Biometrics in the Humanitarian Sector

A current look at risks, benefits and organisational policies

JULY 2023

THE ENGINE ROOM

This report is based on research conducted by The Engine Room, with support from Open Society Foundations, from March to October 2022. Additional fact-checking and a right to reply process was conducted January to July 2023.

Lead Researchers: Teresa Perosa and Quito Tsui (The Engine Room)

Research consultant: Samuel Singler, PhD

Research and writing: Quito Tsui and Teresa Perosa (The Engine Room), Samuel Singler

Project support: Becky Kazansky PhD, Laura Guzmán, Helen Kilbey, Cathy Richards, Olivia Johnson (The Engine Room), Alicja Peszkowska (consultant)

Editing: Niyousha Bastani PhD, Helen Kilbey and Laura Guzmán (The Engine Room)

Illustrations: Surasti Kaur Puri

Advisory committee: Aaron Martin (Maastricht University), Elizabeth Shaughnessy (Oxfam GB), James Eaton Lee (Simprints/Nethope), Matt Mahmoudi (Amnesty Tech), and Zara Rahman (researcher and independent consultant).

The content of this report does not reflect the official opinion of Open Society Foundations nor of advisory committee members. Responsibility for the information and views expressed lies with The Engine Room.

We want to thank all who joined our community calls to share their insights; the people who generously shared their experiences and ideas with us in interviews; and the reviewers who contributed their time and expertise to this report.

Suggested Citation: The Engine Room, Tsui, Q., Perosa, T., and Singler, S. (2023). Biometrics in the Humanitarian Sector.

THE
ENGINE
ROOM

CONTENTS

CONTENTS (CONT.)

EXECUTIVE SUMMARY

Millions of individuals depend upon humanitarian organisations for vital assistance. Across contexts from conflict zones to natural disasters, impacted individuals are increasingly accessing aid via biometric systems that seek to identify and verify recipients.

Though the use of biometrics systems within humanitarian programming has been on the rise for over a decade, detailed research on the benefits and risks of biometric systems has not kept pace with their uptake. Hopes around the positive impacts of biometric technology on humanitarian aid provision remain high, while evidence of risks and harm mounts.

In this report, we take a closer look at recent case studies and new evidence of harm to discuss the potential technical and political risks associated with biometric use. We examine organisational policies that govern the use of biometric systems to understand how humanitarian agencies are understanding and responding to these risks.

Overall, we find a sector that is slowly deepening its awareness of harm, but responding to the risks of biometric technology in fragmented ways.

This research takes place against the backdrop of increased and entrenched use of biometrics to assist with service delivery in the humanitarian sector. Since our scoping report in 2018, technological advances and wider uptake have led to the use of new forms of biometrics (e.g. voice recognition) in a wider set of contexts (e.g. restoring family links[01]). Our research suggests that humanitarian organisations have largely continued with business as usual, despite being confronted with new disclosures and confirmation of risks previously dismissed as speculative.

Key insights from our research

Risks and harms are not fully accounted for

The adoption of biometric technology continues to put data subjects at the greatest risk. Though organisations are also impacted by risks and harms, the sensitivity of biometric data means that impacted communities stand to bear the brunt of potential fallout associated with biometric systems.

There has been a move towards implementing technologies designed to mitigate the risks, but effective use of these technologies requires organisational policies that are sufficiently equipped to deal with the changing risks of biometric systems.

Additionally, the possibility of function creep – of biometric data being used to ascertain secondary information through linkage with other information, or the potential for political or contextual misuse from malicious actors – requires commitment to continuous risk assessments. Beyond weighing assessed risks and harms against likely benefits, realistic appraisals would need to address the risk of function creep as a problem of policy design that calls for ongoing revision and infrastructure updates.

Continued need for more evidence around benefits

Much of the motivation for the use of biometrics rests on claims that it will aid in de-duplication efforts, fraud control and anti-corruption,[02] with limited evidence demonstrating a clear, positive benefit in these areas. Both the proof of these claims and the sensibility of prioritising this set of benefits over risk of harm were queried in our 2018 report.[03]

[01] See more: "Restoring Family Links," International Committee of the Red Cross, July 28, 2014, https://www.icrc.org/en/what-we-do/restoring-family-links.

[02] See: ID4D, "A Primer on Biometrics for ID Systems," World Bank, https://documents1.worldbank.org/curated/en/099025009302216641/pdf/P17159207bc5150a308b380001fc5e8e0ff.pdf; "Biometrics," UNHCR, https://help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN_Final_April2022.pdf.

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

A nuanced weighing of realised benefits against actual costs and risks remains lacking.

Technical literacy among key decision makers remains a challenge

The initial choice to introduce biometric technologies[04] is one that requires technical literacy at key points, from programme officers at the field office level to policymakers at headquarters. Based on interviews with staff across various levels of seniority in humanitarian organisations, we found that non-technologists are making decisions about biometric technologies without the knowledge to empower them to do so safely and responsibly. Additionally, organisational policies are rarely translated down to practical guidelines. Without clear organisational practice, frontline staff operate in the absence of clear direction around the use of biometric systems, opening the door to additional risk.

Organisational policies lack coherence across the sector, and many do not properly account for the specifics of biometric technologies

Despite the increased uptake and use of biometric technologies, a lack of cross-sectoral policy standards persists. Policies specific to biometric technologies remain rare, even in the face of a growing body of evidence regarding the particular risks that biometric technology adoption raises. Additionally, through our interviews and research, we have not yet seen these policies address challenges in implementation. These gaps are compounded by the fact that technological innovations and best practices are ever evolving, requiring that policies be reviewed and continually updated.

Policy implementation is patchy

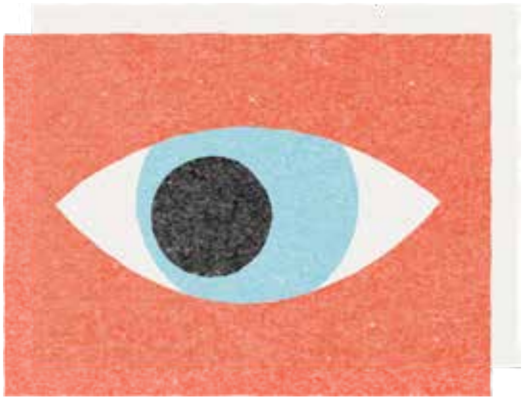
In the instance that organisations do have specific and extensive policies, there are challenges in their operationalisation. Specifically, frontline staff work under pressure and typically lack the required support and resources to implement policies. Upholding more responsible data protection policies may require more time, which can disincentivise the use of more secure practices. Similarly, at a headquarters-level, we also heard reports of responsible biometric data

[04] 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/.

practices being under-resourced, with staff lacking both financial resources and time to create or follow strong practices.

Minority world donors continue to encourage the use of biometric systems without providing adequate funding for safety measures

Larger humanitarian organisations, as well as influential government donors have – through funding requirements, investment and research – created an enabling environment for the use of biometric technologies. However, interviewees report that, for the most part, this push has not been accompanied by parallel investment in the infrastructure and resources required to support responsible use of biometrics.



DEFINITIONS

Minority world/global north; majority world/global south: These terms refer to what are commonly called “developed countries” and “developing countries”, distinctions mapped onto geographic divisions of wealth as well as racial and cultural groupings. The majority world refers to global south countries, where the majority of the world resides (e.g. countries in Africa, Asia, Central/South America and Oceania) and the minority world refers to the global north, which has a much smaller population in total (e.g. countries in Europe, Australia, USA, Canada, Japan). All of these terms have their flaws as dividing the world into a binary through broad characteristics is itself mired with problems; but in this report we use them to think through the lived realities of global economic and power divisions. In particular, we think this terminology reflects the current imbalances of political and economic power that are a result of the past injustices of colonialism and its ongoing legacies as well as current modes of neocolonialism, extraction and exploitation.[05]

Beneficiaries and impacted populations: Beneficiaries refer to those who utilise humanitarian services as they “benefit” from the aid. Impacted populations is a broader term which encompasses beneficiaries as well as all those affected by the policies and practices of humanitarian organisations. This term also mitigates the power hierarchy invoked by “beneficiaries” as a group that solely “benefits from” aid and humanitarian bodies as selfless “benefactors.” In this report, we think of impacted populations as those whose biometric data is

[05] Oxfam International, “Inclusive Language Guide,” March 2023, https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621487/tk-inclusive-language-guide-130323-en.pdf;jsessionid=96CE8EB0EAB5A1ADC6DB4C71C985C58A?sequence=4.

collected and stored by humanitarian organisations whether or not they directly receive aid or services.

Data subject: The individual whose identifying information (personal data) such as their name, contact details, ID number and/or biometrics has been collected, stored or shared by an entity.

Beneficiary registry: These are databases storing the biographical and biometric information of the beneficiaries of humanitarian organisations used for service delivery and record-keeping.

Cash and voucher assistance (CVA)/cash-based assistance: A form of humanitarian aid wherein cash or vouchers are provided to those impacted by natural disasters or displacement or who are in need of food assistance. Currently, these are largely electronic transfers via bank accounts or prepaid debit cards. As biometrics grow in popularity, they have been integrated into CVA programmes to verify the identities of individuals receiving the cash/vouchers.

In-kind assistance: In-kind assistance or aid is the provision of supplies or services (e.g. food, clothing, shelter) rather than monetary funding (e.g. cash).

DLTs and blockchain: Distributed ledger technology (DLT) is a decentralised database that allows for simultaneous shared access and updates across individual computers. It is commonly used for tracking transactions. Blockchain is the most popular type of DLT, and is used for tracking transactions and managing assets. Each individual transaction is recorded as a block of data (holding key details) and each block is then connected in a chain, as assets move from location or ownership in a time-stamped sequence. Blockchain technology is used for cryptocurrency, such as Bitcoin. DLT and blockchain have been held up as secure and transparent for their immutable (cannot be erased) record-keeping, de-duplication and decentralised nature. Blockchain has been used alongside biometrics in digital ID systems and for cash transfers.

Token: A physical (or digital) device such as an ID card or passport which is used to prove (authenticate) someone’s identity. This device can store personal information such as biometrics (images, fingerprints, etc) which can then be verified by a computer system or individual.

DPIAs: Data Protection Impact Assessments (DPIAs) are a process for identifying risks and minimising data protection concerns for a project. They are a required element in GDPR for any project that is “likely to involve ‘a high risk’ to other people’s personal information.”[06]

Informed consent: The practice of notifying potential data subjects of how their personal data (e.g. biometrics) will be used, retained and shared, with acknowledgement of the potential risks prior to collecting personal data. When individuals have a comprehensive understanding of how their data will be used they can consent (opt in) or choose to opt out. The ability to opt out without negative consequences or loss of aid is a key element of informed consent, since someone cannot consent to something that is not a real choice.

De-duplication: The act of removing redundant or repeated data from a database. Biometrics can be used as a tool to de-duplicate beneficiary registries, especially for cash based assistance.

Responsible Data: Responsible data is “a concept outlining our collective duty to prioritise and respond to the ethical, legal, social and privacy-related challenges that come from using data in new and different ways in advocacy and social change.”[07] Elements of responsible data include thinking about data privacy and data protection as well as ethical standards, power dynamics and bias.[08] In this report we use responsible data principles to analyse biometric data collection and governance frameworks.

[06] “Data Protection Impact Assessment (DPIA),” GDPR.EU, August 9, 2018, https://gdpr.eu/data-protection-impact-assessment-template/.

[07] “What Is Responsible Data?,” https://responsibledata.io/what-is-responsible-data/.

[08] Read more about responsible data: “Responsible Data Handbook,” The Engine Room, https://the-engine-room.github.io/responsible-data-handbook/.

THE ENGINE ROOM

1. INTRODUCTION

In 2021, the UN Office for the Coordination of Humanitarian Affairs (UNOCHA) projected that 274 million people would need humanitarian assistance of some form across the world in 2022.[09] In September 2022, this number surpassed the projection, reaching over 313 million people,[10] and is projected to continue increasing to around 339 million people in 2023.[11]

Causes for the increasing need are manifold: the Covid-19 pandemic's impact on increasing extreme poverty, the spread of misinformation and disinformation online fuelling political turmoil and conflict, in addition to wars, natural disasters, and border crises exacerbated by minority world nations' deadly asylum policies.[12] The ongoing climate emergency will continue to intersect with hostile borders, as the World Bank predicts between 50 to 200 million people will be on the move by 2050 due to climate related causes.[13]

Humanitarian organisations already grapple with tremendous challenges: working to provide aid and protection to populations in need, often under precarious conditions and with limited resources. As organisations seek to address existing issues and anticipate future de-

[09] "Global Humanitarian Overview 2022," UNOCHA, https://gho.unocha.org/.

[10] Global Humanitarian Overview 2022.

[11] Irwin Loy and Jessica Alexander, "Key takeaways from the UN's record-breaking tally for 2023 humanitarian needs," *The New Humanitarian*, December 1, 2022, https://www.thenewhumanitarian.org/news/2022/12/01/financing-appeals-OCHA-global-humanitarian-overview.

[12] "Ten Humanitarian Crises and Trends to Watch in 2022," *The New Humanitarian*, January 17, 2022, https://www.thenewhumanitarian.org/feature/2021/12/29/ten-humanitarian-crises-trends-to-watch.

[13] "Climate Change Could Force 216 Million People to Migrate Within Their Own Countries by 2050," World Bank, September 13, 2021, https://www.worldbank.org/en/news/press-release/2021/09/13/climate-change-could-force-216-million-people-to-migrate-within-their-own-countries-by-2050.

mand – particularly as available funding falls short of what's needed[14] – they have increasingly turned towards technological solutions, to varying degrees of success.[15]

Digital biometrics systems have become an increasingly normalised and central part of humanitarian infrastructures. They have been progressively integrated into humanitarian programming since the early 2000s: first in support of registration efforts, and now as a tool for aid distribution and CVA.

In 2018, The Engine Room partnered with Oxfam to better understand the impact, benefits and potential risks of deploying biometrics in humanitarian work. We published a landmark report[16] on the use of biometric data by humanitarian organisations: we queried some of the assumptions behind the promotion of biometrics in the sector (e.g. its actual ability to reduce fraud) and raised concerns about potential risks pertaining to the use of biometrics in fragile contexts.

We have also explored the topic of biometrics further in our work on digital identity,[17] where we consider the overlap and reliance of digital identity systems on biometric identification and verification.[18]

Now, five years after our first report was published, with the support of Open Society Foundations, we revisit the topic. In this report, we map out recent developments and the sector's policy responses to benefits, challenges, documented harms and potential risks of the use of biometrics for humanitarian purposes.

We focus on case studies that exemplify both the tension and utility introduced by these systems, and map current organisational frameworks that govern the adoption of these systems. With this research, we hope to support practitioners and decision-makers in the sector to make responsible and well-informed choices that account for the evidence of harm in more comprehensive ways.

[14] Loy and Alexander, "Key takeaways from the UN's record-breaking tally for 2023 humanitarian needs."

[15] Kristin Bergtora Sandvik et al., "Humanitarian Technology: A Critical Research Agenda," *International Review of the Red Cross* 96, no. 893 (2014): pp. 219-242, https://doi.org/10.1017/s1816383114000344.

[16] The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector."

[17] The Engine Room, "Understanding the Lived Effects of Digital ID," January 2020, https://digitalid.theengineroom.org/.

[18] The Engine Room, Quito Tsui and Teresa Perosa, "Digital Ids Rooted in Justice: lived experiences and civil society advocacy towards better systems," January 2022, https://www.theengineroom.org/wp-content/uploads/2022/01/Engine-Room-Digital-ID-2022.pdf.

1.1 Why revisit the use of biometrics now?

Since our first report was published, we have seen an increase in the use of biometrics and newly realised risks with neither a proportionate security/privacy policy response nor adequate documentation of benefits alongside the accounting of harms. The new developments, listed below, have fostered renewed debate on the topic.

- **Investment in biometric technology has increased**. Biometrics technology is advancing rapidly, with billions of dollars[19] being poured into the development of palm and vein recognition, heartbeat sensing, voice recognition, and gait recognition, among others. There are not just new forms of biometric recognition receiving funding – more commonly used forms of biometric information such as iris scans and fingerprint recognition are being refined through further investment. However, investment in humanitarian-specific biometric technologies still remains relatively small compared to investment in private sector technologies
- **There is a wider push for data governance design to better consider emerging risks, but emerging frameworks do not always consider biometrics specifically**. Data governance in the humanitarian space is evolving both in terms of available frameworks and practice. These developments are happening in the context of a changing regulatory environment, with the adoption of General Data Protection Regulation (GDPR) in Europe and GDPR-inspired legislation across the globe.[20] Despite this broader push for responsible and accountable data usage, specific approaches for how biometric information ought to be governed in the humanitarian sector remains scarce (see: Section 5 – Analysis of organisation policies).
- **The fear of non-consensual access to biometric information has been realised.** In 2021, in Bangladesh, biometric data collected in analogue form by the United Nations High Commissioner for Refugees (UNHCR) from Rohingya refugees was shared with the Myan-

[19] Ayang Macdonald, "Biometrics Investment Continues as Global Market Forecast to Surpass $84B by 2026: Biometric Update," Biometric Update, October 26, 2021, https://www.biometricupdate.com/202110/biometrics-investment-continues-as-global-market-forecast-to-surpass-84b-by-2026.

[20] Christopher Kuner, "The GDPR and International Organizations," *AJIL Unbound* 114 (January 2020): 15-19, https://doi.org/10.1017/aju.2019.78.

mar government – the same authority responsible for the violence that led to their displacement – by the Bangladeshi government without the data subjects' consent[21] (see p. 48, *Case: Non-consensual data sharing of Rohingya refugees in Bangladesh*). Reportedly, the UNHCR breached their own policy, failing to conduct a data impact assessment for its data handling.[22] In Afghanistan, following the withdrawal of US forces, the Taliban took charge of the biometric databases US forces behind, possibly endangering thousands of people.[23] [24]

- **Evidence that humanitarian organisations are the target of security attacks is growing**. Events such as the November 2021 hacking attack on the International Committee of the Red Cross (ICRC), which compromised the personal data of over 500,000 people,[25] and a data breach at the UN's Geneva offices[26] in August 2019 indicate the growing threat of cyberattacks. While there was no biometric data in the compromised databases, these events show that even actors with strong data protection policies and practices are vulnerable to breaches and attacks and confirm that humanitarian organisations are a target for malicious actors[27] and state-sponsored hacking.[28]

In light of these changing conditions, this research sought to understand how the humanitarian sector is currently engaging with biometric technologies.

[21] "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.

[22] Frank Hersey, "UNHCR Shared Rohingya Biometric Data 'without Consent," Biometric Update, June 16, 2021, http://biometricupdate.com/202106/unhcr-shared-rohingya-biometric-data-without-consent.

[23] Eileen Guo and Hikmat Noori, "This Is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban," *MIT Technology Review*, August 31, 2021, https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.

[24] "New Evidence That Biometric Data Systems Imperil Afghans," Human Rights Watch, March 30, 2022, https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.

[25] "Cyber-Attack on ICRC: What We Know," *International Committee of the Red Cross*, June 24, 2022, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[26] Ben Parker, "EXCLUSIVE: The Cyber Attack the UN Tried to Keep under Wraps," *The New Humanitarian*, January 29, 2020, https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

[27] "Comment: Red Cross Data Hack," *The New Humanitarian*, January 24, 2022, https://www.thenewhumanitarian.org/video/2022/1/24/comment-red-cross-data-hack.

[28] "From Cyber Attacks to Bot Farms: The Top Tech Threats Humanitarians Face in Ukraine," *The New Humanitarian*, March 9, 2022, https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms.

Our work was guided by the following key research questions:

- How is biometrics being used/deployed in the humanitarian sector and what are the current main use cases?
- How is biometric data gathered by humanitarian organisations governed (i.e. how is the data used, transferred, and shared? Who has access to it?)?
- What are the organisations' existing policies on biometrics use, and how are they applied in practice?
- What new evidence exists on the benefits of biometric data use in the context of humanitarian context?
- What new evidence exists on the risks and potential harms of using biometrics in the humanitarian context?
- What are the current regulatory frameworks in place that can support a more responsible use of biometrics in the humanitarian context?

1.2 Our standpoint

The Engine Room supports social justice movements to use technology and data in safe, responsible and strategic ways, while actively mitigating the vulnerabilities created by digital systems. We ground our research and analysis in a series of principles, concepts and frameworks relevant to both the theme and the context at hand.

In this work, our analytical perspective is grounded in core humanitarian principles, most notably the "do no harm" imperative for humanitarian action. This report is also informed by other core ethical principles of the sector, including the Sphere standards.[29]

We also draw inspiration from Aarathi Krishnan's concept of a reimagined humanitarian digital ethics and governance. Our analysis draws on Krishnan's notion of a foresight-based ethics that shifts "the focus of current humanitarian digital efforts that prioritise the problem solving

[29] "Sphere Annual Report 2020 (English Only)," Sphere, April 13, 2021, 36, https://www.spherestandards.org/resources/sphere-annual-report-2020/.

of now, to one that aims to mitigate future harm and inequity."[30] This framework advances the argument that organisations deploying technology need to assess "plausible, possible, and probable future harms and impacts that might arise on impacted populations and on their future generations."[31]

Sub-principles and guidance for implementation that also shape our discussion of biometrics include:

- **Understand protection risks in context**. This includes considering and mitigating unintended negative consequences of humanitarian activities; avoiding complicity in the violation of people's rights through "activities that give legitimacy to the policies and practices that cause the problem;"[32] and proactively reducing exposure to risks.
- **Support people's capacity to protect themselves**. This work includes providing alternatives to receiving assistance, with no negative consequences for doing so; obtaining informed consent with no negative consequences for "opting out"; and establishing feedback mechanisms.

Our analysis acknowledges that technological solutions broadly, and biometrics systems specifically, can serve meaningful purposes in humanitarian action and cannot all be dismissed as enablers of "surveillance humanitarianism".[33] As advanced by researchers Keren Weitzberg, Margie Cheesman, Aaron Martin and Emrys Schoemaker: "Components of data collection and identification are essential in delivering aid, and ... there are potential benefits to using digital technology for aid distribution – both for humanitarian institutions and recipients of aid."[34]

This report seeks to facilitate a nuanced discussion about when biometric technology is an appropriate tool for the humanitarian sector. Here, we rely on Linnet Taylor's data justice framework, which advances that fairness in the context of data is based on three pillars:

[30] Aarathi Krishnan, "Humanitarian Digital Ethics: A Foresight and Decolonial Governance Approach," The Carr Center for Human Rights - Harvard Kennedy School, January 20, 2022, https://carrcenter.hks.harvard.edu/publications/humanitarian-digital-ethics.

[31] Krishnan, "Humanitarian Digital Ethics: A Foresight and Decolonial Governance Approach."

[32] "Sphere Annual Report 2020," 39.

[33] Mark Latonero, "Stop Surveillance Humanitarianism," *The New York Times*, July 12, 2019, https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

[34] Keren Weitzberg et al., "Between Surveillance and Recognition: Rethinking Digital Identity in Aid," *Big Data & Society* 8, no. 1 (2021): 205395172110067, https://doi.org/10.1177/20539517211006744.

visibility (referring to both access to representation and the right to informational privacy), engagement with technology grounded on freedom and autonomy, and the ability to counter data-driven discrimination.[35]

Finally, given the immutable nature of biometric data – and how the technology is over-purposed by design, meaning its purpose cannot be limited to a specific use[36] – we approach our analysis of the technology through a wide lens, considering the ways its use in humanitarian contexts can, for example, have direct impacts in migration management.

This report is divided into six sections:

- Section 1 introduces the importance of revisiting biometric technology use in the humanitarian sector now and presents our position and methodology
- Section 2 gives background on the technology and what drives its adoption in the sector
- Section 3 explores what has changed, and what has not, since our report in 2018
- Section 4 presents new evidence on the risks and benefits of biometric technology
- Section 5 looks at the insights we gained from reviewing organisational policies about the challenges of developing and implementing frameworks for the use of biometric systems
- Section 6 takes a step back to consider what needs to change for more intentional and responsible use of biometric technology in humanitarian operations

For an introductory guide to biometrics see our Biometrics Primer. If you are unfamiliar with biometric technology, we recommend you read this first before continuing with this report.

[35] Linnet Taylor, "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally," *Big Data & Society* 4, no. 2 (2017): 1-14, https://doi.org/10.1177/2053951717736335.

[36] Narbel and Sukaitis, "Biometrics in Humanitarian Action: A Delicate Balance."

1.3 Methodology

The research for this project consisted of desk research, interviews and community calls conducted by The Engine Room.

Desk research

We conducted a non-exhaustive literature review between April and May 2022, capturing critical themes in the context of biometric systems use in humanitarian contexts. Our desk research focused on updating our general knowledge of biometrics in the humanitarian context; mapping out key developments since our 2018 report; assessing current state of the field (e.g. use cases, emerging modalities, state of the debate); collecting evidence on the actual beneficial impact of biometrics according to humanitarian organisations' aims and principles and on the risks/negative impacts of the use of biometrics in the humanitarian sector; and collecting policies on biometrics (and more broadly data protection and responsible data practices).

This first phase clarified key themes, guided the selection of the case studies, and allowed us to identify key individuals and organisations to interview.

Community calls

To kick off the project, we held a first community call in April 2022, bringing together humanitarian practitioners and researchers to discuss biometrics in the humanitarian sector through a justice-based and responsible data informed approach. The community call played an important role in helping us map key actors and emerging themes.

After the research was concluded, we held a second community call in October 2022 focused on workshopping our key questions raised in Section 6 (*What needs to change?*).

Interviews

Between May and September 2022, we conducted 21 semi-structured interviews with key stakeholders identified in the desk research phase as well as in the first community call. We spoke to people broadly falling into three groups:

- Representatives from humanitarian organisations who had first-hand experience of using biometrics in the humanitarian sector or who have worked on biometric data storage and management; or people who have been directly involved in internal-facing advocacy or policy design to shape how humanitarian organisations engage with biometrics.
- Researchers working on the intersection of humanitarianism and digital technology (including biometrics use in humanitarian spaces or in relation to forcibly displaced people).
- Other experts in the sector, such as consultants, advocates, funders and civil society activists who engage with the theme in their work.

In these interviews, we sought to understand issues related to drivers for biometrics use, value added by biometrics systems, key themes on programmatic design and the challenges of implementation, organisational data protection policies and practice, potential harms and accountability mechanisms.

The research team collaboratively coded interview transcriptions, and conducted a thematic analysis which led to the articulation of key themes explored in the report.

To protect the parties involved and to allow for frank participation, all interviewees were anonymised in this report.

2. BACKGROUND ON BIOMETRICS IN HUMANITARIAN AID

Digital biometric technology was first introduced in the humanitarian sector as a tool to support registration efforts during crises. Practitioners point to the Rwandan refugee crisis of 1994 as an inflection point in this regard,[37] as the sector grappled with the challenge of registering refugees in an efficient, ethical and dignified manner.[38]

Less than a decade later, following the US invasion of Afghanistan in 2001, the UNHCR adopted a biometrics-based system to manage the repatriation assistance aid given to Afghan refugees. Later, it was found that the system had significant design flaws which lead to exclusion, prompting a debate on ethics and experimentation with vulnerable populations in the sector.[39]

Biometrics use then progressed alongside changes in aid delivery (e.g. the rise of cash-based assistance in place of in-kind aid) and changes in humanitarian strategic goals such as the desire for increased efficiency and accountability to donors. Use of biometrics has expanded in parallel to an increased prioritisation of cash and voucher assistance (CVA). For many organisations, biometrics has become the preferred verification method. This stems in part from a “perceived need”[40]

[37] John Borton, “Twenty Years on: The Rwandan Genocide and the Evaluation of the Humanitarian Response,” *Humanitarian Practice Network*, February 14, 2022, https://odihpn.org/publication/twenty-years-on-the-rwandan-genocide-and-the-evaluation-of-the-humanitarian-response/.

[38] Interview with a former official at a large humanitarian organisation – Interviewee framed the Rwandan crisis as a “sector trauma.”

[39] Katja Lindskov Jacobsen, “Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees,” *Security Dialogue* 46, no. 2 (2015):144-164, https://doi.org/10.1177/0967010614552545.

[40] Kerrie Holloway, Reem Al Masri, and Afnan Abu Yahia, “Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises,” *ODI*, October 6, 2021, 14, https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/#:~:text=Biometrics%20have%20been%20used%20to,this%20technology%20 to%20 receive%20aid.

for more confident assurance over the recipient's identity than if the aid was provided in-kind (e.g. food and clothing parcels). The use of cash means donors and financial service providers are subject to international regulations such as know your customer (KYC), anti-money laundering, and anti-terrorist financing regulations.[41]

2.1 Adoption and advocacy by big players in the humanitarian sector

Various arms of the United Nations have advocated for the use of biometric technologies across a range of services. At the **UNHCR**, the **International Organization for Migration** (IOM) and the **World Food Programme** (WFP), staff have advocated for the ability of biometrics to make service provision more efficient, by speeding up registration processes and last-mile delivery, and more effective, by reducing duplicate registrations and identity theft. Biometrics has also played a key part in the rollout of digital identity systems[42] as part of a wider push for legal identity in the Sustainable Development Goals.[43] The UNHCR sees digital identity as a key aspect of its future work, suggesting that UN agencies will continue to collect biometric information.[44]

In some ways the United Nations, given its size and influence, sets the standard for how humanitarian work is conducted. As UN agencies have increased their own use of biometrics they have also actively encouraged other humanitarian agencies to follow suit. The WFP is another key driving force behind this work. Multiple interviewees told us that in several instances the WFP has explicitly made funding conditional on the use of SCOPE, the WFP's central repository for data on impacted communities (which often, not always, captures biometric data).

[41] Holloway, Al Masri, and Abu Yahia, "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises," 14.

[42] Holloway, Al Masri, and Abu Yahia, 14.

[43] "Home — UN Legal Identity Agenda," UN Stats, https://unstats.un.org/legal-identity-agenda/#:~:text=Sustainable%20Development%20Goal%20Target%2016.9.

[44] Karl Steinacker, "Beyond the Clip: Is Blockchain the Future of Humanitarian Aid?," *UNHCR Blog*, August 20, 2018, https://www.unhcr.org/blogs/beyond-the-clip-is-blockchain-the-future-of-humanitarian-aid/.

Major players: UNHCR and WFP

The WFP and UNHCR are the two largest humanitarian actors that use biometrics systems. The adoption of biometrics by these two agencies is one of the drivers for adoption at large in the sector. Through partnerships and advocacy, the WFP and UNHCR have encouraged other organisations such as Save the Children, CARE, Mercy Corps and Oxfam to integrate biometrics in their programming.

In November 2020, almost 63.8 million identities were registered in the WFP's SCOPE database.[45] The UNHCR's BIMS database at last count had 9.2 million biometrics profiles stored.[46]

Both SCOPE and BIMS allow the WFP and UNHCR respectively to manage and plan service delivery.[47] These databases are not only limited to organisational use — both BIMS and SCOPE are used by other NGOs for programmes in which the WFP or UNHCR acts as donor and/or partner.[48] [49] According to one interviewee, WFP aims to reach 80 million biometric records in the coming years.[50] Another interviewee also conveyed that the strategic vision of WFP is to become a centralised distribution database, with partner NGOs working on service delivery as partners:

> WFP's view of the future is that they are the Amazon of the humanitarian world and all NGOs are just Amazon Prime delivery drivers. That's their whole model and what they are striving for.[51]

[45] World Food Programme, "Internal Audit of SCOPE WFP's Digital Management of Beneficiaries," *WFP*, May 2021, https://docs.wfp.org/api/documents/WFP-0000128891/download/.

[46] "Global Report 2020," UNHCR, https://www.unhcr.org/flagship-reports/globalreport/.

[47] "WFP Scope - User Manual," WFP, https://usermanual.scope.wfp.org/cash-accounts/content/common_topics/introduction/1_introduction.htm?tocpath=_____1#.

[48] According to SCOPE's user manual, the platform allows WFP staff and implementing partners to: know beneficiaries; know what beneficiaries are entitled to; issue instructions to the appropriate partners who deliver the assistance (i.e. financial service providers or cooperating partners); analyse feedback on whether or not the right transfers have been distributed to the right beneficiaries; analyse data on transfer redemption by beneficiaries. More here: "WFP Scope - User Manual," WFP, https://usermanual.scope.wfp.org/cash-accounts/content/common_topics/introduction/1_introduction.htm?tocpath=_____1# .

[49] "Registration Tools – UNHCR – Guidance on Registration and Identity Management," UNHCR, https://www.unhcr.org/registration-guidance/chapter3/registration-tools/.

[50] Interview with digital rights practitioner at large humanitarian organisation

[51] Interview with digital rights practitioner at medium humanitarian organisation

This desire to centralise humanitarian action, along with the increasing reach of the SCOPE database, raises concerns around the security of data, the expansion of biometric based systems, the ability to meaningfully include local communities in the process of aid provision, and the relationships between different humanitarian organisations. This more stratified system – where larger organisations collect and store data, and medium or smaller organisations deliver services – could also complicate responsibility and accountability to impacted communities.

2.2 The role of donor pressure for increased efficiency and transparency

The functioning of the international humanitarian system relies primarily on multilateral funding from large government bodies, and interviewees pointed to donor priorities playing a large role in setting the approach that humanitarian organisations can take.

Extensive financial reporting expectations have resulted in pressure for organisations to verify the accuracy of their accounting.[52] This impetus stems in part from donor desire to maximise their contributions – an ask that is increasingly translated into demands for more efficient program delivery.[53] In recent years the level of insight into spending that donors desire, along with their insistence on efficiency, has made technological solutions (and their promises of verifiability and transparency) more appealing.

Many donors also want to audit projects after their completion, but some of those we interviewed told us that audits can take a long time – with some occurring up to ten years after the completion of the project. This pushes organisations to collect and retain sensitive biometric information far beyond the project life cycle.[54] Despite these

[52] Interview with former official at large humanitarian organisation

[53] Interview with digital rights practitioner at medium humanitarian organisation

[54] Interview with digital rights practitioner at large humanitarian organisation

requests, however, funders do not typically provide resources to properly support safe storage of this data.[55]

The Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) was flagged by interviewees as the exception,[56] having recently added mention of the necessity of data protection policies to its grant application process. ECHO also supports partners with assessment of risks related to data or technology-related programming.[57]

[55] Interview with security expert at non-profit

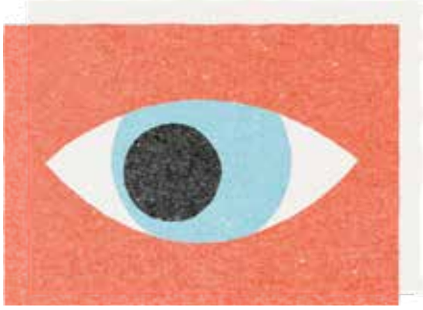
[56] Interview with security expert at non-profit

[57] Interview with policy officer at funding body

Case: Iris scans in refugee registration and private sector providers in Jordan

Iris scan technology use by humanitarian actors in Jordan exemplifies the growth of public-private partnerships as a result of the expansion of the biometrics sector and the increased digitisation brought about by COVID-19 (see next section). In Jordan the UNHCR uses biometric technology provided by IrisGuard, a private sector company, for refugee registration.[58]

Iris scan technology was introduced for the registration of Syrian refugees in camps in Jordan by UNHCR in 2013, as a tool to support de-duplication in registration and aid distribution, and as protection against identity theft and fraud.[59] Reliance on the technology grew from there. In 2016, the UN refugee agency rolled out a cash-based intervention with this system, using iris scans to give refugees access to their financial accounts.



Since then, the use of iris scans has become the main mode of verification for cash assistance, with numerous humanitarian organisations adopting it for their own payment schemes for impacted populations. WFP, for example, adopted the system in its aid programming for Syrian refugees, reaching over 100,000 refugees living in camps.[60]

More recently, WFP and others have started using iris scans in combination with blockchain and digital wallets to transfer payments, cutting out financial institutions entirely.[61] [62] In this context, blockchain is advanced as an innovative alternative that saves resources

[58] Nazih Osseiran, “In Jordan, Refugees Scan Irises to Collect Aid. But Is It Ethical?,” *Context News, December 13, 2022*, https://www.context.news/surveillance/in-jordan-refugees-scan-irises-to-collect-aid-but-is-it-ethical.

[59] Adam Vrankulj, “UNHCR Adopts IrisGuard Technology for Refugee Registration: Biometric Update,” Biometric Update, February 21, 2014, https://www.biometricupdate.com/201402/unhcr-adopts-irisguard-technology-for-refugee-registration.

[60] “World Leaders in Iris Recognition Services and Technology,” Iris Guard, https://www.irisguard.com/technology/case-studies/wfp-jordan/.

[61] “UN World Food Programme Uses Blockchain for Direct Payments,” Ledger Insights, December 24, 2020, https://www.ledgerinsights.com/un-world-food-programme-uses-blockchain-for-direct-payments/.

[62] Margie Cheesman, “Blockchain for Refugees,” *Medium* Data & Society: Points, June 9, 2022, https://points.datasociety.net/blockchain-for-refugees-a46b41594eee.

as transaction fees are eliminated.[63] It is also presented as particularly suited to contexts where financial institutions lack the capacity to process the volume of payments, such as in conflict zones.[64]

But civil society organisations such as Access Now have raised questions on the absence of meaningful informed consent processes for biometric data collection of refugees in the Jordanian context,[65] as well as IrisGuard's ties to national security agencies.[66]

Recent research on the experiences of women refugees with a cash-for-work program that relies on iris scans and blockchain to disburse payments in Jordan also showcased frictions, as the platform does not allow the women to see how much money is in their account at any given time, making it difficult for them to manage their finances.[67] Moreover, women have had their health concerns over the repeated use of iris scans dismissed and delegitimised by aid workers.[68]

Additional evidence from qualitative research shows that authentication via iris scans (tying financial management to a single member of the household) can take away some flexibility enjoyed by refugees using ATM cards – for instance by removing the ability of other family members to access cash in the event of ill health.[69] Despite these concerns, iris scans have remained the primary mode of verification for access to humanitarian services in Jordan.

[63] Russ Juskalian, "Inside the Jordan Refugee Camp That Runs on Blockchain," *MIT Technology Review*, April 2, 2020, https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

[64] "UN World Food Programme Uses Blockchain for Direct Payments."

[65] Alexia Skok, "Iris Scanning of Refugees Is Disproportionate and Dangerous - What's Happening behind IrisGuard's Closed Doors?," Access Now, May 5, 2021, https://www.accessnow.org/irisguard-refugees-jordan/.

[66] Christina zur Nedden and Ariana Dongus, "Tested on Millions of Involuntary People," *Die Zeit*, December 17, 2017, https://www.zeit.de/digital/datenschutz/2017-12/biometrie-fluechtlinge-cpams-iris-erkennung-zwang.

[67] Cheesman, "Blockchain for Refugees."

[68] Cheesman (2022).

[69] Holloway, Al Masri, and Abu Yahia, 19.

3. STATE OF PLAY

3.1 What has changed since our last report?

New evidence and discussion of harms caused by the use of biometric technology has not prompted large-scale change

Since 2018, studies examining use cases of biometrics and biometric-facilitated digital ID systems in Afghanistan,[70] Ethiopia,[71] Yemen,[72] and Myanmar[73] have evidenced risks previously dismissed as speculative.

These high-profile incidents demonstrate the wide range of harms that can accompany the use of biometrics in the humanitarian sector – from the non-consensual sharing of biometric information with hostile governments in the case of Myanmar (see p. 48, *Case: Non-consensual data sharing of Rohingya refugees in Bangladesh*), to disagreements over control of biometric information resulting in the suspension of aid distribution in parts of Yemen (see p. 54, *Case: WFP*

[70] Irwin Loy, Zara Rahman, and Ben Parker, "Biometric Aid Data and the Taliban," *The New Humanitarian*, September 2, 2021, https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban.

[71] Frank Hersey, "Biometrics in Africa: Digital ID for Humanitarian Responses in Ethiopia and Registration Priorities in Nigeria: Biometric Update," Biometric Update, April 19, 2022, https://www.biometricupdate.com/202001/biometrics-in-africa-digital-id-for-humanitarian-responses-in-ethiopia-and-registration-priorities-in-nigeria.

[72] Maria-Louise Clausen and Bruno Oliveira Martins, "Humanitarian Biometrics in Yemen," *NCHS*, September 8, 2021, https://www.humanitarianstudies.no/humanitarian-biometrics-in-yemen/.

[73] "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.

and Houthi standoff in Yemen), and the denial of citizenship rights for some Kenyan-Somalis double registered in refugee and citizenship databases (see p. 51, *Case: Double registration in Kenya*).

Whereas we previously emphasised the duty of humanitarians to identify and mitigate harm that could *potentially* arise from biometric technology, it has since become clear that the use of biometric systems has in fact given rise to new pathways of harm.

Despite these new developments, we found a clear and coordinated response from the humanitarian sector to be lacking. On one hand, there have been conversations connecting biometrics to histories of surveillance of and experimentation on people from the majority world.[74] These analyses have helped precipitate more concerted efforts to think critically about using biometric technologies.

Some interviewees indicated that a turn towards seriously considering the threat of “unknown unknowns” is taking place at the ICRC[75] and Oxfam, and others reported hearing hesitation around the use of biometrics being raised internally to humanitarian organisations within the past year.[76] However, organisations with more experience using biometrics have generally chosen to continue with large scale biometric programs without sector-wide (or publicly available) discussion or setting best practices around specific safeguards that should be put in place.

We also saw continued enthusiasm to accelerate use of biometric technologies – mirroring a trend toward techno-enthusiasm that we have seen across our work in the humanitarian sector.

As a sector, positive change around how organisations approach risk appears to be siloed: organisations clearly differ in terms of how risky they consider biometrics to be and, as a result, the solutions or understanding of responsible use diverge.

The biometrics sector has seen significant expansion and growth, with humanitarian use increasing

[74] 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.

[75] Narbel and Sukaitis.

[76] Interview with digital rights practitioner at medium humanitarian organisation

Since our last report was published in 2018, the number of vendors in the space has grown significantly. This is in part due to increased demand within the humanitarian space and beyond in the development, migration management and public services spaces, such as mobility management more broadly.

Key international funders like the World Bank, UN agencies and the Gates Foundation have all taken a keen interest in the possibilities of biometric technology, encouraging research, investment and uptake of biometric-based systems.[77]

However, supply has not merely followed demand; suppliers' advertising materials and lobbying efforts may have played a large role in drumming up interest and demand. Companies such as Thales Group[78] and Idemia have long been vocal proponents of biometric solutions for passports, ID cards, driver's licences and real-time facial recognition, while others have suggested biometrics could form a key node in service delivery in developing countries.[79] These companies have capitalised on the pandemic, promoting the use of biometric-based vaccine passports and health passes as solutions to the spread of disease.[80]

Public-private partnerships around biometric based technologies have proliferated

Private companies have also sought to align themselves specifically with the humanitarian sector, initiating partnerships with NGOs and international organisations (IOs).

- **Financial services**: Mastercard's Wellness Pass solution, in partnership with the Gavi vaccine alliance, integrates biometric identity verification with the vaccine records of children.[81]

[77] Interview with digital rights practitioner at medium sized humanitarian organisation

[78] "Identity & Biometric Solutions," Thales Group, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government.

[79] Ayang Macdonald, "UNDP, Consultant Highlight Role of Biometrics for Service Delivery in Developing Countries," Biometric Update, January 17, 2023, https://www.biometricupdate.com/202301/undp-consultant-highlight-role-of-biometrics-for-service-delivery-in-developing-countries.

[80] "Idemia Launches Health Travel Pass, Which Seeks to Help Governments Boost Border-Crossing Traveler Traffic," IDEMIA, December 4, 2021, https://www.idemia.com/press-release/idemia-launches-health-travel-pass-which-seeks-help-governments-boost-border-crossing-traveler-traffic-2021-04-12.

[81] Chris Burt, "Trust Stamp Integrating Biometric Hash Solution with MasterCard on Children's Vaccine Record System," Biometric Update, July 6, 2020, https://www.biometricupdate.com/202007/trust-stamp-integrating-biometric-hash-solution-with-mastercard-on-childrens-vaccine-record-system.

- **Information technology consulting**: Accenture has played a key role in the delivery of the UNHCR's biometric registration system.[82] Accenture has also been a keen supporter of biometric technology and digital identity for commercial purposes, collaborating on research with IOs such as the World Economic Forum.[83]
- **The role of tech companies**: Microsoft, along with other tech companies, have increasingly taken an active role in discussions around identity. Working with Accenture, Microsoft developed a digital ID system prototype that uses both blockchain and biometrics to register refugees residing in camps. Microsoft is also part of ID2020 – a high profile public-private digital ID initiative that positions itself as part of a "concerted push to provide digital ID to everyone."[84] ID2020 has support from Accenture, Microsoft, Visa, MasterCard, Mercy Corps, CARE, Kiva, and the Rockefeller Foundation among others.

Humanitarian organisations have also sought out partnerships with the private sector. Notably, the WFP has initiated several partnerships with private sector collaborators including Palantir, Alibaba, Tableau, NEC, GSMA, Google, Facebook, Ericsson, and the Cisco Foundation – a number of which have been criticised for their handling of data (Facebook), and the dubious ethical nature of their work (Palantir).[85] [86] [87]

Interviewees shared apprehension around the extent of private sector involvement in humanitarian use of biometrics, expressing concern over the mismatch of motivation between humanitarian organisations and profit-driven commercial organisations.

As private sector companies are not guided by humanitarian principles, this trend merits further investigation for potential risks and their mitigations.

[82] "UNHCR to Deploy Accenture Biometrics to Assist Refugees," *Biometric Technology Today* 2015, no. 6 (2015): 11, https://doi.org/10.1016/s0969-4765(15)30100-4.

[83] "The Known Traveller Digital Identity," Accenture, January 2018, https://www.accenture.com/_acnmedia/pdf-70/accenture-wef-the-known-traveller-digital-identity.pdf.

[84] "The Need for Good Digital ID is Universal," ID2020, https://id2020.org/digital-identity#approach.

[85] Ben Parker, "New Un Deal with Data Mining Firm Palantir Raises Protection Concerns," *The New Humanitarian*, April 16, 2019, https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

[86] Edward Ongweso Jr, "Palantir's CEO Finally Admits to Helping ICE Deport Undocumented Immigrants," *Vice*, January 24, 2020, https://www.vice.com/en/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants.

[87] Michael Posner, "How Palantir Falls Short of Responsible Corporate Conduct," *Forbes Magazine*, September 12, 2019, https://www.forbes.com/sites/michaelposner/2019/09/12/what-companies-can-learn-from-palantir/?sh=9b6946716e0d.

Digitisation has accelerated as a result of the Covid-19 pandemic

The Covid-19 pandemic accelerated digitisation across sectors, helped normalise the use of digitised services, generated a great deal of new data and technology platforms, and changed norms around the kinds of data individuals expect to have held on them.

In the humanitarian sector, social distancing and isolation exacerbated the challenges of humanitarian work, demanding organisations rethink their reliance on in-person interaction.[88] Moreover, disruptions to humanitarian supply chains have impeded the work of humanitarian organisations, inhibiting their ability to reach communities.[89]

In order to continue their work, many humanitarian organisations deepened their embrace of digital services.[90] Most of this new uptake of technology has focused on scaling up existing technology usage, including mobile phone apps and remote learning platforms for educational purposes[91] and social media platforms such as Whatsapp to convey information.

As humanitarian organisations have expanded their use of cash-based assistance, the use of mobile banking among refugees has also grown significantly.[92] To facilitate this shift in aid priorities, organisations have turned to biometrics for identification and verification. The Covid-19 pandemic has also driven interest in new forms of biometrics deployment, particularly for contactless modalities (e.g. palm biometrics, which can be done from a distance, and voice recognition)[93] that do not rely on tokens or passwords.[94]

[88] "Case Study: Responsible Data Sharing with Governments," CALP, March 2021, https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Responsible-Data-Sharing-with-Governments.pdf.

[89] John Bryant et al., "Bridging Humanitarian Digital Divides during Covid-19," *Humanitarian Policy Group*, November 2020, https://cdn.odi.org/media/documents/Bridging_humanitarian_digital_divides_during_Covid-19.pdf.

[90] 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.

[91] Alexey Lubkov, Oksana Gordienko, and Anastasiya Sokolova, "A Humanitarian Approach to the Digitization of Education," *Education and Self Development* 15, no. 3 (2020): 89-96.

[92] Jo Burton, "'Doing No Harm' in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action," International Review of the Red Cross, March 1, 2021, https://international-review.icrc.org/articles/doing-no-harm-digitalization-of-cash-humanitarian-action-913.

[93] Holloway, Al Masri, and Abu Yahia, 16.

[94] GSMA, "Landscape Report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations," May 23, 2017, https://www.gsma.com/mobilefordevelopment/resources/mobile-money-humanitarian-cash-transfers/.

Case: Cash-based assistance through voice recognition in Somaliland

In 2020, as the Covid-19 pandemic struck, CARE International faced challenges in delivering cash and voucher assistance (CVA) to communities in Somaliland.[95]

Before the pandemic, humanitarian workers travelled regularly to Somaliland to collect fingerprints and signatures for verification of cash disbursement.[96]

To avoid aid disruption, CARE worked with the Global System for Mobile Communications Association (GSMA) and the telecom provider Telesom to provide cash assistance with verification via phone-based voice recognition (funded by Telesom).[97] According to GSMA: "The process was designed to ensure the data flow was secure and responsible, with all sensitive data stored on Telesom's secure servers. All biometric data is linked only to cash programming with Telesom, and is not available for other use cases (as it is deleted at the end of the programme)."[98]

The system was piloted in 2020 with 2,000 people. According to GSMA's post-pilot assessment, most users were satisfied with the process, and CARE estimates that verification costs were halved. However, some struggled with the system, including elderly people and people with disabilities such as stutter, cleft palate, or deafness.[99]

Critical reflection on how verification cost savings should be considered in light of these accessibility issues is missing from the assessment. Next steps in the report did not consider the need to calculate the potential loss of aid for those with accessibility challenges, nor did it weigh up questions of accessibility against other benefits of using the voice-based biometric system.

[95] FSN Network, "Voice ID and Other COVID-19 Adaptations across East and Southern Africa," *Medium*, February 3, 2021, https://medium.com/fsn-network-blog/voice-id-for-cash-distribution-and-other-covid-19-adaptations-what-i-learned-from-a-virtual-trip-b58e33328fe4.

[96] GSMA, "Verifying Recipients of Cash Assistance Through Voice ID: Pilot Project Lessons and Outcomes," GSMA, August 17, 2021, 6, https://www.gsma.com/mobilefordevelopment/resources/verifying-recipients-of-cash-assistance-through-voice-id-pilot-project-lessons-and-outcomes/.

[97] GSMA, "Verifying Recipients of Cash Assistance Through Voice ID: Pilot Project Lessons and Outcomes."

[98] GSMA.

[99] GSMA.

Ideas around self-sovereign identities and data portability have gained traction as data-interoperability has gained importance

The desire to share data in a privacy-preserving manner has led to emerging research on self-sovereign identities and data portability. Earlier conversations and emphasis on the use of blockchain in humanitarian contexts[100] have evolved to centre on discussions around data sharing in particular.

Several of our interviewees highlighted recent efforts to refine blockchain use in part because of "promises around blockchain and specifically around the idea that blockchain and decentralised, cryptographic database systems can give the best of both worlds"[101] by allowing for both transparency of resource allocation and protection of individual identity. Meanwhile, tech startups and private sector actors have advocated for the ability of biometrics alongside DLTs to create truly self-sovereign identities (SSIs)[102] – a vision of a decentralised identity solution that gives individuals control over which parts of their identifying information are accessed.[103] Among humanitarian organisations, this idea has gained traction, with the UNHCR, ICRC, and the IOM all expressing interest in the potential of such an idea to empower refugees.[104]

Recent discussions around data portability[105] facilitated by digital identity raise concerns over the protection of sensitive biometric data in a more interoperable humanitarian datascape. The growth of CVA programming especially has highlighted the importance of secure sharing of usually biometric-based data. Though there is mixed enthusiasm in looking to SSIs and blockchain technology[106] to meet this need, there

[100] See for instance: DH Network, "Blockchain for the Humanitarian Sector: Future Opportunities," Relief Web, December 9, 2016, https://reliefweb.int/report/world/blockchain-humanitarian-sector-future-opportunities.

[101] Interview with Independent researcher on digital humanitarianism

[102] Gary Flood, "5 Large Ngos Looking at Using Digital Identity to Help Deliver Secure Payments," THINK Digital Partners, January 31, 2019, https://www.thinkdigitalpartners.com/news/2019/01/31/5-large-ngos-looking-using-digital-identity-help-deliver-secure-payments/.

[103] Margie Cheesman, "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity," *Geopolitics* 27, no. 1 (April 2020):134-159, https://doi.org/10.1080/14650045.2020.1823836; Fraser Edwards, "How digital identities could shape the future of humanitarian aid." Biometric Update, May 23, 2023, https://www.biometricupdate.com/202205/how-digital-identities-could-shape-the-future-of-humanitarian-aid.

[104] Cheesman, "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity," 134-159.

[105] Paul Currion, "Data Portability and Digital Identity in Humanitarian Aid: A Desk Review," *Collaborative Cash Delivery*, 2022, https://www.collaborativecash.org/_files/ugd/477045_e582d8bf08a74b1ab5891b3bc5389bb0.pdf.

[106] DH Network, "Blockchain for the Humanitarian Sector: Future Opportunities."

remains a sector-wide desire to develop "beneficiary-centric digital identity" to streamline benefit distribution. This approach moves away from the self-managed focus of SSIs though it can provide beneficiaries greater autonomy over their personal data.

Non-profit vendors and pilot projects based on humanitarian and responsible data principles have emerged

The past five years have seen the emergence of pilot initiatives on biometrics for humanitarian and development purposes that intentionally integrate a human-centred, responsible data approach.

- **ICRC** is currently investing in the development of an open-source (i.e. non-proprietary) biometrics system designed to properly protect biometric templates, considering the specific risks of humanitarian contexts.[107] [108]
- **Simprints**[109] works with implementers, amongst them government institutions and humanitarian organisations, to support cash-based assistance and health interventions through biometrics systems, advancing a privacy, transparency and human-centred approach.[110] In January 2023, Simprints published a handbook for the responsible deployment of biometrics in humanitarian and development settings.[111]

These initiatives stand out for their approaches, which centre the specific needs and challenges of the humanitarian context and hold the potential to advance a more considered and responsible use of biometrics in the sector.

Humanitarian actors have re-assessed data governance practices in a changing regulatory environment

[107] Interview with cyber security expert at humanitarian organisation

[108] Justinas Sukaitis, "Building a Path towards Responsible Use of Biometrics,'" Infoscience, April 15, 2021, https://infoscience.epfl.ch/record/285077.

[109] A member of this paper's advisory group was an employee at Simprints at the time of writing.

[110] "How We Work- Our Approach," Simprints Technology, https://www.simprints.com/impact.

[111] Simprints, "A Responsible Biometric Deployment Handbook," Simprints, January 2023, https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/64773ad0beced7dd5b6f6d69_A%20Responsible%20Biometric%20Deployment%20Handbook_Final%20(1).pdf.

Discussion and practice on data governance in the humanitarian space has evolved in the past five years, as the sector has grappled with challenges related to data management and governance.[112]

These developments have taken place within a rapidly changing regulatory environment, with the adoption of GDPR in Europe and GDPR-inspired legislation across the globe[113] prompting important discussions on data management in general, and accountability by data controllers and their handling of personal data specifically.[114] More recently, other regulatory initiatives such as the EU's (still pending) AI Act[115] show both political appetite for, and civil society engagement in, advancing regulation that ensures fairness and ethical standards in the deployment of technology.

In response to these changes, humanitarian organisations have re-assessed their data protection policies – notable examples of responsible data-oriented frameworks include ICRC's 2020 Handbook on Data Protection[116] and UN OCHA's 2021 Data Responsibility Guidelines.[117] Organisations such as the ICRC and Oxfam have also developed biometric-specific data protection policies that are specifically focused on the challenges of introducing the technology in the humanitarian space (see p. 59, *5.2 Organisation policy matrix*).

New mechanisms for assessing risk have been introduced but continue to need strengthening

When we last examined the risks of biometric use in the sector, the GDPR had not yet come into force and a coherent approach to risk assessment was lacking. Since then, the GDPR has brought much needed conversations and practices to the fore. However, in inter-

[112] Sarah Telford, "Data Responsibility in Humanitarian Action: Building Trust through Dialogue," OCHA, March 16, 2019, https://www.unocha.org/story/data-responsibility-humanitarian-action-building-trust-through-dialogue.

[113] "Data Protection and Privacy Legislation Worldwide," UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide; Jonathan Keane, "From California to Brazil: Europe's Privacy Laws Have Created a Recipe for the World", *CNBC*, April 8, 2021, https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html.

[114] Christopher Kuner, "The GDPR and International Organizations," *AJIL Unbound* 114 (2020):15-19, https://doi.org/10.1017/aju.2019.78.

[115] Daniel Leufer, "The EU AI Act Proposal: A Timeline," Access Now, July 14, 2022, https://www.accessnow.org/the-eu-ai-act-proposal-a-timeline/.

[116] "Handbook on Data Protection in Humanitarian Action," International Committee of the Red Cross, June 28, 2022, https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

[117] "Data Responsibility," The Centre for Humanitarian Data, https://centre.humdata.org/data-responsibility/.

views, practitioners still described key issues with DPIAs, which impedes their reliability and effectiveness.[118] The findings throughout this section may not apply to each and every humanitarian organisation; however, the trends around DPIAs that emerged in our research merit detailing here.

First, DPIAs tend to either lack the depth necessary to properly assess the conditions of biometrics use or, where they *do* capture more detail, to encounter new issues around technical literacy, both for those filling out the DPIA and those meant to assess them.

Decentralised systems place responsibility for enacting DPIAs, or applying tool guidance, in the hands of programme officers who are frequently insufficiently equipped with the necessary technical literacy and resources.[119] Given that DPIAs are highly technical documents, this lack of institutional capacity currently limits the extent to which they can be effectively used. There is a risk that DPIAs will merely become procedural – a piece of paperwork that is routinely filled out without meaningfully influencing or shaping the rollout of technological operations.

Additionally, for DPIAs to function properly, they must be refocused to centre those who bear the brunt of the risk. Interviewees shared that currently DPIAs are often focused on reputational risks for relevant organisations rather than risks posed to impacted communities. One interviewee described a sector in which “everyone is worried about the reputational risk of having a system go bad, no one wants to be the donor whose system was used by law enforcement to hunt people down.”[120]

However the same interviewee also described a tendency among organisations to take an approach to privacy assessments that generalises benefits and risks without noting which stakeholder will actually enjoy the benefits and which will bear the brunt of the risks.[121] Making sure DPIAs centre those who carry most of the risk would push decision-makers to make clear choices on the basis of whose benefits ultimately matter most.

[118] Interviews with members of a large humanitarian organisation and Interview with researcher on digital human rights

[119] Interview with researcher on digital human rights

[120] Interview with digitisation and data expert at development consultancy

[121] Interview with digitisation and data expert at development consultancy

Minority world donors are funding the securitisation of migration

Since our last report, minority world governments have ramped up their efforts to prevent the entry of asylum seekers and refugees. A growing migration-humanitarian nexus has looked to manage this hostility. This means that patterns of behaviour and trends in technology use in migration settings are increasingly relevant to the humanitarian sector.

The growing overlap between the two parallel sectors renders the biometric data of people on the move even more sensitive than before, and adds a layer of complexity for humanitarian organisations engaged in data exchanges with national authorities who enforce asylum and migration systems.[122]

Minority world governments are using biometric systems not only as technologies to manage migration, but also (specifically when it comes to the US and Europe[123] [124]) to externalise their borders.[125] By incentivising biometric registration in transit countries in both the minority and majority world,[126] minority world states are building a surveillance network that facilitates deportations and prevents the movement of people deemed illegal.[127] [128]

The United States – an influential donor to international agencies – has, for instance, supported, through policy and resources, the use of biometrics both across the humanitarian sector and in migration control initiatives. Humanitarian organisations such as the UNHCR share biometric information of refugees being considered for resettlement in

[122] "The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change," Privacy International, October 15, 2021, https://privacyinternational.org/long-read/4651/eu-externalisation-migration-control-and-id-systems-heres-whats-happening-and-what

[123] Giacomo Zandonini, "Biometrics: The New Frontier of EU Migration Policy in Niger," *The New Humanitarian*, March 5, 2020, https://www.thenewhumanitarian.org/news-feature/2019/06/06/biometrics-new-frontier-eu-migration-policy-niger.

[124] "Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds," Privacy International, November 10, 2020, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

[125] "The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change."

[126] Zandonini, "Biometrics: The New Frontier of EU Migration Policy in Niger."

[127] "The EU, the Externalisation of Migration Control, and ID Systems."

[128] Katja Lindskov Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism," *International Review of the Red Cross*, February 1, 2022, https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916

the US as part of formal data sharing agreements.[129] This data is stored on servers belonging to the Department of Homeland Security and accessible to other federal agencies including national security agencies with a demonstrated interest in biometrics for counter-terrorism purposes.[130] Meanwhile, there is no requirement to notify the data subject of data transfer between different parts of the US government, leaving refugees little insight or agency to prevent the sharing of their personal data once given to humanitarian organisations supporting resettlement.[131]

Developments in migration management are often intertwined with the humanitarian sector. For instance, humanitarian visas and resettlement schemes explicitly link humanitarian institutions and migration management efforts, and create a data flow between the two sectors. The IOM in particular has supported the responsible use of biometrics[132] within migration management.

This confluence of interests necessitates important ethical discussions for humanitarian organisations, as nation states will continue to seek data of populations on the move to support their surveillance and border control measures.

[129] Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism." And written correspondence to The Engine Room as part of our fact-checking and right to reply process in July 2023.

[130] Jacobsen (2022).

[131] Jack Corrigan, "DHS Is Collecting Biometrics on Thousands of Refugees Who Will Never Enter the U.S.," Nextgov, April 13, 2021, https://www.nextgov.com/emerging-tech/2019/08/dhs-collecting-biometrics-thousands-refugees-who-will-never-enter-us/159310/.

[132] "IOM and Biometrics," IOM, November 2018, https://www.iom.int/sites/g/files/tmzbdl486/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf.

Case: IOM & biometrics – merging humanitarianism and border management

In recent years, the International Organization for Migration has become a very influential institutional actor in the field of biometric technologies for identity management.

Despite its primary focus on migration and border management, the IOM also highlights Humanitarian Border Management (HBM) as a key area of its expertise, indicating the overlap between humanitarian operations and migration management.[133] The organisation presents biometric technologies as crucial to HBM, for instance through humanitarian visa schemes.[134]

The IOM has developed and deployed a range of migration control tools that use biometric data. The Migration Information and Data Analysis System (MIDAS)[135] was created in 2009, and has since been followed by other tools such as the WFP's Biometrics Registration and Verification System (BRaVe), to support member states with humanitarian crises and pandemic response. In the Philippines, BRaVe was used as part of the country's Covid-19 Social Amelioration Program.[136] In South Sudan, BRaVe data was shared with WFP's SCOPE system to deliver humanitarian assistance.[137]

The case of the IOM demonstrates how the deployment of biometrics in the humanitarian sector is influenced by logics and practices originally developed in separate policy fields, such as border control and health management. The tools developed in those other contexts are then imported into the field of humanitarian action under the banner of technological development and interoperability.

[133] Florian G Forster, "International Organization for Migration (IOM) Identity Management and Biometrics," IOM, 2016, https://www.icao.int/Meetings/TRIP-Symposium-2016/Documents/Forster2.pdf.

[134] "IOM and Biometrics."

[135] "A Comprehensive and Affordable Border Management System," IOM, https://www.iom.int/sites/g/files/tmzbdl486/files/our_work/DMM/IBM/updated/midas-brochure18-v7-en_digital-2606.pdf.

[136] "IOM Strengthens Sap through Biometrics Equipment in Philippines," United Nations Philippines, September 7, 2020, https://philippines.un.org/en/89762-iom-strengthens-sap-through-biometrics-equipment.

[137] "IOM, WFP Conduct First Beneficiary Data Exchange in South Sudan," IOM, June 28, 2019, https://www.iom.int/news/iom-wfp-conduct-first-beneficiary-data-exchange-south-sudan.

However, it is worth highlighting and critically considering the original policy contexts in which biometric tools are developed, particularly when these contexts focus more on state security than on human rights and the wellbeing of people in need of assistance. Such considerations raise concerns regarding the suitability or desirability of importing these tools directly into the humanitarian sphere, which should be guided by a distinct set of humanitarian principles.

3.2 What hasn't changed since our last report?

Certain elements of the landscape appear the same as when we last investigated biometric use in humanitarian work. We highlight two areas where we anticipated more change – a continued lack of nuance and evidence in discussions of "benefits" of biometric technology, and a continued donor push despite clear evidence of risks.

Evidence deficit regarding the claimed benefits of biometric technologies

There remains a lack of evidence in support of the claimed benefits of biometric systems In particular, and the way benefits are considered and discussed has not changed substantially in the face of increased evidence of harm. Interviewees expressed concern about the lack of critical analysis regarding the use of biometrics.

As one interviewee put it, organisations must consider whether they can "do the project successfully without using biometrics." The interviewee explained that "[If] the answer is yes, then there is no Legitimate Interest." They argued that if biometric technology is seen as necessary "for specific reasons", then there needs to be "actual evidence" that it fulfils the function it is deemed necessary for.[138]

Discussions of benefits must be updated to account for potential harms, especially as recent cases of hostile actors gaining access to the biometric data of vulnerable groups – like the sharing of Rohing-

[138] Interview with Privacy expert at humanitarian organisation

ya people's biometric data (see pp. 8 - 17 *Section 1, Introduction*) – demonstrate how potential risks can be realised. Interviewees pointed to a lack of updated discussion around the cost-benefit analysis of biometrics systems.

Additionally, interviewees indicated that there was a continued lack of meaningful consultation with impacted communities, including around how these individuals understand benefits and whether this aligns with organisational perceptions. One security expert at non-profit described a situation in which "almost nobody gets transparency and accountability":

> How does your group, how does your population…feel about this collection activity? How will they feel in five years' time? Meaningfully including people, which again is a problem that's much bigger than biometrics.[139]

Though there are some smaller pockets of work happening around this, big players – both donors and humanitarian organisations - were not found to be particularly engaged or focused on this line of inquiry.

Donor emphasis on evidence-based programming

The push for increasing adoption of biometric technologies in humanitarian contexts is underpinned by a general turn toward 'evidence-based policymaking'[140] from the 1990s onward.[141] Biometrics are seen as a key part of enabling accurate data collection to provide a basis for evidence.

While there is clear utility for humanitarian actors to base their actions on evidence about what works and what does not – interventions that directly impact the lives of highly vulnerable individuals should be justified through empirical evidence[142] – the question of whether biometric technologies meaningfully contribute to measuring impact remains to be fully examined.

[139] Interview with security expert at non-profit

[140] Trisha Greenhalgh and Jill Russell, "Evidence-Based Policymaking: A Critique," *Perspectives in Biology and Medicine* 52, no. 2 (Spring 2009): 305, https://doi.org/10.1353/pbm.0.0085.

[141] Linda Courtenay Botterill, "The Promise and Challenge of Evidence-Based Policy making," in *Drought, Risk Management, and Policy*, eds. Linda Courtenay Botterill and Geoff Cockfield (Boca Raton: CRC Press, 2013), 139-150.

[142] Liesbet Heyse et al., eds, Humanitarian Crises, *Intervention and Security: A Framework for Evidence-Based Programming* (London: Routledge, 2015), https://www.routledge.com/Humanitarian-Crises-Intervention-and-Security-A-Framework-for-Evidence-Based/Heyse-Zwitter-Wittek-Herman/p/book/9781138236622.

Evidence-based decision-making tends to privilege easily measurable and analysable quantitative evidence over more nuanced and complex social evidence.[143] [144] In particular, an emphasis on quantified outcomes often comes at the expense of other, community- and people-focused[145] forms of evaluation (which may be more accurate and/or require fewer resources). As one interviewee, a former official from a larger humanitarian organisation, explained:

> I am not convinced that our targeting is any more effective through our algorithms and increasingly technical processes, [or that these processes] can do better than sitting down in a community meeting, because there are lots of nuances that cannot be captured in the algorithms.[146]

[143] Sally Engle Merry, *The Seductions of Quantification: Measuring Human Rights, Gender Violence, and Sex Trafficking* (Chicago: The University of Chicago Press, 2016), 4.

[144] Jerry Z. Muller, *The Tyranny of Metrics*, (Princeton: Princeton University Press, 2018), 6.

[145] John Bryant, " Digital tools deepen the power imbalance in aid. Here's how to fix that," *The New Humanitarian*, July 4, 2022, https://www.thenewhumanitarian.org/opinion/2022/07/04/Digital-tech-tools-deepen-the-power-imbalance-in-aid.

[146] Interview with former official at large humanitarian organisation

4. A CLOSER LOOK AT BENEFITS AND HARMS

In our research, we encountered several detailed cases of risks or harms becoming realised. At the same time, we did not see a congruent documentation of realised benefits, or an assessment of how risks and harms may reduce the value of perceived benefit. In the sections below, we dig into new evidence around both benefits and harms.

4.1 Potential benefits

Anticipated benefits associated with biometric systems have not changed significantly since 2018. Potential benefits include improving the process of aid distribution due to greater registration efficiency; traceability, de-duplication and fraud control; and as an anti-corruption tool. You can read more about these anticipated benefits in our Primer.

Additionally, advocates of using biometrics in overlapping migration and humanitarian contexts (among those we interviewed, and as cited in relevant literature) argue that issuing a means of legal identity to people on the move contributes to economic benefits both for organisations and for individuals on the move themselves.

This argument rests on two key premises: for individuals lacking ID or with a shared or unknown identity, biometric systems can allow them to access financial services, while for organisations delivering aid, a more efficient registration process and reliable verification and traceability can help cut operational costs caused by duplication and corruption.

Evidence of benefits

Perception of benefits is often based on evidence from outside the humanitarian sector

In our discussions with practitioners, ease of identification and verification were the most cited benefits, followed by de-duplication of data, efficiency gains and some limited discussion of financial inclusion benefits for impacted communities.

Most of the newly documented evidence of benefits that we encountered comes from outside the humanitarian sector.[147] Wider application and uptake of biometrics outside of the humanitarian sector provides examples of different ways these benefits may be realised. In particular, in some cases, health programming in the development sector demonstrated improved treatment outcomes for individuals tracked by biometric systems.

Significantly, only two of our interviewees pointed to evidence of the benefits of biometrics, and both gave examples focused on benefits recorded in the development sector. The majority of those we spoke with did not see new evidence of biometric benefits in the humanitarian sector, indeed several practitioners we spoke with called for "a cost/benefit evidence based analysis,"[148] with one interviewee suggesting that biometric systems should be measured against non-biometric based systems "so we can see the real benefits regarding the speed, regarding perception, [and] beneficiary preference."[149]

Providing more accurate identification for people whose primary identifiers might be shared or unknown

In contexts where many people have the same name, or where a person's name might be spelled in different ways or an exact date of birth is unknown,[150] biometric systems can offer more reliability as a unique identifier – one that is less susceptible to cultural context and human error.

The need for unique identifiers is especially pressing in the context of health-related humanitarian programming, for which it is essen-

[147] Finbarr Toesland, "African countries embracing biometrics, digital IDs," *UN Africa Renewal Magazine*, February 5, 2021, https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids.

[148] Interview with Independent researcher on digital humanitarianism

[149] Interview with cyber security expert at humanitarian organisation

[150] UNICEF, "Faces, Fingerprints & Feet," July 2022, https://data.unicef.org/resources/biometrics/.

tial that a given intervention reaches the right individual and the right amount of people. As one interviewee shared:

> [It is useful] if you're doing something like a vaccine intervention, where you rely on having a certain number of people vaccinated for your whole intervention to work at all. If you vaccinate ten people, but no one else, the action just doesn't matter for a population at all. The properties of biometric information enable humanitarian and health workers to know that 'I have reached 275,395 people, because the data tells me that'.[151]

Other health-related examples that came up in interviews included delivery of scarce resources (such as HIV treatments), ensuring patient tracking for treatment completion, and supporting the adherence to and continuity of care.[152] In this area, there is evidence of positive impact: findings from a tuberculosis treatment study in Uganda and a cholera vaccination trial in Vietnam[153] showed that patient tracking through biometrics was linked to better success rates in comparison to those not biometrically tracked.

These are important findings and highly positive outcomes. However, crucially these interventions are not evidence of benefits observed directly within the humanitarian sector and we still lack evidence of how benefits accrue within humanitarian contexts.

Humanitarian actors may not be as focused on gaining the same benefits from biometrics as development actors. For instance, in interviews, de-duplication and efficiency were most frequently cited as benefits, contrasting with the emphasis on patient care and medical process tracking in health programming.

Overall, the pace of biometric uptake has not been matched by more extensive evidence-gathering in the humanitarian sector. The evidence that is available suggests limited use and prompts us to review and reconsider the claims of biometrics benefits.

[151] Interview with security expert at non-profit

[152] Sarah Grieves and Siobhan Green, "Using Biometrics to Fight COVID-19," UK Aid, https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/61addcb00fc8459c6d6427ba_Using%20Biometrics%20to%20Fight%20COVID-19.pdf.

[153] Grieves and Green, "Using Biometrics to Fight COVID-19," 12.

Reviewing the claims of biometric benefits

- **Accurate data**: The perceived benefits of biometric data increasing data accuracy are not as clear cut as they might appear – semantic challenges, misspellings and incorrectly entered information continue to be common issues. Consequently, in pursuit of more accurate data, we saw a tendency on behalf of humanitarian organisations to collect both a greater volume and granularity of data on people receiving assistance (even without the introduction of biometric systems). This increased volume and granularity increases the potential risks associated with these datasets. Further, as one interviewee put it, the normalisation of biometrics and its embeddedness in multiple processes with regard to identity management and delivering assistance, increases the riskiness of holding this data.[154] In other words, holding more accurate data can mean holding data that has a higher risk of causing harm in the wrong hands.

- **Efficiency**: Biometrics systems are often proposed as a tool for speeding up cumbersome registration processes, which is especially relevant in contexts with overwhelming numbers of people to reach.[155] Evidence on this proposed benefit, however, is mixed. While efficiency gains can be found when switching from paper-based to digital biometrics processes, sometimes the disruptions caused by the introduction of biometric systems reduce the extent of these gains. For example, in Tanzania, intermittent network failures affected the registration system and led to “delays, disruption and cancellation” of food distribution, causing long queues.[156] Without the necessary infrastructure, organisations could struggle to access potential gains. Furthermore, net efficiency in terms of gains to registration process speed versus the additional time and resources required to implement a new biometrics system is yet to be comprehensively assessed. Furthermore, some measures of efficiency gain, such as money saved by the implementing humanitarian organisation, may not present the full picture. While they may capture financial efficiency gains for the implementer, they do not account for gains/losses or disruptions faced by aid beneficiaries or their communities.

[154] Interview with officials at large humanitarian organisations

[155] Katja Lindskov Jacobsen, “On Humanitarian Refugee Biometrics and New Forms of Intervention,” *Journal of Intervention and Statebuilding* 11, no. 4 (2017): 529-551, https://doi.org/10.1080/17502977.2017.1347856.

[156] Jacobsen, “On Humanitarian Refugee Biometrics and New Forms of Intervention,” 529-551.

- **Fraud control**: Evidence of substantial gains in terms of fraud control after the introduction of biometrics systems remains scarce (see p. 44, *4.2 Risks and potential harms of using biometrics*). Though there is available evidence discussing cost savings of biometric systems,[157] it is often limited in scope, and does not provide a comprehensive assessment or comparative analysis of savings versus implementation and upkeep costs. Arguments for using biometrics systems for fraud control still almost exclusively rely on claims that these systems increase the reliability of identification and authentication processes. However, as stated in our previous report, this argument focuses disproportionately on "downstream fraud" (i.e. that committed by beneficiaries) as opposed to "upstream fraud" (i.e. that committed along supply chains); in doing so, it burdens beneficiaries with the issue of accountability, when there are substantial problems with fraud elsewhere in the ecosystem.[158]

Realising the benefits of biometric systems requires that systems work properly in the first place. But the time, money and effort required to set up biometric systems, along with the technical challenges of operating in low-connectivity may hinder systems. For further discussion on the difficulty of implementing biometric systems, you can read more in our Primer about the high implementation and maintenance costs of biometric systems, and the risks of running them without full operational protections.

4.2 Risks and potential harms

Mapping the risks and potential harms of using biometrics is to some degree a speculative endeavour. However, since 2018 we have seen growing evidence of these risks, and the realisation of harms due to the use of biometric systems.

Biometric systems can be both the cause or the amplifier of risk and harm. Some of these risks are enduring: function creep, the current technical limitations of protecting data, and the limitations of informed consent are all evergreen risks associated with data sha-

[157] UNHCR, WFP, and Programme Alimentaire Mondial, "Joint Inspection of the Biometrics Identification System for Food Distribution in Kenya," WFP, August 2015, https://documents.wfp.org/stellent/groups/public/documents/reports/wfp277842.pdf.

[158] See: The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector," 8.

ring broadly. In these instances, the introduction of biometrics raises the potential harm level due to the sensitivity of the data. It can also make it harder to undo the damage of a risk being realised due to the ease with which biometric data can be reused. You can read more about these risks and potential harms in the Primer.

Evidence of technical risks

Our interviewees pointed to technical challenges and risks that span the entire life cycle of biometric systems.[159] Interviewees were most worried about the challenges of risk mitigation, followed by concerns about data security and harm to impacted communities. Surveillance and the misuse of data as well as the possibility of function creep were mentioned in more than half of our interviews. This points to clear technical concerns with the use of biometric systems.

Function creep

Function creep refers to the notion that from the moment biometric data is collected, it can always reveal "more about the person than is needed for the original intended purposes."[160] For example, if iris scans or vein patterns are collected for identification purposes, there is nothing that technically prevents a later use of this same data to obtain, for instance, health information on the individuals they collected the data from. ICRC frames this issue as biometrics being "over-purposed by nature."[161] Biometric data is highly reusable, making it difficult for implementers to limit the purpose of biometric information. Consequently, once biometric data is collected, one should assume there is an ever-present risk of it being used for purposes other than what was originally envisioned.

This characteristic not only enables those collecting data to obtain secondary information, but also increases the possibility of political misuses or abuses.[162] For example, ongoing research by Human Rights Watch indicates that biometric data collected in the context of the unified national ID in Iraq (an endeavour advanced and sponsored by minority world donors) has been made accessible to armed groups in the country that have targeted, tortured and killed civilians, including

[159] Interview with Privacy expert at humanitarian organisation, interview with Independent researcher on digital humanitarianism

[160] Narbel and Sukaitis.

[161] Narbel and Sukaitis.

[162] Cheesman (2020).

many protest organisers in the context of large-scale anti-corruption protests in the south and centre of the country in 2018 and 2019.[163] This illustrates possible ways in which biometric data can be misused should it fall into the wrong hands, and highlights that this risk should be taken seriously by humanitarian implementers given the rise in data residency requirements. As more states seek to place limits on storage location and accessibility of data, humanitarian organisations should be wary of the potential safety risks of collecting biometric data that states may later seek or claim access to.

Evidence of contextual socio-political risks

Potential harms of institutional contexts

Biometrics vendors argue that mitigation strategies through the establishment of standards, policies and governance mechanisms around privacy protections and data security can address concerns about the misuse of biometric information.[164] However, issues like opaque data sharing agreements between humanitarian agencies and host countries (see p. 15 of the Biometrics Primer, *Opaquely governed data sharing*), lack of data protection legislation in host countries, and the pervasive power asymmetries that exist between organisations and beneficiaries (see p. 47, *Limitations of informed consent*) can jeopardise the effectiveness of these mitigation strategies.

Organisational contexts can amplify technical harms – in particular, limited capacity to implement policies can reduce the extent to which biometric data is protected. There is a significant distance between policy and practice (see p. 86 Annex 1, *1.2 Organisational policy analysis*), with practice and implementation often falling short due to a lack of resources and knowledge among local offices. One interviewee, an IT consultant for the development sector, emphasised the extent to which organisational context is frequently the reason for implementation challenges:

> It is not a technology problem, it is a design and prioritisation and resource problem. The number of times when I have seen people say, 'Well our IT system is really great, but we download personally identifying information in excel spreadsheet and email

[163] Interview with researcher on digital human rights

[164] "Biometrics Must Get the Big Questions Right: Privacy, Consent and Function Creep," Thales Group, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometrics-questions.

> them out.' And half of those people are using Gmail accounts because their company can't afford to buy proper domain and antivirus software [...]. The status of the data protection work is absolutely atrocious – I cannot describe how horrible this security environment is. So adding biometrics into that terrifies me. Because I see over and over again the lack of funding and the lack of skills to understand how to use this stuff responsibly.[165]

These concerns are illustrative of the wider data handling environment that biometric data is being introduced into and the increased risk factor of organisational limitations in ensuring policies are properly implemented.

Limitations of informed consent

A bedrock of data sharing, informed consent – and clear understanding on behalf of participants as to how their information will be used – is the critical ethical practice underpinning the collection of biometric data. But the conditions under which data is collected, the inherent limitations of safety guarantees and the technical understanding required in order for informed consent to be given, undermine the extent to which it may be possible for impacted communities to meaningfully grant consent to organisations processing their data.[166]

Power differentials are also important to take into account in this context, as refugees generally have few realistic alternatives to relying on humanitarian organisations: they usually lack other means of providing for themselves, are restricted to purchasing goods within camps, and face hostility from host governments that often prevent them from working.[167] As a result, they lack the meaningful alternatives necessary to ensure consent is freely given.[168] The absence of options creates a coercive atmosphere, with many refugees agreeing to share their data for fear of having nowhere else to go.[169]

In one interview, employees of a large humanitarian organisation told us that when impacted individuals do not wish to be subject to bio-

[165] Interview with digitisation and data expert at development consultancy

[166] Paola Verhaert and Madeleine Maxwell, "Unpacking 'Informed Consent'," *The Engine Room*, November 27, 2019, https://www.theengineroom.org/unpacking-informed-consent/.

[167] Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies," 581-599.

[168] Irwin Loy, "'It's like the wild west': Data security in frontline aid," *The New Humanitarian*, February 28, 2022, https://www.thenewhumanitarian.org/interview/2022/02/28/data-security-in-frontline-aid.

[169] "UN Shared Rohingya Data Without Informed Consent."

metric data collection, aid officials focus on emphasising the utility of biometrics as compared to paper-based mechanisms. Interviewees noted that individual concerns were usually overcome by such explanations.[170] Crucially, interviewees did not explain whether impacted individuals had actually changed their minds, having had their worries successfully assuaged, or if they had acquiesced to biometric use.

Though it may be the case that biometrics is faster than other systems, emphasising this aspect in the face of concerns minimises room for actual discussion and reinforces the skewed nature of power in this context.[171] As this dynamic is an inescapable aspect of humanitarian contexts, scholars and practitioners have questioned the plausibility of any consent granted under such conditions. With such little transparency around data flows and third party data sharing, refugees lack both the knowledge and control necessary to have a meaningful say in how their biometric data is used.[172]

[170] Interview with members of a large humanitarian organisation

[171] Interview with researcher on digital technology

[172] Cheesman (2020), 138.

Case: Non-consensual data sharing of Rohingya refugees in Bangladesh

Rohingya refugees have long expressed concern over the registration and data collection efforts of humanitarian agencies.173 Improper data collection and risky data sharing by the UNHCR with the Bangladeshi government – who then nonconsensually passed this information on to the Myanmar government – have both strengthened these fears and underlined the fraught nature of consent in humanitarian contexts.

Historical experiences with Nationality Verification Cards (NVCs) in Myanmar, which were used to facilitate targeted attacks on the Rohingya population, have resulted in the community's deep mistrust of identity documents. Subsequent attempts to issue smart cards in Bangladeshi refugee camps such as Cox's Bazaar have been met with protest and resistance.[174] Many fear that identity documents will be used to facili-

[173] "Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps," *Radio Free Asia*, November 26, 2018, https://www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html/.

[174] Natalie Brinham, "'Genocide cards': Rohingya refugees on why they risked their lives to refuse ID cards," *Open Democracy*, October 21, 2018, https://www.opendemocracy.net/en/genocide-cards-why-rohingya-refugees-are-resisting-id-cards/.

tate forced or premature returns to Myanmar, or help pave the way for a more restricted citizenship status that may disempower the Rohingya population.[175] Disagreement over whether the identity cards should say “refugee” or “Rohingya” have only compounded these concerns.[176]

Nonetheless, most, if not all, of the 900,000 refugees who fled to Bangladesh have been enrolled in the UNHCR’s biometric system, and had their information processed through a joint verification exercise between the Bangladeshi Government and the UNHCR.[177] Iris scans, fingerprints and photographs were collected by the UNHCR as part of a process intended to preserve their right to voluntary return and furnish them with an individual identity document.

Biometric data in the form of thumbprints on paper documents were then shared by the Bangladeshi government with the Myanmar authorities as part of right to return efforts. Many refugees, however, did not know that this information would be shared by the Bangladeshi government with Myanmar authorities to potentially facilitate repatriation.

The UNHCR denied wrongdoing,[178] and shared (in direct correspondence with The Engine Room) that they undertook counselling in local languages and obtained signatures of consent following a double-confirmation process. However, interviews with refugees conducted by Human Rights Watch point to ineffective consent practices, including English-only scripts which only 3 of the 24 refugees interviewed could read.[179] Refugees reported that they were unaware their information would be shared for purposes other than receiving aid, and did not know it might be used to discern repatriation eligibility.[180] Reportedly, the UNHCR breached their own policy, failing to conduct a full data impact assessment of this data collection and sharing.[181]

[175] “Rohingya return to Myanmar: Confusion and fear in refugee camps,” *BBC*, November 15, 2018, https://www.bbc.co.uk/news/world-asia-46217505.

[176] Shafiur Rahman, “For Rohingya refugees, ID systems have brought coercion, violence and denial of ethnic identity,” *Advox*, February 18, 2020, https://advox.globalvoices.org/2020/02/18/for-rohingya-refugees-id-systems-have-brought-coercion-violence-and-denial-of-ethnic-identity/.

[177] “Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway,” UNHCR, July 6, 2018, https://www.unhcr.org/news/briefing-notes/joint-bangladesh-unhcr-verification-rohingya-refugees-gets-underway.

[178] “News comment: Statement on refugee registration and data collection in Bangladesh,” UNHCR, June 15, 2021, https://www.unhcr.org/uk/news/press/2021/6/60c85a7b4/news-comment-statement-refugee-registration-data-collection-bangladesh.html.

[179] “UN Shared Rohingya Data without Informed Consent.”

[180] “UN Shared Rohingya Data without Informed Consent.”

[181] Hersey, “UNHCR Shared Rohingya Biometric Data ‘without Consent.”

Lack of accountability mechanisms

Accessible accountability mechanisms to remedy problems within biometric systems are few. In instances where information is incorrectly recorded, or not recorded at all, for example, refugees can face complicated bureaucracies in attempting to correct such mistakes.[182] In a case in Kenya in which Kenyan citizens were registered as refugees while simultaneously being registered as citizens (see p. 51 *Case: Double registration in Kenya*), civil society organisations supporting those who had been double-registered noted how difficult it was for both impacted individuals and civil society organisations to contest the decision of a machine rather than a person.[183]

When it comes to accountability, international NGOs occupy a complex legal grey area, and the global nature of their work results in ambiguity regarding how they may be held responsible for wrongdoing. Large agencies such as the United Nations are covered by immunity — a measure intended to reduce the potential for coercion and influence, and to ensure independence — which weakens the ability to enforce accountability mechanisms around agencies' responsibilities to impacted communities, as has been documented elsewhere and was shared with us by some practitioners. Accountability is weakened further by the introduction of technologies that can misdirect attention to the technology itself, rather than an organisation's own practices.[184] For example, without clear mechanisms that are actively communicated to impacted communities, data protection policies are functionally unenforceable.[185]

[182] The Engine Room, "Understanding the Lived Effects of Digital ID," January 2020, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

[183] Interview with members of civil society organisation

[184] Interview with former official at large humanitarian organisation

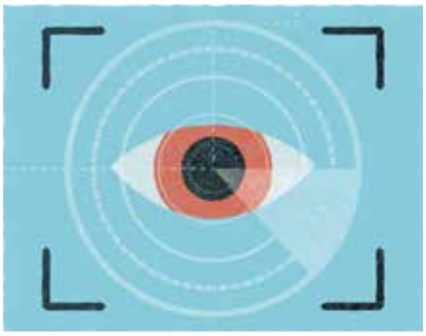
[185] Interview with former official at large humanitarian organisation

Case: Double registration in Kenya

Double registration of Somali Kenyan nationals exemplifies how using biometric systems can introduce the likelihood of unexpected future risks. In this case, the use of biometrics in humanitarian settings and sharing with national governments led to double registered Somali Kenyans losing their citizenship rights. The use of biometrics also meant redress was especially difficult; the binary nature of this technology reduced the ability of Somali Kenyans to contest their incorrect categorisation.

In the early 1990s, hundreds of thousands of Somali refugees fleeing the violence of civil war crossed the border into Kenya, the majority ending up in refugee camps such as Dadaab.[186] In the following decades, thousands more Somalis continued to seek refuge in the country as droughts had severe impacts on the whole region, including the northeastern part of Kenya, an area where historically marginalised and economically deprived communities live.[187]

In refugee camps, populations had access to food aid, education, medical services and other support; these services and opportunities were made available to refugees, but not to host communities, which were also severely impacted by the droughts.[188] In this context, many ethnic Somali Kenyan nationals sought out aid in refugee camps and ended up being registered as refugees in order to access aid.



UNHCR introduced biometric data into its refugee registration process in 2007, collecting biometric data from refugees and storing it in their own databases.[189] As the Kenyan government started to take over the refugee registration process in 2011, UNHCR shared its databases with the authorities, who integrated it with their own processes for registering persons and issuing national IDs.

[186] Haki na Sheria, "Biometric Purgatory," 2021, https://drive.google.com/file/d/1ziw6aEqHdAL5Ly7Ct51TA_CN-ZaX-XAp/view.

[187] "When ID leaves you without identity: the case of double registration in Kenya," Privacy International, December 20, 2021, https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya.

[188] Haki na Sheria, "Biometric Purgatory."

[189] Keren Weitzberg, "In Kenya, thousands left in limbo without ID cards," *Coda Story*, April 13, 2020, https://www.codastory.com/authoritarian-tech/kenya-biometrics-double-registration/

Since then, the Kenyan government has been able to run any person's fingerprints through its database; if the person is flagged as holding refugee status, they cannot have IDs issued.[190]

In Kenya, like in most countries, a national ID is required to access many necessities – the job market, education opportunities, welfare programs, financial services and more.[191] The estimated 40,000 Kenyan citizens registered in the refugee database – the majority of whom are below the age of 40, many having had their data captured when they were children[192] – have been rendered de facto stateless.[193]

Civil society organisations such as Haki na Sheria have been advocating for these individuals to have access to citizenship documents.[194] So far, around 14,000 people have had their rights restored, but no clear process for de-registration from the refugee database has been established. Moreover, virtually no mechanisms for redress were made available to these victims, from the Kenyan government or from UNHCR.

UNHCR notes, in correspondence with The Engine Room, that since the issue was identified, there have been several attempts to identify Kenyan nationals who were double registered, but that the agency ultimately views this issue as the responsibility of the Kenyan government. Though these efforts to address double registration can prevent the continuation of harm, they do not provide redress for the harms already inflicted. Neither the Kenyan government nor UNHCR have provided mechanisms for redress.

[190] Weitzberg, "In Kenya, thousands left in limbo without ID cards."

[191] Haki na Sheria, "Biometric Purgatory."

[192] Haki na Sheria, "Biometric Purgatory."

[193] "When ID leaves you without identity: the case of double registration in Kenya."

[194] Haki na Sheria.

Refusing to share information is challenging

Once data is collected, it is difficult for humanitarian organisations to refuse sharing it with host governments – especially when biometric information may be required to access services in countries of asylum.[195] Humanitarian organisations are reliant on the host country

[195] Katja Lindskov Jacobsen. *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity.* (London: Routledge, 2015).

to conduct their operations and are vulnerable to this dependency being leveraged against them.

Not all non-humanitarian use of this data is unexpected: the UNHCR considers data sharing with host countries a legitimate use of data.[196] However, any sharing of data can carry risk with it and this exchange of data is all the more risky in instances where biometric information is involved, migration is treated as a national security threat[197] and registration programmes can limit access to asylum.[198]

Further, information shared for humanitarian purposes can in some instances be used for non-humanitarian objectives. In 2019 the UNHCR signed a deal with the United States Citizenship and Immigration Service to share biometric information of refugees for potential resettlement.[199] [200] These profiles are accessible to other United States federal agencies, and may be kept by the Department of Homeland Security even if refugees do not end up in the US.[201]

The scope creep embedded in biometric technology raises concerns about future requests humanitarian organisations may get to share this data, and the potential difficulties of declining requests to share biometric data. In this case, biometric data collected by the UNHCR for registration purposes may instead be used by the Department of Homeland Security for security purposes as these DHS databases are accessible for counter-terrorism and national security needs.[202] Once biometric data is collected it can always potentially be requested by national governments, even if that was not the initial goal or purpose of biometric collection.

[196] Claire Walkey, Dr. Caitlin Procter and Dr, Nora Bardelli, “Biometric refugee registration: between benefits, risks and ethics,” *LSE blog*, July 18, 2019, https://blogs.lse.ac.uk/internationaldevelopment/2019/07/18/biometric-refugee-registration-between-benefits-risks-and-ethics/.

[197] Gus Hosein and Carly Nyst, “Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries,” *Privacy International*, September 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229.

[198] Keren Weitzberg,”Gateway or barrier? The contested politics of humanitarian biometrics,” *Data Rights Africa*, January 11, 2021, https://datarightsafrica.org/gateway-or-barrier-the-contested-politics-of-humanitarian-biometrics/.

[199] Chris Burt, “DHS to store tens of thousands of refugee biometric records from UNHCR,” Biometric Update, August 21, 2019, https://www.biometricupdate.com/201908/dhs-to-store-tens-of-thousands-of-refugee-biometric-records-from-unhcr.

[200] “United Nations High Commissioner for Refugees (UNHCR) Information Data Share,” DHS, August 13, 2019, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf.

[201] Corrigan, “DHS Is Collecting Biometrics on Thousands of Refugees Who Will Never Enter the U.S.”

[202] Corrigan.

Case: WFP and Houthi standoff in Yemen

Since the outbreak of conflict in Yemen in 2014, the WFP has been providing millions in the country with desperately needed food aid, and implemented biometric registration using the SCOPE system in 2018.[203] However, they faced difficulties implementing the system in Houthi-controlled regions, enrolling a mere 20,000 individuals in Sana'a as compared to 1.6 million people in government-controlled areas.[204]

Following allegations that Houthi operatives had been interfering in the delivery of food aid – blocking convoys and disrupting food distribution, as well as diverting food aid through local partners[205] – the WFP repeated its requests to the Houthi leadership for the implementation of a biometric system.[206] They continued to refuse, citing concerns about data sovereignty and a lack of control over the data. Claims that the WFP was not a neutral actor buttressed Houthi leadership's claims that biometric data collection constitutes a national security matter.[207]

Ongoing disagreement led to the WFP introducing a partial aid suspension in June 2019, before coming to an agreement with the Houthis a few months later. The deal emphasised the need for total transparency in aid beneficiary registration and included a biometric database,[208] with the information stored on a joint server[209] housed in Yemen that is not connected to the internet.[210]

The situation in Yemen demonstrates the manner in which the political nature of aid extends to the tools used to support aid dissemination. The Houthi government's focus on the sovereignty of data is indicative of

[203] World Food Programme, "Logistics & Emergency Telecommunications Augmentation and Coordination to Support Humanitarian Operations in Yemen," 2018, https://docs.wfp.org/api/documents/WFP-0000103871/download/.

[204] Marie-Loiuse Clausen, "Piloting Humanitarian Biometrics in Yemen," *PRIO Middle East Centre*, 2021, https://mideast.prio.org/utility/DownloadFile.ashx?id=65&type=publicationfile.

[205] Aziz El Yaakoubi and Lisa Barrington, "Yemen's Houthis and WFP dispute aid control as millions starve," *Reuters*, June 4, 2019, https://www.reuters.com/article/us-yemen-security-wfp-idUSKCN1T51YO.

[206] "World Food Programme to consider suspension of aid in Houthi-controlled areas of Yemen," *WFP*, May 20, 2019, https://www.wfp.org/news/world-food-programme-consider-suspension-aid-houthi-controlled-areas-yemen#:~:text=Earlier%20this%20month%2C%20WFP%20wrote,a%20phased%20suspension%20of%20aid.

[207] Clausen, "Piloting Humanitarian Biometrics in Yemen."

[208] "Yemen's Houthis, WFP reach deal to resume food relief," *Al Jazeera*, August 4, 2019, https://www.aljazeera.com/news/2019/8/4/yemens-houthis-wfp-reach-deal-to-resume-food-relief.

[209] World Food Programme, "Internal Audit of WFP Operations in Yemen," January 2020, https://docs.wfp.org/api/documents/WFP-0000113105/download/.

[210] Clausen.

how biometric data collection introduces a new dimension to long-standing questions around political neutrality and humanitarian action. By choosing to suspend aid, the WFP has set a watershed precedent that agencies can use the withholding of aid as leverage to erode resistance to the use of technology.

5. ANALYSIS OF ORGANISATION POLICIES

Since 2018, we've seen a wave of critical discussion emerge on the use of biometrics in the humanitarian sector, spurred by questions and concerns raised by civil society actors and impacted communities.

Within this context, and with the research presented in this report in mind, we reviewed the data management policies of humanitarian organisations known to work with biometrics, in order to understand how they are responding to challenges and potential risks. We analysed the policies of eight large humanitarian organisations who play key roles in shaping discourse and practice around humanitarian operations due to their size, influence and resources.

Our aim was to assess if and how concerns – both potential and realised – are being translated into policy and practice. In particular, we sought to assess the extent to which existing policies account for the specificities of biometrics use, and put checks and balances in place to prevent misuse of biometric data and ensure proper biometric data protection.

Below we discuss our general findings across the organisational policies we considered (for each individual assessment, see p. 59, *Organisation policy matrix*).

5.1 Gaining insights from organisational policies

Data protection and biometrics policy documents offer a window into how organisations are thinking about evolving notions of risk and the particularities of biometrics. They also provide insight into how humanitarian organisations are making decisions around their use of data, and the different rationales guiding the introduction of biometric data in humanitarian operations.

When assessing these policies we sought to capture the often complex nature of governance practices. Rather than adjudicating policies through a binary of good or bad, we focused our reviews on thinking through the dynamics of operationalisation, and the different benefits and drawbacks of each organisation's approach.

We looked at eight organisations: ICRC, IOM, Mercy Corps, Save the Children International, Oxfam, UNHCR, UNICEF, and WFP. We reached out to individuals at all of these organisations and interviewed individuals at five of the eight evaluated organisations based on availability and responsiveness. These organisations were selected based on a combination of operational size and reach within the humanitarian sector, documented use of biometrics or engagement with biometric systems and publicly availability of data management policies.

Our rubric

For our assessment, we drew inspiration from a comparative analysis of responsible data practices in the humanitarian sector conducted by GovLab and Leiden University[211] that uses a table to provide a quick visual comparison (see p. 59, *5.2 Organisation policy matrix*), and qualitative analysis (see p. 86, Annex 1.2 *Organisational policy analysis*) to give further depth.

Where organisations had a biometrics-specific policy (ICRC and Oxfam), we focused on these documents, since their general data protection policies were already analysed in GovLab's research.[212] In the case of organisations that lacked a biometrics-specific policy, we

[211] Jos Berens, Ulrich Mans, and Stefaan Verhulst, "Mapping and Comparing Responsible Data Approaches," *GOVLAB*, June 2016, https://thegovlab.org/static/files/publications/ocha.pdf.

[212] Berens, Mans, and Verhulst, "Mapping and Comparing Responsible Data Approaches."

looked at their general data protection policy and other pertinent documents (e.g. guidance documents), focusing on what we assessed to be aspects especially relevant to the responsible use of biometrics (e.g. DPIAs, data sharing agreements, storage of sensitive data).

Based on responsible data principles,[213] our previous and current research, and a preliminary assessment of the selected data protection and biometrics policies, we developed a detailed template for analysis and comparison between organisational approaches. Our assessment looked at six facets of organisational policies:

01. Policy basics
02. Proportionality and appropriateness
03. Data lifecycle considerations
04. Risks and potential harms
05. Accountability
06. Operationalisation

Within each category we outlined several questions and answered each with 'yes' or 'no'. In cases without a clear-cut answer, additional explanation is provided. For a more in-depth explanation of our methodology, see Annex 1.1.

[213] "What Is Responsible Data?"

5.2 Organisation policy matrix

1. Data protection & responsible data

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
1.1 Does the organisation have a data protection policy?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1.2 Is it grounded in responsible data principles?	Yes	*	Yes	Yes	Yes	*	No	*
1.3 Are policies accessible?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1.3.1 Are they available in a succinct version?	No	No	No*	No	No*	No	No	No
1.3.2 Is the policy freely accessible to impacted communities and the general public?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1. Data protection & responsible data (cont.)

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
1.4 Does the organisation have a biometrics-specific policy?	Yes	No	No	Yes	No	No	No	No
1.4.1 If no biometrics policy - does the policy contain language referencing or citing biometrics?	N/A	**	**	N/A	**	**	*	**

IOM: *Mention of “considering the special circumstances and vulnerabilities of data subjects” (pp. 17), but no other RD principles. **Only very limited (pp. 14, 27, 109). Mentions biometrics mainly as a kind of personal data; suggests risks of biometrics specifically (pp. 27), without explaining them.
Mercy Corps: *Main version is already short. **Only in passing, as it notes that biometrics is a form of sensitive information
SCI: *Main version is already short. **Mentions biometrics mainly as a kind of personal data (pp. 7).
UNHCR: *UNHCR policy looks to data protection principles, some of which overlap with responsible data principles. **Very limited mention in both the formal policy and guidance, more present in the guidance for registration. The UNHCR has an internal document on the used of Biometrics in Refugee Registration Verification Processes but we have not been able to view it.
UNICEF: *Biometrics mentioned as part of a list as opposed to a standalone concern. Also, mentions are very limited, as a form of personal data which needs special consideration when in use in combination with evolving technologies (pp. 1) and as a particular sensitive form of personal data (pp. 8).
WFP: *Alludes to ethical considerations and human rights, and states data minimization as a grounding principle, but no other RD principles are mentioned. **Very limited mention, qualifying biometrics as sensitive personal data (pp. 3) and as a new challenge on terms of data privacy (pp. 8), and cite it in different use case examples.

2. Proportionality & usefulness

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
2.1 Does the policy consider the appropriateness/proportionality of introducing biometrics?	Yes	No	No	Yes	No	*	Yes*	*
2.2 Does the policy outline examples of appropriate use cases?	Yes	No	No	Yes	No	No	No	No
2.3 Does it specify what types of biometrics are permissible (i.e. fingerprints, iris scans, etc) or outline criteria/ circumstances for assessment and decision-making in this regard?	Yes	No	No	Yes	No	No	Yes**	No
2.4 Does the policy specify how the biometric data should/shouldn't be associated with other types of personal data?	Yes*	No	No	Yes*	No	No	No	No

ICRC: *Establishes that pseudoanonymization techniques should be applied to personal data associated with biometrics (pp. 9).
Oxfam: *Establishes segregation from other data (pp. 9).
UNHCR: *Tangentially, as it talks of proportionality of data at large as a principle (Policy pp. 16).
UNICEF: In general, most of the biometrics specific discussion is in the guidance document and, as such, specifics or directional/ imperative instructions are missing. It's mostly suggestions about how one should go about it across a wide range of contexts. *In the biometrics guidance document. **Not permissible at large, but does discuss how to assess what type of biometrics is suitable within the flowchart.
WFP: *When discussing the specified and legitimate purpose principle, outlines biometric data collection should "be limited to the stated purpose and should never be used or shared with any other purpose, including for example, alleged security measures" (pp. 23).

3. Data lifecycle considerations

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
3.1 Does the policy consider the full data life cycle (from collection to deletion)?	Yes	*	*	Yes	Yes	Yes*	Yes*	*
3.2 Does the policy specify how biometric data should be stored (e.g. location, format - template or raw images, etc)?	Yes	No	No	Yes*	No	*	**	No
3.3 Does the policy specify processes for how biometric data should be collected?	Yes	No	No	No	No	Yes**	Yes***	No
3.4 Does the policy discuss how, when and with whom biometric data is shared?	Yes	No	No	Somewhat	No	Yes***	****	Yes**

IOM: *Somewhat, but not biometrics specifically; e.g. “assessing continued relevance” (pp. 38).
Mercy Corps: *Brief mention of life cycle.
Oxfam: *No raw data is to be stored (pp. 9).
UNHCR: *Mainly on the guidelines, and it is not biometrics specific. **Guidance on Registration and Identity Management discusses how to process personal data which includes biometrics. However, no specific guidance on biometrics. ***Under personal identifiable information and through UNHCR information notices in context-specific instances of data collection.
UNICEF: *Not specifically for biometrics, but in the overall personal data protection policy. **Discusses location (pp. 46). ***Doesn’t specifically instruct on how to collect, but provides questions that should be answered and addressed for collection to be done properly. ****It provides guidance to think through who it’s shared with and why, but as it’s only guidance it doesn’t provide definitive instructions.
WFP: *Not specific to biometrics. **Has a comprehensive data sharing section for data at large and when discussing the specified and legitimate purpose principle, outlines biometric data collection should “be limited to the stated purpose and should never be used or shared w/ any other purpose, including for example, alleged security measures” (pp. 23).

4. Risks and potential harms

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
4.1 Does the policy display a comprehensive (i.e. considers unknown unknowns/ potential future risks and the RD precautionary principle) understanding of risks in the context of using biometrics?	Yes	Yes*	No	Yes	No	No	Yes*	Yes
4.2 Does the policy include an impact and/or risk assessment both before and during the project life cycle? Is this assessment context-specific?	Yes	Yes	Yes	Yes	Yes	Yes*	Yes**	*
4.3 Does the policy address security considerations of using biometric technologies specifically, and their technical implications?	Yes	No	No	Yes	No	No	Yes*	No
4.4 Does the policy have a provision/ procedure in case of data breaches?	Yes	Yes**	No*	Yes*	Yes	Yes	Yes	Yes
4.5 Is the organisation direct/explicit about its mandate for biometrics use?	Yes	***	No	Somewhat	No	Yes**	Yes***	No**
4.6 Does the policy consider potential unintended impacts?	*	No	No	Yes	No	Yes	Yes	***
4.7 Does the policy specify anything about government/authority requests for biometric data?	Yes	No****	No	Yes	No	Yes***	Yes	Yes****

4. Risks and potential harms (cont.)

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
4.8 Does the policy include provisions for a vendor assessment? Does it address issues of reliance on vendors?	Yes	No	Yes**	Somewhat	No	Yes	Yes****	*****
4.9 Does the policy or praxis consider introduction of biometric through partner organisations or funders?	Yes	*****	No	Yes	No	****	Yes	No

ICRC: *(pp. 1)
IOM: *Present, although not in the language of unknown unknowns (see e.g. pp. 16–17). **Internal data protection auditing body (pp. 99). ***Vague, even biometrics doc is very expansive, and mentions "responsible use", but only ever in vague terms. ****IOM is an intergovernmental body, therefore can be considered a special case compared to humanitarian organisations. ****Not biometrics specifically, but includes "Relevant IOM principles reflected in written contracts" with partners under "legal considerations" (pp. 21). Biometrics doc does mention ICAO, UNDP, UNHCR, UNICEF, WFP, ICRC, and World Bank.
Mercy Corps: *Just says to inform IT. **Has a PIA for vendors specifically (pp. 4), but no discussion on issues of reliance on vendors.
Oxfam: *Demands response policy to be developed for each system (pp. 7).
UNHCR: *DPIAs are discussed in both the Data Protection Policy and the General Policy on Personal Data Protection and Policy (pp. 29). As noted previously the DPIAs is designed for personal data collection but not biometric data collection specifically. **It outlines that under its international mandate it is required to process personal data of persons of concern (Guidance pp. 55). *** For data in general. ****Talks about implementing partners, but not specifically for biometrics.
UNICEF: *In guidance document. **Mention that If context changes then another DPIA should be undertaken (PDP doc pp. 6, Guidance doc pp. 51–53). ***Asks the questions, but doesn't explicitly say if there is a firm yes or no on the mandate). ****Has suggestions for requesting independently verified data on vendor claims.
WFP: * Privacy assessment only determined for before implementation. **Vague mention, as it outlines that data will be collected to satisfy WFP's mandate. ***Yes, in its understanding of risks, but nothing specific to biometrics. ****For data in general (pp. 19–20). *****Procurement policy is referred to, but not available publicly.

5. Accountability

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
5.1 Does the organisation have an appropriate lawful basis and praxis for informed consent or some other social settlement with data subjects which is specific to biometric collection?	Yes*	*	No	Yes	Yes	Yes*	Yes*	Yes*
5.2 Does the policy outline how consent could be given or not given by affected people?	Yes**	*	No	Yes	No	Yes*	Yes**	Yes**
5.3 Does the policy include any mention of gathering feedback from affected populations?	Yes	No	No	Yes	No	Yes	***	Yes
5.4 Does the policy consider the accountability of the organisation/biometrics implementer towards communities?	Yes	No**	No	Yes	No	**	Yes****	Yes***
5.5 Does the policy specify processes for handling complaints about how biometric data is managed/used/the experience of people with this whole process?	Yes	***	No	*	No	***	*****	****
5.6 Does the organisation conduct a periodic review (e.g. a minimum of every 5 years) of its biometrics policy?	Yes	No	No	Yes**	No	No	No	No

5. Accountability (cont.)

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
5.7 Does the policy specify what happens if the policy is not followed/who is responsible for following up on this?	Yes	****	*	Yes	Somewhat	Yes****	******	No*****
5.8 Does the policy outline anything on transparency/commitment to transparency?	Yes	*****	**	Yes	No	Yes	Yes	No

ICRC: *Legitimate interest (pp. 6). **Provision of biometrics not mandatory for service provision (pp. 8), indicating other options available.
IOM: *Only data generally, not biometrics specifically (pp. 42–43). **Biometrics document says that biometrics "enables IOM and partners to plan and target projects with increased accountability and precision", unclear to whom or what this means. ***Only data generally, not biometrics specifically (pp. 43, 65). ****For data generally, not biometrics specifically, but there is a process for annual internal auditing outlined (pp. 98–99). *****For data generally, not biometrics specifically but it is one guiding principle: "access and transparency" (pp. 65 onwards); biometrics doc vaguely says "It is essential for IOM to identify areas for effective cooperation with the private sector, ensure access to the latest technologies and best practices, and embrace transparent and responsible cooperation models."
Mercy Corps: *Vague descriptions of which role is responsible for following up (pp. 4 RD policy). **For data generally, the policy notes the importance of being transparent.
Oxfam: *(pp. 5). **Commited in the policy announcement to a 12–24 month review.
UNHCR: *Only for data in general, consent or legitimate use. **It lists data subject rights and instances for engagement as part of GDPP ***Data generally, not biometrics specific. ****Data controller (which is an internal UNHCR person defined at the beginning of each project) at the first level, who then reports to the Chief Data Protection Officer.
UNICEF: *In the case of biometrics, it is discussed as a hypothetical question (Guidance doc pp. 26). **In the guidance document. ***Discusses potential reasons why it might not be suitable and encourages implementers to consider how communities might perceive the use of biometrics. ****Discusion about DPIAs being designed to "guarantee accountability, and adopt a beneficiaries' rights-oriented approach" (pp. 50). *****Mentions the need for complaint procedures, but does not specify in the guidance doc what that should look like. ******General discussion that not following policy could equal breach of conduct, but not specific to biometrics (pp. 7).
WFP: *Informed consent for general data (pp. 16), but template for consent form breaksdown consent for each data type, including biometrics. **Offers consent templates with checkboxes in which data subject might opt out of consenting to biometrics. ***Not biometrics specific. ****Not biometrics specific. *****Vague, as country director's listed as those who sign off in DPIAs (pp. 89).

6. Operationalisation

	ICRC	IOM	Mercy Corps	Oxfam	SCI	UNHCR	UNICEF	WFP
6.1 Does the policy provide clear steps for the operationalisation of the policy? (e.g. does it explain who is responsible for implementation, monitoring, and review)?	*	*	Yes*	No	No	Yes*	Yes	Yes

ICRC: *Establishes who is responsible to make sure the policy is followed, but no additional information.
IOM: *General DP policy specifies that field project “data controllers” are responsible for implementation and monitoring, and an internal auditor should conduct annual reviews (e.g. pp. 17).
UNHCR: *The Guidance document is dedicated fully to operationalisation.

5.3 Lessons learned, challenges and implementation

Across the organisational policies we reviewed, we observed wide variability regarding approach, understanding of biometrics, and specificity of policies. Some organisations have developed highly comprehensive, biometric-specific policies that diligently outline risks and proportionality, while others have more nascent policies, or none at all.

The lack of cohesion across the sector means there is no established best practice approach to the use of biometrics within the humanitarian ecosystem. These gaps in policy have tangible impacts, increasing the risk vectors for communities that come into contact with biometric systems.

Accessibility

It is important that organisational policies are easily accessible to those inside and outside of the organisation. Having documents that are both easy to locate and easy to understand (through, for example, a brief, clearly-structured summary of the policy, written in plain language)[214] is necessary for both implementers and individuals whose biometric data may potentially be collected, and for auditing by independent civil society organisations.

Of the policies we reviewed, few were both easy to locate and easy to understand, with ICRC and Oxfam being two notable exceptions. Others, such as those of the UN agencies, were simple to find, but, due to their technical language and length, would be difficult for a casual reader to understand. A few organisations had policies that were only available on request – creating a further layer of bureaucracy for those seeking out information.

[214] We did not include in this assessment if the policy was available in other languages but would like to note that this would be relevant when thinking about accessibility.

Specificity

Nearly all the organisational data policies acknowledged biometrics as an example of especially sensitive data; however, only two organisation's policies (the ICRC and Oxfam) contained processes designed to deal with the unique nature of biometric information. Though the remaining six all had some specific language referencing biometrics, this was limited in scope and usually consisted of merely noting biometrics as a category of sensitive information.

Given the immutable properties of biometric data, it is not possible to merely transpose existing data practices onto the management of biometric information. Several organisations utilised other policies (such as general data protection policies) when determining how to collect, use and store biometric data; however, these policies cannot be assumed to be attuned to the nuances of biometric use.

Without a clear position on biometrics and its use, collection, storage and deletion, field offices are left without consistent guidance, and in turn, head offices cannot be certain of how biometric information is being handled.

Proportionality, harms and risks

A crucial consideration for responsible technology deployment is whether a particular technological intervention is necessary in the first place. The immutable qualities of biometric information as well as the vast technological infrastructure required to support its use increases the need to ask fundamental questions about proportionality. Policies and guidance must support decision-makers across humanitarian organisations to think through if, when and how biometrics should be used

Five of the eight policies we looked at did not discuss the proportionality of using systems. Of the three that did review proportionality, two provided examples of appropriate use cases and offered insights into how potential risks and harms ought to factor into decision-making. Across the policies we did see clear association between biometric systems and possible harm, with five organisations mentioning and indicating an understanding of the risks of biometric systems. However we only saw limited reflection on assessing the need for biometric systems, indicating that some of the deeper reflection on proportionality is still missing from the sector.

Implementation

While implementation of policies is harder to assess than the policies themselves, many of our interviewees with experience in the field noted that implementation of biometric policies and guidance in practice is uneven. At the same time, very few policies engaged deeply with how policies would be properly implemented. Only UNICEF and ICRC discussed how biometric data should be collected, while the specifics of storage format and the importance of segregating biometric data were noted by the ICRC and Oxfam alone.

The gap between policy and practice is marked: large agencies are often highly decentralised and local offices often lack the resources to implement policies, resulting in data being shared insecurely by poorly-trained or under-resourced staff.[215] With many smaller, often less resourced organisations collecting information as implementing partners of larger organisations, there is a clear need for all organisations to share a baseline biometric data use practice to ensure cohesion across all levels of data collection.

As one interviewee, a digital rights practitioner at a medium humanitarian organisation, put it:

> Policies don't matter if people don't know about them. It's not the policy that's bad - generally speaking they are quite good but nobody knows about them. You craft the policy and tick it off but that socialisation or marketing of it to the frontline staff is never thought about and that is where everything falls apart.[216]

Proactive organisational guidance and discussion around translating policies into practice is the crucial final stage of ensuring policies are a reality. The minimal discussion around this points to a clear blind spot in organisational policies around biometric use.

[215] World Food Programme, "Strategic Evaluation of WFP's Use of Technology in Constrained Environments," January 2022, https://docs.wfp.org/api/documents/WFP-0000136278/download/.

[216] Interview with digital rights practitioner at medium humanitarian organisation

6. WHAT NEEDS TO CHANGE?

Charting a path to responsible biometric policies

The humanitarian landscape is particularly challenging and complex, requiring that practitioners introduce any innovations with even more care than in other sectors. In particular, the nature of biometric technology makes it essential that users thoroughly assess adoption risks, take steps to safeguard data subjects, and continually monitor the technology's use.

While some of the policies we reviewed had a stronger approach to responsibly deploying biometric technology – notably ICRC and Oxfam – the lack of coherence across the policies indicates a missing shared standard with which the sector could hold itself to account.

As such, we propose a five-pronged approach to thinking through the changes needed to create a healthier policy environment for the use of biometric technologies. Our suggestions are informed by the need to apply humanitarian principles proactively.

In order to help ground each section we have offered some curated key questions to support organisations in thinking about what they might need to change when approaching the use of biometric systems.

We hope the suggestions that follow can aid efforts to advance a more responsible and restrained approach to the use of biometrics in the humanitarian sector.

6.1 Continued interrogation of the necessity of biometrics

Key questions

- How do we think about necessity in the context of biometrics?
- Are biometric technologies the only option for addressing a given challenge?
- How can humanitarian practitioners create space for alternative solutions?
- How do we resist path dependency?
- What steps can be codified to ensure that real need drives the adoption of biometrics?

As discussed in this report, evidence on the realisation of the anticipated benefits of biometric technologies remains uneven. In some cases, adoption of the technology has brought additional risk, delays and unanticipated challenges. The technology itself is technologically complex and resource-intensive.

This points to a continued need for the space to interrogate whether biometrics are actually necessary. Decision-makers, program managers and country office staff must fully consider alternatives to biometrics. There may be other technologies or approaches that are more affordable, easier to implement or more secure.

However, given the current momentum behind adoption of biometrics, individual practitioners report a sense of inevitability to adopting the technology. This path dependency – with big organisations already using these systems in much of their work, making their continued use seem both unavoidable and vital – limits the ability to take a problem-first, intentional approach.

Next steps for humanitarian practitioners

- Creating tools for – and normalising conversation around – assessing the necessity of biometric technologies. These can highlight what biometric technology can uniquely make possible alongside what unique risks it brings. (More information on these can be found in our Primer.)

- Mapping alternatives to biometric systems, demonstrating what different approaches may better solve particular challenges.
- Conducting more thorough, systematic investigations capturing the realised (not anticipated) benefits of biometric technology adoption, and assessing them alongside the particular contextual and implementation factors required to realise these benefits.
- A review of the appropriateness and feasibility of informed consent in the context of biometrics systems.

Next steps for funders

- Providing incentives that encourage – and support – a problem-first approach to adopting technology, rather than technology-first. For example, by not promoting biometric technology adoption unless there is a clear and unique need that these systems would address.
- Funding viable alternatives to biometrics and supporting work that seeks to measure the realised benefits of any new technology that is adopted.

6.2 More nuanced policy design and implementation

Key questions

- Who is considered in the policy design and implementation process?
- Are our policies accessible?
- Can our policies be implemented?
- How do we create space for feedback and engage with criticism?
- In what ways do staffing processes e.g. high turnover, short-term contracts, impact how we design and implement policies?

Regardless of where organisations stand on the use of biometrics, there is a universal need for clear and accessible policies. These policies should be specific to biometrics and make clear why biometric information is unique. Additionally, there is a universal need for implementers – especially those in regional and country offices, and volunteers – to have access to the resources and knowledge necessary to implement these policies.

Addressing these needs starts from the beginning of policy design. In particular, impacted communities should be consulted in the creation of policies and their participation guaranteed. Once policies are made, they must be accessible and easy to find. Clear and concise versions of all policies should be available to the individuals whose biometric data is being collected. Additionally, local staff have the most interaction with impacted communities, and as such, high-level policy making needs to happen in collaboration with country offices from the start.

A significant number of humanitarian organisations have their headquarters in a minority world country, with smaller regional and country offices located across the majority world. To allow regional and country offices to respond to their own contexts, many of these smaller offices (and the program managers within them) have significant autonomy over decision-making. However, these local staff are often ill-equipped to implement the policies handed down to them, lacking sufficient training, attention and resources. Furthermore, data protection staff in headquarter offices also face a lack of financial and staff resources to better support local staff.

Frequently we found that the will to implement policies was not the main obstruction to successful implementation: rather, the financial and technical resources needed to create and socialise policies were absent. Without this support, necessary policies cannot be actioned, leaving a disconnect between what organisations want to achieve and what they are equipped to deliver.

To bolster the implementability of policies, donors must make grants that account for the resource-intensiveness of mitigating risk and, in turn, implementers should make adequate protection/policy development a core part of their fundraising efforts.

Next steps for humanitarian practitioners

- Review policy-making processes and ensure that they centre impacted communities and local staff expertise.
- Ensure that policies also consider impacted communities' ability to seek redress specific to their biometric data, and establish clear, accessible, and well-understood mechanisms for redress.
- Have a clear process to assess a policy's feasibility and the resources local staff will need in order to ensure it is implemented effectively.
- Review existing risk frameworks and ensure they consider the unique needs of biometrics, with a particular focus on making sure they are attuned to the specific needs and responsibilities of the humanitarian sector, and consider the full scope of potential risks that may arise.

Next steps for funders

- When funding any technology intervention, and biometrics in particular, include a requirement of dedicated support for technological and backend support, digital security support, and training to improve technical literacy.
- Specifically provide support to implementers to develop processes for the development and implementation of robust and contextual policies around biometric technologies.
- Ensure that funding is in place to familiarise staff with safer and more responsible approaches to biometrics.

6.3 Establishing community-centred standards of practice

Key questions

- Are similar and/or partnered organisations operating on a shared framework of understanding?
- How do we create coherency in the sector with regards to the use of biometrics?

As documented earlier in this report (see p. 48 Section 5, *Analysis of organisation policies*), despite the increased uptake and use of biometric technologies, a lack of baseline policy standards persists, especially around biometrics-specific policies. Furthermore, there is no international standard around accountability or remedy for harms, and the deployment of biometric technologies by humanitarian organisations often takes place in contexts with little or non-existent data protection and privacy regulations.

Accordingly, humanitarian organisations – as distinct entities and an entire sector – have an important responsibility to uphold data protection and privacy standards themselves, as their deployment of biometric technologies could become the basis for regulations and best practices later on.

Strong international standards could help alleviate biometrics-related risks by providing a basis for shared rules, expectations, and accountability mechanisms between donors, humanitarian organisations, and beneficiary communities. Shared standards could also reduce uncertainty and opacity when deploying new biometric tools on the ground.

However, the development of robust international standards will not be effective if solely approached from a technical perspective or top-down fashion. Instead, both implementers and donors have a role to play in connecting community-driven standards to the global level.

Implementers can continually facilitate a feedback cycle that connects emergent community-level standards to high-level policy discussions and vice versa, while funders should explicitly sponsor this work. Work on both fronts is important but the latter may allow for smaller incremental changes to happen faster. Donors should focus their support on those working towards immediate change in the way biometric information is used and handled.

The development of these standards is itself a political process that is highly contextual – requiring that on-the-ground realities play a central role in discussions – and that will have direct impacts on the recipients of aid.[217] As such, standardisation should not replace assessments of the appropriateness of biometric technologies in particular local contexts, and due consideration is required for translating standards into practice.[218] Though standardisation alone cannot ad-

[217] Interview with digital advisor at humanitarian organisation

[218] Interview with members of a large humanitarian organisation

dress the shortcomings of data management practices that pervade the humanitarian space,[219] it can create a shared baseline of operating standards for the use of biometrics.

Next steps for humanitarian practitioners

- Push for coherence across the humanitarian sector's high-level approach to biometric technologies.
- Centre local- and community-led needs and approaches in conversations around shared standards, ensuring that local humanitarian implementers and impacted communities play a role both in shaping standards and localising and executing them.
- Establish regular dialogue between humanitarian organisations, practitioners and impacted individuals on responsible biometrics use and implementation.

Next steps for funders

- Support the discussion around and creation of shared standards specifically around biometric technology use.
- Do not fund approaches that do not consider data safety and security in a proactive manner (see p. 73, *6.2 More nuanced policy design and implementation*).
- Once sectoral standards exist, support funding recipients to align their work accordingly.

6.4 Strengthen practices around Data Protection Impact Assessments (DPIAs)

Key questions

- How do we ensure that DPIAs are understood by all stakeholders?
- How do we develop sufficiently detailed DPIAs?

[219] Loy, "'It's like the wild west': Data security in frontline aid."

- How do we maintain DPIAs and mitigate new risks after the initial assessment and during a project's lifecycle?

Data Protection Impact Assessments, or DPIAs, were included as a critical step in most policies we reviewed; however, they were frequently overloaded by commitments that, according to our analysis, currently go largely unfulfilled (see p. 37, *What hasn't changed since our last report?*). Given that many policies relied on DPIAs as a key aspect of mapping out potential risks and harms, their revision is crucial for successful policy implementation.

Next steps for humanitarian practitioners

- Make DPIAs more legible to "non-technical" people by, for example, consistently including consultation with impacted communities in the process of creating DPIAs.
- In particular, redesign DPIAs to (1) better identify potential harms even when performed by non-experts, (2) effectively outline risks and benefits to each stakeholder, and (3) encourage practitioners to map out potential imbalances between who reaps the benefits and who carries the risks.
- Ensure DPIAs are integrated into programme design, and are undertaken before any data is collected, in order to properly inform decision-making around and implementation of biometric technologies.
- Consider making DPIAs or their findings publicly available and auditable by those whose lives will be impacted by the introduction of the new technology, while monitoring the potential impacts doing so may have on projects, the thoroughness of analyses and impacted communities themselves.

Next steps for funders

- Standardise the practice of asking humanitarian organisations about DPIAs in the funding process.
- Fund and encourage cost recovery around the resources required to create and implement DPIAs.

- Incentivise funding recipients to ensure they consult with impacted communities in the DPIA development process.
- Establish practices around auditing DPIAs.

6.5 More sophisticated ecosystem-wide analysis of technology

Key questions

- What ways of thinking are driving decision-making?
- How do we acknowledge the resource constrained environments of humanitarian contexts, while avoiding an over reliance on technological solutions?
- What is the appropriate role of private sector actors that do not explicitly adhere to humanitarian principles?

The challenges to safer adoption of biometric technologies are connected to broader trends within the humanitarian ecosystem. In particular, attitudes towards technology generally show a bias towards techno-solutionism and a lack of investment in scoping out alternatives to high-tech solutions.

Though the desire for efficiency and hope that technology can inherently improve processes are understandable within the context of limited resources and growing humanitarian need, a more critical analysis is required.

Evidenced in our interviews, and in literature discussing biometrics, is a tendency to outline the pros and cons of biometrics as though all elements can be weighed equally, with benefits and harms directly weighed against each other. However, it is increasingly clear from recent events in Afghanistan, Myanmar and Kenya, where some of the most-feared risks of biometrics were realised, that the pros and cons of biometrics use do not have equal weight.

Discussion around how to account for the impacts on beneficiaries — for instance, the trauma of fearing your citizenship is in jeopardy, or, on the other hand, the lived benefit of faster access to cash assistance – while also looking at impacts for aid implementing agencies (such as those listed in the Biometrics Primer) is necessary. These discussions are and will be complex – they cannot be resolved through a cost-benefit analysis or balance sheet.

More accurately weighing potential benefits that underpin common justifications for biometrics (e.g. around compliance, accountability and reporting) – and having nuanced discussions when they are simply incomparable to potential harms – is a collective step that requires all parties of the humanitarian system to take action.

Organisations must rethink the appropriateness of their growing role as data brokers, and whether their existing data collection is absolutely necessary for their operations. Those already using biometric systems on a large scale should take time to critically reflect on their use of these systems, and consider pausing any expansion.

Donors, too, should consider the ways in which their demands place pressure on organisations to implement biometric systems. The urge for evidence-informed action and extensive reporting contributes to an enabling environment for biometric systems that can sway funders' decision-making. Despite the desirability of evidence-informed humanitarian action, a focus on easily measurable empirical evidence should be tempered with considerations regarding the fairness and consequences of the policymaking process. A more cautious approach would consider not only what works but also what the overall goal should be, and whether particular solutions are appropriate in, or potentially detrimental to, specific local contexts.[220]

Additionally, donors have a responsibility to develop their own familiarity with data security and privacy broadly and with the sensitivity of biometrics in particular – our research suggested that this is currently lacking.[221]

Next steps for humanitarian practitioners

- Embrace radical commitments to transparency regarding, and open dialogue around, the reasoning, purpose and technical limitations of using biometric systems.

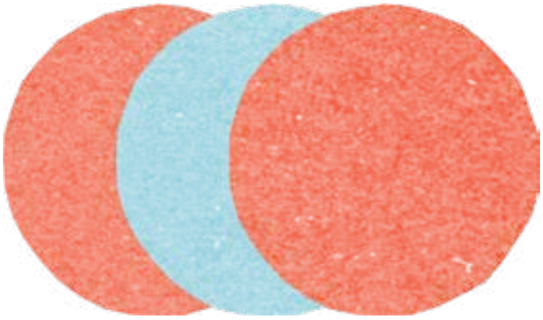
[220] Greenhalgh and Russell, "Evidence-Based Policymaking: A Critique," 310.

[221] Interview with researcher on digital human rights

- Define explicit steps to address feedback and concerns from impacted individuals and communities.
- Develop clear mitigatory measures in response to the worst case scenarios we have seen play out.
- Develop and circulate new frameworks for if, when, how biometrics should be used, which make space for technical and non-technical alternatives.
- Conduct research to thoroughly account for the costs – financial, time and human – required to responsibly and sustainably deploy biometric technology, ensuring that benefits/risks are properly weighted in accordance with the severity of their impact.

Next steps for funders

- Fund work that accounts for the actual costs of designing, implementing and protecting a biometric system.
- Support greater evidence gathering that contextualises the benefits of biometric systems in relation to the real severity of risks.
- Provide assistance and funding for organisations to address foundational digital safety and security concerns.
- Invest time and money in alternatives to biometric technologies, and create space for organisations to choose not to use biometrics.



ANNEX 1 ORGANISATIONS’ POLICIES: RUBRIC AND ANALYSIS

1.1 Explaining our rubric

Policy basics

This set of questions evaluates basic aspects of the data protection governance in the selected organisations; namely, the presence of a data protection policy and of a biometrics-specific policy, how accessible these are, and the principles underpinning organisational policy. A key aspect of our evaluation of these policies is whether they incorporate responsible data principles, i.e. consideration or inclusion of language contemplating issues of power dynamics between data holders and data subjects; unknown unknowns; precautionary principles; thoughtful innovation; aiming for higher standards than current normative frameworks; issues of diversity and bias; and the goal of building better behaviours.

- Does the organisation have a data protection policy?
  - Is it grounded in, or aligned with, responsible data principles?
  - Are policies accessible?
  - Are they available in a succinct version?
  - Is the policy freely accessible to impacted communities and the general public (e.g. for download) or only available upon request?
- Does the organisation have a biometrics-specific policy?
  - If not: does the general policy contain language referencing or citing biometrics?

Proportionality and appropriateness

Policies should be equipped with the capacity to assess appropriateness, with decision-making criteria in relation to the use of biometrics considered through the lens of proportionality. The principle of proportionality "implies that data collected may not include more than is required to fulfil the purpose for which they were collected. According to this principle, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed."[222] For organisations to assess this, use cases of biometric technologies are important to include in order to demonstrate what situations do or do not meet the bar of their policy stipulations and exemplify the appropriateness of introducing biometrics.

- Does the policy consider the appropriateness/proportionality of introducing biometrics?
- Does the policy outline examples of appropriate use cases?
- Does it specify what types of biometrics are permissible (i.e. fingerprints, iris scans, etc) or outline criteria/circumstances for assessment and decision-making in this regard?
- Does the policy specify how the biometric data should/shouldn't be associated with other types of personal data?

Data life cycle considerations

The use of biometrics requires special considerations with regard to the particularities of its data life cycle, especially given its immutable nature and common reuse for purposes other than those originally specified (with the potential for harmful function creep). In this regard, it's important to consider the details of any data sharing agreements made by humanitarian organisations with other humanitarian partners, commercial actors, and governments, as data subjects cannot currently know the full trajectory of their data due to opaque data practices and policies. Our third set of questions seeks to assess these aspects of biometric data.

[222] Yue Liu, "The principle of proportionality in biometrics: Case studies from Norway," *Computer Law & Security Review* 25, no. 3 (2009): 237-250, https://doi.org/10.1016/j.clsr.2009.03.005.

- Does the policy consider the full data life cycle (from collection to deletion)?
- Does the policy specify how biometric data should be stored (e.g. location, format – template or full images, etc)?
- Does the policy specify processes for how biometric data should be collected?
- Does the policy discuss how, when and with whom biometric data is shared?

Risks and potential harms

We want to understand how organisational policies map out and protect against or mitigate risks in the context of biometrics. This is especially important given that the risks and harms of biometric use are likely to evolve over time,[223] which biometric policies must be equipped to deal with.

Because organisations often design data protection policies to be applied to a range of use cases, policies tend to take a broad high-level approach that does not consider the specific security issues associated with biometrics use.

The questions that follow were designed to assess the level of specificity and comprehensiveness in relation to known and unknown risks. We also probe the organisational rationale for introducing or relying on biometrics in their operations, and assess the degree to which organisational mandates provide legitimacy and grounds for using and requiring biometric data from their beneficiaries. Finally, we broach the subject of humanitarian organisations and their relations with third parties and providers, assessing issues ranging from the technical (e.g. vendor lock-in, interoperability) to the social/political (e.g. access by third parties, enforcement of protection policies by partners).

- Does the policy display a comprehensive understanding of risks? (i.e. Does it consider unknown unknowns/potential future risks and the Responsible Data precautionary principle?)
- Does the policy include an impact and/or risk assessment both before and during the project life cycle? Is this assessment context-specific?

[223] Krishnan.

- Does the policy address the security considerations and technical implications of using biometric technologies specifically?
- Does the policy have a provision/procedure in case of data breaches?
- Does the organisation explicitly state its mandate to use biometrics?
- Does the organisational policy account for/consider potential unintended impacts?
- Does the policy specify anything about government/authority requests for biometric data?
- Third-party related risks
  - Does the policy include provisions for a vendor assessment? Does it address issues of reliance on vendors?
  - Does the policy or practice consider the introduction of biometric systems through partner organisations or funding channels?

Accountability

Key to the discussion on biometrics is accountability to the populations whose data is being collected in the first place. The following set of questions covers different aspects of accountability, from consent and other lawful bases for data collection, to the handling of complaints and the attribution of responsibility.

- Does the organisation have an appropriate lawful basis and practise for informed consent (or a similar legal principle) from data subjects that is specific to biometric collection?
- Does the policy outline how consent could be given or refused by affected people?
- Does the policy include any mention of gathering feedback from affected populations regarding their opinions or experiences of biometric technologies?
- Does the policy consider the accountability of the organisation/ biometrics implementer towards communities?
- Does the policy specify processes for handling complaints about how biometric data is managed/used/the experience of people with this whole process?
- Does the organisation conduct a periodic review (e.g. a minimum of every 5 years) of its biometrics policy?

- Does the policy specify what happens if the policy is not followed/ who is responsible for following up on this?
- Does the policy outline anything concerning transparency or state a commitment to transparency?

Operationalisation

Organisations face a number of challenges when attempting to implement data protection policies in their work (see: Section 5.2 *Lessons learned, challenges and implementation*). This last question seeks to assess if and how the policies of humanitarian organisations provide guidance on their realisation.

- Does the policy provide clear steps for the operationalisation of the policy? (e.g. does it explain who is responsible for implementation, monitoring, and review?)

1.2 Organisational policy analysis

ICRC

The International Committee of the Red Cross (ICRC) was the first humanitarian organisation to produce and implement a data protection policy focused on biometrics, and can be considered a standard bearer in the sector. Their policies are thorough and provide a clear and systematic approach to the use of biometrics that prioritises the data subject.

The **2019 Policy on the Processing of Biometric Data**[224] is a complement to the ICRC's wider reaching **Rules on Personal Data Protection,**[225] and addresses the specific challenges of using biometrics in programming.[226] Notably, the policy outlines acceptable/pre-appro-

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

[225] International Committee of the Red Cross, "ICRC Rules on Personal Data Protection," June 12, 2020, https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

[226] "The ICRC Biometrics Policy."

ved use cases for biometrics, which include travel documents provided by ICRC to persons with no valid identity documents; fingerprint data, facial scans and DNA to identify human remains originated from situations of violence; and services and assistance provision with a token-based verification credential (i.e. card) that can be used to verify receipt. This provides a clear rubric to assist program officers with decision-making while also demonstrating the uses the ICRC deems automatically acceptable.

Current approved use cases outlined in the policy do not require ICRC to hold biometric data, an approach the organisation refers to as a beneficiary-centric (or user-centric) approach to the ownership of the data. This approach prioritises data-subjects and ensures their privacy and security is upheld.

DPIAs are also discussed in depth within the policy, which outlines their necessity for approved use cases along with a regular review system. The policy also establishes the need for the assessment prior to any biometric data transfers to a government or authority.

On the theme of sharing biometric data with authorities, the policy adopts a conservative approach, understanding that the purpose of interest in this data might be incompatible with ICRC's mandate (the document cites border and migration control, counter-terrorism activities and national security as examples of incompatible data usage). By limiting sharing with governments, the ICRC makes clear its commitment to impacted communities first and foremost.

While the theme of consent is not explicitly addressed in the biometrics policy (only in the **general data protection policy**), it states that in cases when data subjects object to providing their biometrics, ICRC must ensure service provision regardless.[227] Used in conjunction with ICRC's general data protection policy, the policy provides a thoughtful framework for the governance of biometrics in the humanitarian space, in line with responsible data's precautionary principle and understanding of checks and balances that would alert in case of unexpected impacts.

IOM

Despite documented use of biometric technologies, it is difficult to evaluate or hold the IOM accountable for its deployment of biometrics

[227] "The ICRC Biometrics Policy," 15.

given the scarcity of publicly available policies relating to these technologies. The primary data protection document, the **Data Protection Manual** lacks specifics on biometric use, while the single biometric focused document, “**IOM and biometrics**” does not present comprehensive data protection considerations or guidelines.

The IOM bases its data protection practices on its own **Data Protection Manual**, published in 2010.[228] The document is dated, lacking what have now become standard terminology and considerations related to responsible data principles, for instance. The document also fails to consider biometric data as a special category of sensitive data, and only mentions biometrics in passing as one of many categories of “personal data.”[229] One “example” box states that “the arbitrary use of biometric data” could lead to “unfair discrimination or limit the free and lawful movement of migrants,”[230] yet such risks are never discussed in more detail elsewhere in the Manual.

The organisation has only publicly discussed its attitudes toward biometric data in an ‘info sheet’ titled “IOM and biometrics.”[231] The info sheet represents biometrics primarily as beneficial to migration management and humanitarian action without discussing potential risks arising from the deployment of these technologies. The info sheet mentions that the organisation has carried out a “comprehensive in-house assessment” of its use of biometric technologies; however, that assessment has not been made public.

The organisation’s Data Protection Manual does address several key considerations related to data protection generally. It accounts for the full data life cycle, provides an outline for conducting risk–benefit assessments to determine the appropriateness of collecting personal data, considers potential issues related to informed consent in the field, and outlines internal auditing mechanisms to ensure the implementation of the data protection policies in practice. However, the Manual does not discuss the applicability of these general considerations to biometric data specifically.

[228] IOM, “IOM Data Protection Manual,” 2010, 12, https://publications.iom.int/books/iom-data-protection-manual.

[229] IOM, “IOM Data Protection Manual,” 14.

[230] IOM, 27.

[231] IOM, “IOM and Biometrics,” November 2018, https://www.iom.int/sites/g/files/tmzbdl486/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf.

Even when supplementing the Data Protection Manual with statements from the IOM's biometrics-specific documentation, it remains clear that the organisation lacks coherent, comprehensive, and publicly available policy frameworks for the collection and use of biometric data.

Mercy Corps

Mercy Corps' policies offer little in the way of specific policy or guidance related to biometric use. Mercy Corps data protection practices are based on a **Responsible Data Policy**,[232] and the organisation has also published a set of **Data Protection and Privacy Guides**[233] to "help Mercy Corps staff better understand and implement responsible data privacy."

The Responsible Data Policy is based on a set of clearly outlined principles such as transparency, privacy, and fairness. Improper sharing of such data, according to the document, can result in "harm to a person, such as sanctions, discrimination and security threats" and can result in "negative impact on Mercy Corps' ability to carry out activities and reduced trust or public perception."[234]

The privacy guides mention biometric data as one type of "sensitive data."[235] Yet this mention is the only explicit reference to biometric data in Mercy Corps' data protection documentation, despite the fact that the organisation's "Technology for Impact" report presents biometric technologies as crucial to its cash distribution programs.

Many of the underlying principles within the policy and guide draw on best practices around responsible data and are a welcome start. For instance, the comprehensive understanding of informed consent[236] and beneficiaries' expectations regarding data sharing indicates a good understanding of the dynamics of informed consent. Having both a general policy and more practical guidelines is also a desirable first step.

Nonetheless, it is difficult to assess the organisation's attitude toward biometric data specifically due to the absence of such considerations

[232] Mercy Corps, "Responsible Data Toolkit," December 18, 2018, https://www.mercycorps.org/research-resources/responsible-data-toolkit.

[233] Mercy Corps, "Data Protection and Privacy Guides," 2022, https://dldocs.mercycorps.org/DataProtectionPrivacyGuides.pdf.

[234] Mercy Corps, "Data Protection and Privacy Guides," 1.

[235] Mercy Corps, 1.

[236] "Responsible Data Toolkit."

from the policy or practical guidelines. Nowhere in these documents are issues such as proportionality, risks and harms, and accountability in the use of biometrics discussed. More detail is needed in order for the guides and policy to shape implementation in a clear and directed manner.

Save the Children International (SCI)

This analysis is of the 2019 SCI Policy: Data Protection Policy, which SCI informed us they had taken offline after we shared this analysis in our right to reply process. SCI informed us that this policy was no longer in use and that a more current policy was being used to inform decision-making. However we were not able to review this newer policy as it is internal. At the time of writing, the 2019 SCI Policy is still available online. We have chosen to keep the analysis in this report while noting that the original document we reviewed may no longer be available online.

Save the Children International's (SCI) data protection policy provides a useful basis for outlining data protection practices in more detail. However, the lack of publicly available documentation on more specific procedures combined with the absence of considerations relating to biometric data specifically, make it difficult to evaluate the organisation's deployment of biometric technologies.

SCI's data protection practices are based on the publicly available **Data Protection Policy document**.[237] The document outlines the responsible data principles that underpin it, and makes reference to legal frameworks such as the EU General Data Protection Regulation (GDPR), which SCI staff are expected to understand and comply with. The policy also lists several **related documents** that outline more specific procedures related to data breaches, for instance, as well as guidance relating to issues such as consent.

However these related documents cannot be readily accessed by the public, thereby limiting external review and feedback.

As with many other organisational data protection policies, SCI's policy does not consider biometric data in detail. "Genetic and biometric data" is mentioned only in passing, as one of several categories of "sensitive personal data."[238] The organisation has not published any

[237] Save the Children International, "SCI Policy: Data Protection Policy," September 1, 2019, https://www.savethechildren.net/sites/www.savethechildren.net/files/Appendix%2010-%20Data%20Protection%20Policy.pdf.

[238] Save the Children International, "SCI Policy: Data Protection Policy."

further documentation relating specifically to biometric data collection in its projects.

Although the Data Protection Policy is quite short, it does outline a relatively comprehensive set of considerations relating to principles such as fairness, transparency, purpose limitations, and accountability throughout the project life cycle. However, based on existing documentation, it remains unclear how far SCI views biometric technologies as requiring unique considerations compared to data protection more generally.

Oxfam

Oxfam's biometric policies extensively consider the complexity of using biometrics. Oxfam's **Biometric and Foundational Identity Policy**[239] was published in 2021, and is reflective of considerable internal consultation processes that included a qualitative survey as well as informal sessions with staff.[240] The policy supplements Oxfam's **Data Protection Policy** and the **Responsible Data in Program Policy**,[241] and considers the specificities of biometric data.

The policy contains provisions on some key features related to the responsible deployment of biometrics: it explicitly considers the risks of reusing this type of data, prohibits the storage of raw biometric data and requires DPIAs throughout the project lifecycle.

Several aspects of the policy are noteworthy. Instead of assuming admissible use cases for biometrics, the policy states that any use of biometrics and identity databases must have a demonstrable benefit to individuals and communities[242] and that if said benefit is not a "demonstrable fundamental use case with benefit", Oxfam would not move forward nor participate in the project. This would mean that in the early stages of design a clear benefit for the data subjects would have to be assessed and proved, which can likely push decision-makers to have to clearly outline the distribution of benefits and risks among stakeholders.

[239] Oxfam, "Oxfam Biometric and Foundational Identity Policy," May 18, 2021, https://oxfam.app.box.com/v/OxfamBiometricPolicy.

[240] James Eaton-Lee and Elizabeth Shaughnessy, "Oxfam's New Policy on Biometrics Explores Safe and Responsible Data Practice," *Views & Voices blog*, June 24, 2021, https://views-voices.oxfam.org.uk/2021/06/oxfams-new-policy-on-biometrics-explores-safe-and-responsible-data-practice/.

[241] Oxfam, "Oxfam Responsible Program Data Policy," Oxfam, August 27, 2015, https://policy-practice.oxfam.org/resources/oxfam-responsible-program-data-policy-575950/.

[242] Oxfam, "Oxfam Biometric and Foundational Identity Policy," 4.

Accountability to communities is also considered throughout the document, embedded in different principles, which helps to centre impacted communities in the consideration of biometrics. Oxfam's is the only policy to speak on the power imbalance between data subjects and organisations[243] that needs to be taken into account when considering the choice to give or withhold biometric data. This acknowledgement in a governance document is a welcome critical reflection on one of the key aspects that pervade the relationship between "beneficiaries" and humanitarian organisations that needs to be taken into account when developing programming. The document offers a holistic perspective on biometric use and the potential impacts of its use in programming.

UNHCR

Beyond common standards of data protection, UNHCR does not provide substantial insight on the treatment of biometric data by the agency. UNHCR's personal data protection practices are based on the 2015 **Policy on the Protection of Personal Data of Persons of Concern,**[244] the 2018 **Guidance on the Protection of Personal Data of Persons of Concern**[245] (henceforth referred to as policy guidance) and the 2022 **General Policy on Personal Data Protection and Privacy** (GDPP).[246]

The first document outlines basic principles while the second offers guidance and considerations for the operationalisation of the policy. GDPP is a broader document that offers pathways to implementation for the previously released UN **Principles on Personal Data Protection and Privacy** from 2018.[247] Relevant to the governance of biometrics specifically is the **Guidance on Registration and Identity Management** (henceforth referred to as registration guidance), a web-based guide designed to support registration efforts by UNHCR staff.[248] UNHCR does have a policy on **Biometrics in refugee registration and verifica-**

[243] Oxfam, "Oxfam Biometric and Foundational Identity Policy," 5.

[244] UNHCR, "Policy on the Protection of Personal Data of Persons of Concern to UNHCR," *Refworld*, May 2015, https://www.refworld.org/docid/55643c1d4.html.

[245] UNHCR, "Policy on the Protection of Personal Data of Persons of Concern to UNHCR."

[246] UNHCR, "General Policy on Personal Data Protection and Privacy," *Refworld*, December 2022, https://www.refworld.org/docid/63d3bdf94.html.

[247] "Principles on Personal Data Protection and Privacy," UNHCR, 2018, https://unsceb.org/principles-personal-data-protection-and-privacy-listing.

[248] UNHCR, "Guidance on Registration and Identity Management," 2018, https://www.unhcr.org/registration-guidance/.

tion released in December 2010,[249] but it is an internal document and not available for our review.[250]

Language on biometrics is quite sparse across the policies and is usually mentioned as an example of sensitive personal data, or in the context of registration. In the policy guidance, for example, biometrics is cited as an increasingly necessary way to identify a person[251] and as a tool in efforts towards accuracy.[252] Biometric data is also cited as an example of data systems "perceived or expected to carry inherent privacy risk"[253] requiring a DPIA before being introduced into operations. DPIAs are required in the policy for any new systems, projects and policies, as well as before entering new data transfer arrangements.[254]

In terms of accountability, while the policy guidance offers some frameworks for handling complaints from data subjects, neither document discusses how the organisation will gather feedback from impacted communities on data collection and management processes. Though this theme is explored more at length in the registration guidance, it is done so strictly in the context of continued registration.[255]

On the theme of data transfers to third parties and data sharing agreements, it is worth noting that the policy guidance establishes DPIAs as a best practice prior to any agreement, focusing specifically on data security capabilities of third parties[256] but not clearly addressing other potential unintended consequences, such as potential malicious/political use of the data by third parties (e.g. governments).

Overall, these documents do not provide substantial insight on the treatment of biometric data by the agency, beyond common standards of data protection.

[249] UNHCR, "UNHCR Resettlement Handbook," 2011, 165, https://www.unhcr.org/in/sites/en-in/files/legacy-pdf/46f7c0ee2.pdf.

[250] This internal policy was confirmed via the UNHCR's response provided as part of the right to reply process.

[251] UNHCR, "UNHCR Resettlement Handbook," 9.

[252] UNHCR (2018), 20.

[253] UNHCR (2018), 53.

[254] UNHCR (2018), 28.

[255] UNHCR, "Communication in the Context of Continuous Registration," 2018, https://www.unhcr.org/registration-guidance/chapter4/communication-in-the-context-of-continuous-registration/.

[256] UNHCR (2018), 57.

UNICEF

UNICEF lacks a clear policy on biometric data, choosing instead to focus on broader guidance that relies on the discretion of local offices for implementation. Overall the guidance itself does provide a useful learning tool to prompt discussion and reflection; however, as it is not explicitly paired with clear policy, it is ultimately unenforceable and thus cannot be relied upon to prevent harms arising from the use of biometric technologies.

UNICEF's data protection measures consist of both a **Personal Data Protection policy**,[257] and a guide to help country and regional offices assess biometric technologies for inclusion in their programs, titled "**Faces, Fingerprints & Feet**."[258] The Personal Data Protection policy covers the use of identifiable personal data such as name, date of birth, location, while "Faces, Fingerprints & Feet" is a guidance document focused specifically on advice related to biometric technologies.

Most of the biometric-specific content is housed in the "Faces, Fingerprints & Feet" biometrics guidance document which is intended to inform policy, offering suggestions for how to approach the use of biometrics rather than direct instructions. This limits the extent to which we can assess the effectiveness of UNICEF's evaluative framework regarding the use of biometric technologies. The emphasis on guidance within the document leaves ambiguity regarding implementation, and is evident in the lack of specifics around data storage, data sharing and appropriate use cases.

Despite raising concerns about potential risks, such as "if a host country was to request or demand humanitarian data to repurpose for law enforcement,"[259] it does not provide country offices with clear directions on how to proceed in such instances. Ultimately the guidance is designed to assist offices in navigating decision-making, not to mandate specific action.

UNICEF's policy on personal data protection is relatively minimal – especially when compared to other UN agencies. The personal data protection policy is intended to be applicable across data applications, and addresses data governance issues within the organisation. It men-

[257] UNICEF, "UNICEF Policy on Personal Data Protection," July 15, 2020, https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.

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

[259] UNICEF, 44.

tions biometrics briefly as an example of an “evolving technology”[260] and a form of “particularly sensitive data.”[261]

The absence of direct policy instructions for the use of biometrics within the data protection policy leaves significant ambiguity around how the guidance specifically applies to biometrics. Despite placing biometrics as falling under the category of particularly sensitive data, there are no specific directions on how to handle biometric information.

The guidance does make attempts to think about the way in which biometric technology, and the risks associated with its use, might evolve with time. This includes consideration of the various potential risks of using biometrics generally, and for children specifically, in section two of the report. It also indicates when risk levels or an ability to ameliorate threats should result in halting the use of biometrics.

Further, it considers the larger web of actors beyond the biometric system itself, encouraging for instance that offices independently verify vendor claims regarding the effectiveness and benefits of their technologies. UNICEF’s guidance captures the complexities of mapping risk and harm in relation to biometric use, and takes the critical step of making clear when biometrics should not be used. As a result this guidance equips decision makers with a full picture of the implications and impact of introducing biometric technology into programming.

WFP

The WFP **Guide to Personal Data Protection and Privacy**,[262] from 2016, is the agency’s main document on data protection and governance. It outlines five grounding principles (lawful and fair collection and processing; specified and legitimate purpose; data quality; participation and accountability; data security) for the management and protection of data by WFP personnel and their implementing partners plus some general considerations and guidance on operationalisation.

The policy is extensive (over 120 pages) and somewhat comprehensive, outlining example use cases and potential risks. However, similar to other UN agencies’ data protection policies, it contains limited language specifically on biometrics. In the policy, biometric data is qualified

[260] UNICEF, 1.

[261] UNICEF, 8.

[262] World Food Programme, “WFP Guide to Personal Data Protection and Privacy Fighting Hunger Worldwide,” June 2016, https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

as sensitive data and sparsely cited in biometric use cases throughout the text. Where mentioned, the policy characterises biometrics as an example of sensitive information "which should never be used or shared for any other purpose, including, for example, alleged national security measures."[263]

Especially relevant to biometrics are the discussions on DPIAs and data sharing policies. DPIAs are used "for early stages of project design"[264] and throughout the document issues deemed to be potential risks are flagged to be included in these assessments. The WFP also discusses the potential impact of including national data protection laws that could be in conflict with WFP's mandate,[265] indicating an attempt to foresee unintended impacts. Though the policy provides an outline for these risk assessment exercises, it does not discuss the use of DPIAs during project implementation.

In terms of data sharing, the policy outlines basic requirements for data sharing, both inbound and outbound.[266] Most notably it reiterates throughout the text the need for clear communication with beneficiaries to facilitate their informed consent and provides a framework for risk and benefit analysis. The consent form template, provided as an annex, breaks down consent per type of data to be collected (including biometrics), and offers the possibility to opt out.[267]

Regarding participation and accountability, the document states that "beneficiaries should be consulted about the processing of their personal data before and during all stages"[268] and informs that consultation of beneficiaries on the types of data they would be comfortable with should be part of the projects' DPIAs.

General guidance on operationalisation (e.g. a quick set of questions to ensure the practice of data minimisation is followed)[269] is provided throughout the document, referring to the Data Protection Officer at HQ as the ultimate authority for advice and guidance in case of doubt.

[263] World Food Programme, "WFP Guide to Personal Data Protection and Privacy Fighting Hunger Worldwide," 23.

[264] World Food Programme, 16.

[265] World Food Programme, 19.

[266] World Food Programme, 56.

[267] World Food Programme, 112.

[268] World Food Programme, 28.

[269] World Food Programme, 27.

Beyond that, however, as flagged in the independent review of the agency's use of technology in constrained environments published in 2022, WFP remains without a single position, review or reflection on its use and experience with biometrics[270] despite being one of the largest actors in regards to biometrics deployment in this sector and its role in pushing other organisations to biometrics use via service delivery.

[270] World Food Programme, "Strategic Evaluation of WFP's Use of Technology in Constrained Environments WFP EVALUATION," January 2022, 27, https://docs.wfp.org/api/documents/WFP-0000136278/download/.

THE ENGINE ROOM