Primer

Biometrics in the Humanitarian Sector

JULY 2023

THE ENGINE ROOM

CONTENTS

This primer provides key background information for those new to biometrics or looking to refresh their knowledge. It presents a high level overview of biometric data and its uses. The primer is designed to be a companion to our main report, “Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023)” (which you can access here) but can also stand alone. In particular, the primer contains a discussion of the risks and benefits of biometrics that are not discussed in detail in our main report.

What are biometrics?

Biometrics is a term that is commonly used to refer to a set of systems/technologies that allow for “establishing the identity of a person based on the physical or behavioural attributes associated with an individual.”[1] They work by capturing a digital representation of an individual’s biometric data, which in turn is used as a point of comparison for the purpose of recognition – in this sense, they can be thought of as **technologies of “capture and comparison”**.[2]

Biometric data

Biometric data is “any automatically measurable, robust and distinctive physical characteristic [attribute] or personal trait that can be used to identify an individual or verify the claimed identity of an individual”.[3] Physical (or physiological) attributes are those related to the shape or composition of the body, such as fingerprints, palmprints, iris patterns, facial features, vein patterns, and DNA.[4] Behavioural attributes include gait,

[1] Arun Ross and Anil K. Jain, “Biometrics, Overview,” in *Encyclopedia of Biometrics,* eds. Stan Z. Li and Anil Jain (Boston: Springer, 2009), 168-172, https://doi.org/10.1007/978-0-387-73003-5_182.

[2] UNICEF, “Faces, Fingerprints & Feet,” *UNICEF,* July 2022, https://data.unicef.org/resources/biometrics/.

[3] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age* (New York: McGraw-Hill/Osborne, 2003).

[4] World Bank, “Technology Landscape for Digital Identification,” *World Bank,* 2018, https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf.

keystroke patterns, and mouse usage.[5] Voice pattern is considered both a physiological and a behavioural attribute.[6]

The type of attribute collected and compared is known as **modality** – for example, fingerprint and iris are different biometric modalities. Modality, as well as choices of software and hardware, are typically driven by the application envisioned (ie. needs, context, goals).[7] Emerging modalities include vein patterns,[8] earprint, footprint, hand geometry, DNA and even heartbeat (EKG).

Modalities in the humanitarian sector

The most common modalities of biometrics seen in the humanitarian sector are fingerprints and iris scans, widely employed across a variety of use cases, for both identification and verification purposes. Facial recognition systems were cited as a modality of interest for the sector by interviewees. The use of voice recognition is an emerging modality and was piloted by CARE to support verification in the context of a cash-based assistance program in Somaliland (read more in "Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023)," Section 2: State of Play).[9]

While the use of biometrics is not new, the use of digital systems based on biometrics has increased in past decades due to their potential to establish a person's identity with high confidence compared to other forms of personal data. It is worth noting, however, that while biometrics can act as digital tools to enhance identity management systems, they "are not enough in their own right to establish a legal identity."[10] That means biometrics alone cannot convey any of the other information that is usually required to create an

[5] World Bank, "Technology Landscape for Digital Identification," 15.

[6] Jean Hennebert, "Speaker Recognition, Overview," in *Encyclopedia of Biometrics,* eds. Stan Z. Li and Anil Jain (Boston: Springer, 2009), 1262-1270, https://doi.org/10.1007/978-0-387-73003-5_182.

[7] David Day, "Biometric Applications, Overview," in *Encyclopedia of Biometrics,* eds. Stan Z. Li and Anil Jain (Boston: Springer, 2009), 169-174, https://doi.org/10.1007/978-1-4899-7488-4_20.

[8] Beau Karlskin, "5 Reasons Why Palm Vein Scan Is the Best Biometric," Keyo, September 24, 2021, https://www.keyo.co/biometric-news/5-reasons-why-palm-vein-scan-is-the-best-biometric.

[9] GSMA, "Verifying Recipients of Cash Assistance Through Voice ID: Pilot Project Lessons and Outcomes," *GSMA*, August 17, 2021, https://www.gsma.com/mobilefordevelopment/resources/verifying-recipients-of-cash-assistance-through-voice-id-pilot-project-lessons-and-outcomes/.

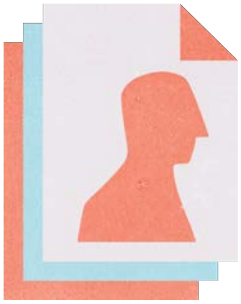
[10] UNICEF, "Faces, Fingerprints & Feet."

identity record (names, places of origin or birth, parents' names, nationality, etc) nor does its presence in a document automatically render it proof of legal identity.

For processes of authentication, on the other hand, biometrics are viewed as more reliable and secure when compared to many other forms of data, such as passwords and tokens (e.g. physical objects such as keys and cards), as they are directly linked to a person.[11]

How are biometrics currently used?

In terms of current uses, biometrics-based identification systems can be roughly divided into two categories: foundational systems and functional systems.[12]



Foundational systems comprise general or multipurpose identification systems, such as national IDs, and national population registers.[13] They are also referred to as official or legal identity systems (although some types of functional systems can also work as legal identification proof). Within the humanitarian sector, UNHCR is the only organisation with a legal mandate to provide displaced and stateless people with foundational IDs.[14]

Functional systems refer to systems designed to address a specific demand or sectoral use cases, such as voter IDs, driving licences, health registers and financial services registers.[15] Most use cases in the humanitarian sector fall within this category, since beneficiary registers are used to organise aid and service delivery at large.

[11] Greg Cannon, Philip Statham, and Asahiko Yamada, “Biometric Security, Standardization,” in *Encyclopedia of Biometrics,* eds. Stan Z. Li and Anil Jain (Boston: Springer, 2009), 122-129, https://doi.org/10.1007/978-0-387-73003-5_230.

[12] Alan Gelb and Julia Clark, “Identification for Development: The Biometrics Revolution,” *Center for Global Development,* CGD Working paper 315, (January 2013): 1-66, https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf.

[13] “Types of ID Systems,” World Bank, October 2019, https://id4d.worldbank.org/guide/types-id-systems.

[14] UNHCR, “Note on the Mandate of the High Commissioner for Refugees and His Office,” *UNHCR*, October 2013, https://www.unhcr.org/uk/protection/basic/526a22cb6/mandate-high-commissioner-refugees-office.html.

[15] “Types of ID Systems.”

These systems are usually used for two authentication-related purposes within humanitarian work: verification (one-to-one) or identification (one to many).

- **Biometrics for verification** (one-to-one authentication) involves using biometrics to verify if a person is who they say they are. It is also known as one-to-one authentication, as it checks live biometric data from an individual against a biometric record to determine if they are who they claim to be. Biometrics for verification is used by organisations to ensure that service delivery (e.g. cash assistance, food, healthcare and medicine, etc.) is being accurately distributed and reaching the intended recipients, which in turn is intended to prevent both fraudulent claims and wasting of resources. The increased prioritisation of cash-based assistance over in-kind (ie. food, shelter, clothing, etc.) in the past decade supports increased demands for accuracy in verification, as a tool to monitor and account for every resource spent by organisations and donors[16] (read more in "Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023)," Section 2: State of Play).

- **Biometrics for identification** (one to many authentication) is used to identify an individual with an identity in a database, i.e. to answer the "who are you" question. Known as one-to-many, in these systems an individual's biometric data is compared against a database of biometric profiles, serving to assert an individual's unique identity. Beneficiary registers (ie. databases containing all the biographical information collected by humanitarian agencies for registration and service delivery purposes) often allow for this type of authentication.

One-to-many schemes raise more concerns in terms of accuracy and data protection than one-to-one schemes, as one-to-many systems require databases with many people's biometric data, and generally have higher error rates.[17]

[16] The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector," *The Engine Room*, March 2018, https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf.

[17] Amba Kak, ed., "Regulating Biometrics: Global Approaches and Urgent Questions," *AI Now Institute*, September 1, 2020, 31, https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions.

Biometric templates

Biometric information is acquired using a capture device that takes an initial recording of a biometric trait such as a fingerprint. Key aspects of the biometric sample are then extracted from this raw image and turned into a biometric template. This template is a “mathematical representation of features or characteristics from the source data.”[18]

For instance, fingerprints are captured by a fingerprint device such as an optical scanner, that notes the particular ridges and valleys across a fingerprint. The machine notes important points such as where ridges and valleys end or meet. This is called minutiae.[19] These minutiae form the biometric template which is then stored and compared with a biometric input for identification, with a match decided based on a probabilistic threshold.[20]

Different biometric traits have varying salient data points, and so the way information is extracted changes based on the biometric input.[21] Regardless of the biometric feature being recorded, most systems turn the raw biometric image into a template that summarises these key markers.

What makes biometrics unique?

As explained in our previous report,[22] certain attributes of biometric data mean it is an especially sensitive type of personally identifying information (PII), which warrants specific considerations before being deployed by humanitarian organisations.

- **Uniqueness and immutability** – unlike other types of personal data, such as names or addresses, most forms of biometric data are immutable (i.e. cannot be changed) and are uniquely related to the individual in question. These qualities of biometric data make biometric

[18] Tyler Choi, “Biometric Template Explainer,” Biometric Update, May 9, 2022, https://www.biometricupdate.com/202205/biometric-template-explainer#:~:text=A%20biometric%20template%20is%20a,a%20database%20as%20reference%20data.

[19] R. Manjula Devi, et al., “Retina biometrics for personal authentication,” in *Machine Learning for Biometrics* eds, Partha Pratim Sarangi, et al., (Academic Press, 2022), 87-104, https://doi.org/10.1016/B978-0-323-85209-8.00005-5.

[20] Vincent Graf Narbel and Justinas Sukaitis, “Biometrics in Humanitarian Action: A Delicate Balance,” *Humanitarian Law & Policy Blog*, September 2, 2021, https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/.

[21] Justinus Sukaitis, “Building a path towards responsible use of biometrics,” (Master’s Thesis, EPFL, 2021), https://infoscience.epfl.ch/record/285077?ln=en.

[22] The Engine Room and Oxfam, “Biometrics in the Humanitarian Sector.”

systems a particularly effective and convenient tool in support of authentication processes. However, as technologies for the remote tracking of biometric traits mature, and techniques for mining and linking sensory and demographic data evolve, the collection of this data raises important concerns over privacy and consent.[23] Indeed, the same characteristics that make biometric data effective mean that once collected and processed, a person's biometrics may be used to track them over time.

Improvements in data protection have helped to counter the reusability of biometric data. For example, biometric templates that convert raw biometric data into mathematical files can reduce reversibility, or the ability to glean information about the original biometric sample from the simplified template.[24] Though this does not protect against all repurposing possibilities – nor does it alter the unchangeable nature of many personal biometric features – it highlights the potential of adopting these systems in more privacy-respecting ways.

- **Richness of information.** Depending on the modality, biometric data can convey more information about a person than was intended for in the original purpose for its capture. This is obvious in the case of DNA, for example, which can convey a vast amount of information about an individual (from health information to family ties), but it is also the case with palm prints, from which one can infer a specific condition, such as Down Syndrome. In this sense, biometric data collection may provide much more information than the original purpose envisioned, and therefore the consequences of its misuse, abuse, loss, or theft can be greater than other forms of personal data.

- **Flexibility of use.** While in one context, biometric data may be used to support aid distribution, in other contexts it may be used for monitoring and surveillance purposes, especially of historically oppressed and marginalised populations, such as refugees, migrants and other minoritised groups. In this sense, collection of biometric data from vulnerable populations generates highly sensitive, highly sought-after information which can be targeted by actors who do not have the best interests of these populations as a goal. There are many actors exploring

[23] Jain and Kumar, "Biometric Recognition: An Overview."
[24] See more: Sukaitis, "Building a path towards responsible use of biometrics."

ways to mitigate these possibilities via technological means – by, for example, collecting and storing data in a way that reduces its ability to be reused.

Anticipated benefits and potential risks of biometric systems

Benefits of biometrics

The adoption of biometric technology is driven, in part, by a desire to realise the benefits that the technology touts. These potential benefits include providing identification for people without IDs, improving the process of aid distribution due to greater registration efficiency; traceability, de-duplication and fraud control; and use as an anti-corruption tool.

Providing identification for people without IDs

The World Bank estimates that one billion people around the world lack proof of identity.[25] Humanitarian actors often work in contexts in which foundational identity systems – such as the kind of top-down general purpose identification systems[26] of civil registers and national IDs – are absent.

In the case of humanitarian emergencies, natural disasters and conflict often means that populations on the move lack identification documents, either because they did not exist in the first place, or because they were left behind or were damaged or destroyed in the move.

Nevertheless, IDs are frequently required for accessing general services and aid provided by humanitarian agencies and host countries; these services range from acquiring a SIM card to enrolling for cash assistance. Biometric systems are sometimes adopted by organisations to “bridge the gap between

[25] World Bank, “ID4D Data: Global Dataset,” *World Bank,* https://id4d.worldbank.org/global-dataset.
[26] Joseph J. Atick, et al., “Digital Identity Toolkit: A Guide For Stakeholders In Africa,” *World Bank,* June 11, 2014, https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/147961468203357928/digital-identity-toolkit-a-guide-for-stakeholders-in-africa.

unidentified beneficiaries and the assistance they are entitled to"[27] and "as a means of assigning an official identity to beneficiaries"[28] in ways deemed reliable and trustworthy. However, it is important to note that biometrics are neither a necessary nor a core part of legal identity. As such, identification for those without IDs can be provided via other means.

Improving the process of aid distribution

The increased use of biometrics takes place against a backdrop of resource constraints in the humanitarian sector,[29] with donors and organisations alike increasingly looking towards new and emerging technologies as potential tools for mitigating a growing funding gap.[30] Advocates envision biometric systems as tools to accelerate all aspects of aid distribution, from registration to aid disbursement, reducing accompanying personnel costs in the process. In parallel, they also argue that biometrics can improve operating efficiency by reducing the costs of duplication, fraud and corruption, and speed up the processes of registration and aid distribution.

Improved registration efficiency

Digital biometrics systems have been used to facilitate registration processes in place of paper-based systems in the context of development and humanitarian work.[31] Organisations have made numerous claims about gains made in the speed and efficiency of registration, aid distribution and aid delivery as a result of biometric databases.

When large influxes of people arrive at refugee camps, staff face immense pressure to register individuals as quickly as possible: many new arrivals have been on the move for extended periods of time and require urgent medical attention, food, water and shelter. As one interviewee put it: "That is where efficiency comes in: they need to do [registration] as fast as possible, to as many people as possible."[32] In this kind of case, where scale puts a lot of pressure on operating systems, biometrics may be a particularly

[27] The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector."
[28] The Engine Room and Oxfam.
[29] Mike Pearson, "2022 Forecasts: Year Ahead for Humanitarian Sectors: Humanitarian Funding Forecast," *Humanitarian Funding Forecast,* January 28, 2022, https://humanitarianfundingforecast.org/stories-2022-forecast/.
[30] Leonie Arendt-Cassetta, "From Digital Promise to Frontline Practice," *UN OCHA,* April 2021, 1, https://www.unocha.org/sites/unocha/files/OCHA%20Technology%20Report.pdf.
[31] Gelb and Clark, "Identification for Development: The Biometrics Revolution," 1.
[32] Interview with humanitarian policy expert at humanitarian organisation

effective solution,[33] helping to speed up verification and to avoid delays caused by incorrect information.

Some humanitarian practitioners argue that despite being resource-intensive during development and initial implementation, once running, biometrics-based systems require fewer resources (e.g. personnel).[34]

Traceability, de-duplication and fraud control

Biometrics are also promoted as a way to increase the accuracy of aid targeting and allocation by reliably accounting for need, de-duplicating registries, supporting traceability of funds, and reducing fraud in the aid distribution process.[35] In the case of cash-based assistance, for instance, biometrics-based verification works as an asset for ensuring funds are reaching the intended beneficiaries and that regular transfers are being made.

Advocates of biometrics argue that the technology can protect vulnerable individuals from being exploited. One interviewee cited the case of a community that used pin codes to access their cash-assistance cards stored in local shops. Local operators maintained a list of names and pin codes, and charged individuals a premium when they forgot or misplaced their code, resulting in aid being taken away from the intended recipients via inflated prices in their shopping transactions. As the interviewee explained: “For this, you don't need more info, you can have a phone number and biometrics. This is where I think the benefit is: ensuring that goods and services reach the people who they are supposed to reach.”[36]

Some available evidence suggests there are economic gains originating from the de-duplication of target population registries. In 2017, the IOM reported savings of USD 1 million just a month after the introduction of biometrics-based registration in South Sudan. The deduplication process led to a 45% decrease in the estimated population requiring aid.[37]

[33] Interview with humanitarian policy expert at humanitarian organisation
[34] Arendt-Cassetta, “From Digital Promise to Frontline Practice,” 19.
[35] World Food Programme, “Strategic Evaluation of WFP’s Use of Technology in Constrained Environments,” *WFP*, January 2022, 5, https://docs.wfp.org/api/documents/WFP-0000136278/download/.
[36] Interview with technical expert at non-profit
[37] Christin Roby, “Biometric registration aids conflict regions, but gaps still exist,” *Devex,* October 9, 2017, https://www.devex.com/news/biometric-registration-aids-conflict-regions-but-gaps-still-exist-91117.

Biometrics as an anti-corruption tool

While much of the discourse surrounding biometric technologies has focused on the reduction of fraud by potential beneficiaries, biometrics may also provide avenues for reducing opportunities for corruption by state and other officials.

Researchers have conceptualised biometric technologies as one of many tools of "e-governance"[38] that could limit opportunities for corruption. In practice, biometrics could reduce the extent of discretion and absenteeism of officials dispersing aid, in other words their ability to distribute aid unfairly or not show up to carry out their responsibilities.[39]

According to the U4 Anti-Corruption Resource Centre, when biometrics are used to register beneficiaries there are fewer opportunities for political abuse and clientelism, such as when local officials levy informal 'taxes' on aid.[40] The World Bank has also noted the importance of new ID technologies for reducing what it calls the 'leakage' – a euphemism for fraud and political abuse – of transfers and benefits payments.[41]

Highlighting the potential of biometrics to reduce corruption by officials can also reframe the discussion regarding fraud in the humanitarian sector, shifting the emphasis away from beneficiaries and towards governments and officials instead.[42] Such a reframing can help counter arguments that place the blame

[38] Jordan Gans-Morse et al., "Reducing Bureaucratic Corruption: Interdisciplinary Perspectives on What Works," *World Development* 105 (May 2018):171-188, https://doi.org/10.1016/j.worlddev.2017.12.015; Karthik Muralidharan, Paul Niehaus, and Sandip Sukhtankar, "Building State Capacity: Evidence from Biometric Smartcards in India," *American Economic Review* 106, no. 10 (January 2016):2895-2929, https://doi.org/10.1257/aer.20141346.

[39] Fredrick Mutungi et al., "Towards Digital Anti-Corruption Typology for Public Service Delivery," Proceedings of the 20th Annual International Conference on Digital Government Research, 2019, https://doi.org/10.1145/3325112.3325266.

[40] Inge Amundsen, "Covid-19, Cash Transfers, and Corruption," *Chr. Michelson - U4 Anti-Corruption Intitute,* 2020, https://www.researchgate.net/profile/Inge-Amundsen/publication/344189638_Covid-19_cash_transfers_and_corruption_Policy_guidance_for_donors/links/5f59f4d0299bf1d43cf9242b/Covid-19-cash-transfers-and-corruption-Policy-guidance-for-donors.pdf.

[41] World Bank, "Public ID4D Catalog of Technical Standards," *World Bank*, August 2022, 1, https://documents1.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf.

[42] Philip Kleinfeld and Paisley Dodds, "Corrupt Aid Workers Exploit Congo Crisis," *The New Humanitarian,* September 4, 2020, https://www.thenewhumanitarian.org/investigation/2020/06/12/Congo-aid-corruption-abuse-DFID-DRC-UN-NGOs.

for fraud solely on beneficiaries. One interviewee (a former official at a large humanitarian organisation) also pointed to the need to avoid locating inefficiencies and corruption only in local practices on the ground: "The bias in the international organisations, from the donors to the organisations, that somehow all these local systems are corrupt or worse than ours is a horrible assumption that is untested, and unsupported."[43]

Risks of biometrics

Given the particularities and level of sensitivity of biometric data, its use in humanitarian work brings significant challenges and risks. Some are related to the technical aspects of biometrics while others are related to contextual socio-political issues.

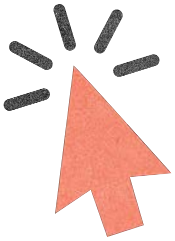
Technical risks

Risk of vendor lock-in can limit long-term options

Biometrics systems used in humanitarian contexts are usually implemented through partnerships with private sector companies that develop the technology (e.g. IrisGuard, Accenture, Thales Group, etc.). These systems and their features (e.g. template-generating algorithms) are often proprietary, and as such, belong to the companies.

Mitigation against the risks of private sector ownership brings its own challenges. Organisations can, for example, choose to store all their collected raw biometric data themselves, which would make it possible to reprocess the data (e.g. re-convert it into templates) in another system, should the organisation choose to change vendors. However, this creates a new set of risks and potential harms related to data security and potential access by hostile actors, as a database full of raw data if breached/taken over can be easily reused.

This strengthening of ties between private companies and humanitarian organisations also brings important ethical and technical questions. Vendors frequently utilise existing commercial software, which is then repurposed for humanitarian organisations. These tools are designed for commercial contexts,



[43] Interview with former official at large humanitarian organisation

which have differing threat models – and value systems – to humanitarian contexts, raising concerns about the appropriateness of protections or other assumptions that may be built into the tools. Further, the use of humanitarian datasets to develop private sector technology raises an ethical discussion on using the data of vulnerable populations to improve products that will then be sold on the private market. Use of incomplete technology, or developing technology in humanitarian contexts can be considered experimentation on vulnerable populations.[44]

Current technical limitations for data protection

There are currently no sufficient existing data protection techniques fully able to remove the potential risk of biometric data being accessed by hostile third-party actors who might take control of databases. Techniques that are available to protect other types of sensitive data (e.g. hashing for passwords)[45] are not yet fully developed for the protection of biometric data. This lack of protection is particularly concerning for biometric data stored in the form of templates – a unique sequence of characters generated to represent biometric data in place of raw images, as is currently used for fingerprints and iris scans. Sector-specific research has shown that biometric data samples can be in fact reconstructed by reverse engineering unprotected templates.[46]

Moreover, the resources currently available, such as the encryption of databases, are not sufficient to ensure adequate protection – the risk of data theft at the moment of decryption, for example, remains a challenge.[47]

Meaningfully addressing the risks outlined above comes with tradeoffs. For example, per their policy, ICRC restricts the storage of biometric data collected to tokens (e.g. ID cards) held by the user. Biometric data is only stored on the physical token, and no data is uploaded to a centralised

[44] Kristin Bergtora Sandvik, "Humanitarian Wearables: Digital Bodies, Experimentation and Ethics," in *Ethics of Medical Innovation, Experimentation, and Enhancement in Military and Humanitarian Contexts,* eds. Daniel Messelken and David Winkler (Springer Cham, 2020), 87-104, https://link.springer.com/chapter/10.1007/978-3-030-36319-2_6.

[45] Jamin Becker, "What Is Password Hashing (and How Does It Work)?," Make Tech Easier, August 25, 2014, https://www.maketecheasier.com/what-is-password-hashing/.

[46] Marta Gomez-Barrero and Javier Galbally, "Reversing the Irreversible: A Survey on Inverse Biometrics," *Computers & Security* 90 (2020): 101700, https://doi.org/10.1016/j.cose.2019.101700.

[47] Frank Hersey, "'You Cannot Trust a Vendor': Understanding Biometrics in the Humanitarian Sector," Biometric Update, October 4, 2021, https://www.biometricupdate.com/202110/you-cannot-trust-a-vendor-understanding-biometrics-in-the-humanitarian-sector.

database.[48] However, storing biometric data solely in a token compromises some functionalities that are core to the most advanced benefits of biometrics – for example, holding biometric data in databases is needed when implementing one-to-many identification processes. It is worth noting the ICRC is currently investing in the development of an open-source biometrics system designed to properly protect biometric templates – however this is not yet functional at the time of writing.[49]

High implementation and maintenance costs run the risk of systems running without full operational protections

Biometrics technologies can be expensive for providers to deploy,[50] and require staff training and technical support for implementation. Investment in secure deployment means investment in systems that require more resources, such as internet connectivity, often necessary for the operation of template-generating algorithms. In that regard, while efficiency and traceability gains related to the implementation of biometrics systems have been documented in the context of humanitarian action (read more in "Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023),", Section 4.1: Potential benefits), evidence on the cost of implementation relative to these gains is not available.

Additionally, the cost of protecting information against evolving threat scenarios requires ongoing investment. As it is, the full integration of data protection methods for non-biometric data is uneven in the humanitarian sector. This is in part due to a lack of resources for maintenance and upkeep of systems, as well as the cost of data privacy and protection measures. It is unlikely that, in this context and current apportioning of funds, the added costs of securely operating biometric systems will be provided. For the claimed benefits of biometrics to be realised, a fully functioning system is required. Biometric systems need ongoing maintenance in order to ensure protection against emergent threats. As such, the way we consider benefits should also be contextualised in light of what is required for benefits to accrue.

[48] "The ICRC Biometrics Policy," International Committee of the Red Cross, October 16, 2019, https://www.icrc.org/en/document/icrc-biometrics-policy.

[49] Interview with cyber security expert at humanitarian organisation

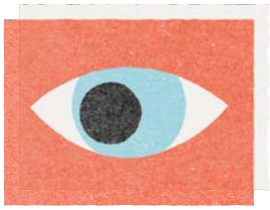
[50] VISA, "Assessing the Role of Biometrics in Advancing Financial Inclusion," *VISA,* 2019, 2, https://usa.visa.com/content/dam/VCOM/regional/na/us/about-visa/documents/assessing-the-role-of-biometrics-in-financial-inclusion-visa.pdf.

Contextual socio-political risks

While discussions around data governance broadly have matured, data governance in the humanitarian space has not kept apace. At large, data flows between organisations, donors[51], and national governments are opaque and inaccessible. Moreover in many contexts where humanitarian organisations operate there is a lack of robust national legislation regarding data protection.

Opaquely governed data sharing

One way humanitarian organisations can, and do at times try, to govern the flow of biometric data is through data sharing agreements. These agreements can be made between different humanitarian organisations, between humanitarian organisations and private companies, or between humanitarian organisations and host states (or in some cases other states). However, data-sharing agreements are often private and inscrutable to external actors such as civil society; they are also – by admission of humanitarian organisations themselves – particularly challenging to enforce.[52] Further, there are cases where data has been shared without data-sharing agreements first being entered into.[53]



In terms of the data sharing agreements themselves, opacity is common, and signatories tend not to make them publicly available – meaning agreements cannot be audited by those whose data is the subject of the document. Theoretically this information should be shared with individuals through the process of gaining informed consent, but in practice we have seen instances such as with the Rohingya in Bangladesh (read more in "Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023)," Case Study: Non-consensual data sharing of Rohingya refugees in Bangladesh) where information was shared with state actors without the prior knowledge or consent of the refugees. Without knowing what is covered by a data sharing agreement it is not possible to ascertain whether data is being properly protected, or know when it is being

[51] Larissa Fast, "Data Sharing between Humanitarian Organisations and Donors," *NCHS*, April 26, 2022, https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/.

[52] World Food Programme, "Strategic Evaluation of WFP's Use of Technology in Constrained Environments;"
Interview with members of a large humanitarian organisation; Interview with privacy expert at humanitarian organisation

[53] Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies," *Television & New Media* 20, no. 6 (February 2019): 581-599, https://doi.org/10.1177/1527476419857682.

shared in a manner that individuals have consented to. This lack of information prevents meaningful accountability.[54] As an example, requests by Human Rights Watch to see a copy of the data sharing agreement between UNHCR and the government of Bangladesh were declined: the UNHCR said it could not publish the agreement without the government's consent.[55]

Some organisations like the ICRC say they won't share data where it isn't "possible to effectively implement...guarantees,"[56] regarding how biometric data is processed. Given the highly charged nature of conflict environments, and the tense political situations that often accompany them, it is unclear how data sharing agreements can ever be written to fully anticipate rapid shifts in the political environment. The WFP, for example, admits that there is no evidence that data-sharing agreements properly account for such contingencies, making clear that even with the best intentions, effective implementation is limited at best.[57]

Data sharing agreements are not the only means of protecting shared information or preventing incorrect sharing of information. However they are an important part of understanding the intricacies of the humanitarian biometric data ecosystem, and one we currently do not have a full enough understanding of due to issues of opacity.

National data protection laws and their impacts remain uneven

It can be tempting, given the discussion of data agreements, to turn towards domestic laws. But these cannot guarantee proper handling of data. National data protection laws are often insufficient and there is a general absence of legal frameworks governing the protection of biometric data.[58] Poor enforcement and "dilute[d] privacy and data protection standards"[59] further imperil data collected in host countries, and reduce the access of individuals to their data rights. With most countries that humanitarian organisations operate in lacking basic data protection regulations, the onus to keep data protected falls to international organisations. As explored in our main report (read more in "Biometrics in the humanitarian sector: a current look at risks,

[54] Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies."
[55] "Un Shared Rohingya Data without Informed Consent," Human Rights Watch, June 15, 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent.
[56] "The ICRC Biometrics Policy."
[57] World Food Programme, "Strategic Evaluation of WFP's Use of Technology in Constrained Environments."
[58] Madianou, "The Biometric Assemblage."
[59] Sacha Robehmed, "The future of biometrics: Digital ID and Lebanon," *SMEX,* January 2021, https://smex.org/wp-content/uploads/2021/01/210121_SMEX_PI_ElectoralDigitalID_Draft5_EN.pdf.

benefits and organisational policies (July 2023)”), however, inadequate organisational policies within humanitarian organisations also could put biometric data at risk.

In some instances, countries have passed their own data protection laws based on the European Union’s General Data Protection Regulation (GDPR), which contain provisions around local storage of data collected within the country. For example, Turkey’s 2016 Personal Data Protection Law, which requires data collected in Turkey to be processed within Turkish territory, prevents humanitarian organisations from processing data collected on refugees in Turkey on their own organisational overseas servers.[60] Legislation such as this complicates data integrity and security practices that rely upon the use of servers in different geographies to protect data and ensure organisational control and oversight over information stored on them. These cases also highlight, again, the importance of humanitarian organisations adopting strong standards.

Conclusion

The unique nature of biometric technology presents the humanitarian sector with both the potential to bring more efficiency to their operations and significant risk of harm, especially for impacted communities. Within this context, each humanitarian organisation’s policies and practices as well as sector-wide standards or expectations are critical to shaping systems that are both effective and mitigate risk. However, as our report, “Biometrics in the humanitarian sector: a current look at risks, benefits and organisational policies (July 2023),” indicates, there is still much more to be done for organisations individually, and the sector as a whole, to adopt responsible policies and practices around biometric technology.

[60] Zoe H Robbin, “Jordan: Is the UN’s biometric registration for Syrian refugees a threat to their privacy?,” *Middle East Eye*, October 23, 2023, https://www.middleeasteye.net/news/jordan-syrian-refugees-un-biometrics-threat-data-privacy.