on 5 October 2023).

UNHCR and WFP (World Food Programme) (2018) *Addendum on Data Sharing to the January 2011 Memorandum of Understanding Between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP)*. September. https://emergency.unhcr.org/sites/default/files/WFP%20Addendum%20on%20data%20sharing%20%282018%29.pdf (last accessed on 5 October 2023).

UNHCR and WFP (2020) *Joint Guidance: Targeting of Assistance to Meet Basic Needs*. https://www.unhcr.org/media/joint-guidance-targeting-assistance-meet-basic-needs (last accessed on 5 October 2023).

United States Department of Homeland Security (2019) *Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share*. DHS/USCIS/PIA-081. 13 August. https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf (last accessed on 5 October 2023).

Weitzberg, K., M. Cheesman, A. Martin, and E. Schoemaker (2021) 'Between surveillance and recognition: rethinking digital identity in aid'. *Big Data & Society*. 8(1). https://doi.org/10.1177/20539517211006744.

Wendehorst, C. and Y. Duller (2021) *Biometric Recognition and Behavioural Detection*. PE 696.968. August. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968 (last accessed on 5 October 2023).

WFP (World Food Programme) (2014) *SCOPE in Five Minutes*. https://documents.wfp.org/stellent/groups/public/documents/communications/wfp272586.pdf (last accessed on 5 October 2023).

WFP (2015) *Annual Performance Report for 2014*. https://documents.wfp.org/stellent/groups/public/documents/eb/wfpdoc063825.pdf (last accessed on 5 October 2023).

WFP (2016) *WFP Guide to Personal Data Protection and Privacy*. June. https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/ (last accessed on 5 October 2023).

WFP (2017a) 'Blockchain against hunger: harnessing technology in support of Syrian refugees'. Website. 30 May. https://www.wfp.org/news/blockchain-against-hunger-harnessing-technology-support-syrian-refugees (last accessed on 5 October 2023).

WFP (2017b) 'First cash assistance to secondary girl students using biometrics in Fata'. Website. 24 May. https://www.wfp.org/news/first-cash-assistance-secondary-girl-students-using-biometrics-fata (last accessed on 5 October 2023).

WFP (2018) *Annual Performance Report for 2017*. https://docs.wfp.org/api/documents/5c0a93ecec0f4dcc9916c3978bae238e/download/ (last accessed on 5 October 2023).

WFP (2019a) 'IOM, WFP conduct first beneficiary data exchange in South Sudan'. Website. 27 June. https://www.wfp.org/news/iom-wfp-conduct-first-beneficiary-data-exchange-south-sudan (last accessed on 5 October 2023).

WFP (2019b) 'World Food Programme begins partial suspension of aid in Yemen'. Website. 20 June. https://www.wfp.org/news/world-food-programme-begins-partial-suspension-aid-yemen (last accessed on 5 October 2023).

WFP (2020a) *Afghanistan: Annual Country Report 2020*. https://www.wfp.org/publications/annual-country-reports-afghanistan (last accessed on 5 October 2023).

WFP (2020b) *WFP: Philippines Country Brief. December 2020*. https://docs.wfp.org/api/documents/WFP-0000122988/download/ (last accessed on 5 October 2023).

WFP (2021) *Annual Performance Report for 2020*. https://www.wfp.org/publications/annual-performance-report-2020 (last accessed on 5 October 2023).

Willems, A. (2018) 'Ebola vaccine Deployment, Acceptance and Compliance (EBODAC) – the simple story'. European Federation of Pharmaceutical Industries and Associations website. 3 September. https://www.efpia.eu/news-events/the-efpia-view/blog-articles/03092018-ebola-vaccine-deployment-acceptance-and-compliance-ebodac-the-simple-story-guest-blog/ (last accessed on 5 October 2023).

WVI (World Vision International) (n.d.) 'How LMMS works'. Website. https://www.wvi.org/disaster-management/how-lmms-works (last accessed on 5 October 2023).

WVI (2018) *EBODAC: Ebola Vaccine Trial Brochure*. https://www.wvi.org/sites/default/files/EBODAC_Flyer_2018-06-14_v08_final.pdf (last accessed on 5 October 2023).

WVI (2021) *Global Annual Report 2020*. https://www.wvi.org/sites/default/files/2021-07/World%20Vision%20International%20Global%20Annual%20Report%202020%20%282%29.pdf (last accessed on 5 October 2023).