Biometrics in the Humanitarian Sector

THE ENGINE ROOM

OXFAM

This report has been commissioned by Oxfam's Global Humanitarian Team funded by Oxfam Intermon with support from the Oxfam ICT in Programme team. Ownership of Data Protection will vary by affiliate depending on the context and operational model, but for the purposes of this report we reference Oxfam.

The research for this report was conducted by The Engine Room from December 2017-March 2018. The content of this report does not reflect the official opinion of Oxfam, and responsibility for the information and views expressed in the report lies entirely with The Engine Room.

Commissioning Editor and Content Support: Anna Kondakhchyan
Lead Researcher: Zara Rahman (The Engine Room)
Research Assistant: Paola Verhaert (The Engine Room)
Research Consultant: Carly Nyst (Independent)

The Engine Room requests due acknowledgement and quotes from this publication to be referenced as: The Engine Room and Oxfam: Biometrics in the Humanitarian Sector: March 2018. This report is available at https://theengineroom.org.

Table of Contents

1. Introduction

As Oxfam reaches the end of a two-year self-imposed moratorium on the introduction of biometrics into its programmatic work[1], the organisation has commissioned The Engine Room to provide advice and recommendations regarding the future of biometrics in Oxfam's programmes. The primary objective of this report is to provide Oxfam with sufficient information, backed up by evidence, to take an informed decision about how they should engage with biometrics over the short term, i.e. three to five years.

After providing context on how biometrics are currently used in the humanitarian and development sector, this report outlines the benefits and potential harms.

1.1 BACKGROUND

The context in which Oxfam is deciding whether and how to integrate biometrics into its programmes is one defined by the following factors.

• **Widespread deployment of biometrics in development and humanitarian contexts**: In 2015, UNHCR began rolling out its global Biometric Identity Management System ("BIMS"). UNHCR and WFP now operate wide-ranging biometrics registration systems, to which implementing partners also have access and contribute, broadening programmatic uses beyond refugee protection to cash-based interventions[2] and voter registration.[3]

• **Increased pressure by international donors to integrate biometrics into aid delivery**: Recent years have seen increased pressure put on and by donor institutions to demonstrate the effectiveness of humanitarian interventions, alongside highly-hyped new technological tools such as biometrics.[4] Stakeholders report that USAID and WFP are encouraging local organisations and INGOs to integrate biometrics to meet such requirements.

• **The growing preference for cash-based interventions**: Another aid-effectiveness tool increasingly prioritised by donors and humanitarian agencies alike is cash-based interventions. One implication of this transition towards cash is that INGOs and other humanitarian actors are under even greater pressure to monitor and report on the distribution of assistance. Furthermore, organisations implementing cash transfers are, in many cases, obliged to integrate their programmes with the biometrics-based systems of private sector actors involved in the cash transfer value chain.

• **A changing regulatory environment**: Among other areas of regulation, data protection law covers how organisations acquiring biometric data must process, retain, store and destroy such data. Unfortunately for INGOs, there is little coalescence of data protection regulation outside of Europe, with many developing countries lacking any data protection regulation. 2018 will see the European General Data Protection Regulation ("GDPR"), the most rigorous legal framework

anywhere in the world, come into force. The GDPR places onerous obligations on organisations, especially with regards to biometric data. There is also a strengthening of controls around terrorism financing, through the vehicle of UN Security Council Resolutions and recommendations of the FInancial Action Task Force,[5] which has imposed on financial institutions and other regulated entities stricter "Know Your Customer" requirements. These requirements have, in turn, driven the adoption of biometrics as a purported tool for more reliably authenticating identity claims.

• **Hype around new technologies in the humanitarian sector**: Amid pushes for innovation, the humanitarian and international development sector have been home for sometimes 'experimental' uses of technology, more easily employed in this context since developing countries typically have weaker regulatory environments for data protection. Despite a lack of evidence demonstrating whether these technologies actually solve humanitarian problems,[6] they are subject to hype and attention. Biometrics fall in this category.

2. Understanding the options

2.1. What are biometrics?

Biometric data are "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual."[7] The term "biometrics" is commonly used as shorthand to describe technical systems which involve the collection of biometric data to conduct authentication or identification of an individual. Biometrics are not new – photographs have been used in this sector for years, but current discourse around "biometrics" commonly refers to fingerprints, face prints and iris scans. As technology continues to advance, capabilities for capturing other forms of biometric data are also improving, such that voice prints, retinal scans, vein patterns, tongue prints, lip movements, ear patterns, gait, and of course, DNA, can be used for authentication and identification purposes.

2.2. Why are biometrics different?

The debate around biometrics is grounded in the assumption that biometric data is qualitatively different to other types of personal data.

HOW HAS THE BIOMETRICS SECTOR CHANGED SINCE 2015?

Since information was gathered in 2015 by Oxfam to inform the decision on the moratorium, biometric technologies have further developed. Beyond the cases documented here on the use of biometrics in the humanitarian sector, other trends of how biometrics uses and potential uses in other sectors to be aware of include: (note: this is a non-exhaustive list.)

- Greater integration of consumer-facing products which include biometrics technology (eg. smartphones with integrated fingerprint sensors; smartphones with facial recognition systems; vehicles with biometric technology for deployment)

- Integration of machine learning and artificial intelligence; for example, voice-controlled virtual assistants.[8]

- The development of more elaborate spoofing or 'adversarial' biometric recognition techniques[9], often using machine-learning technologies, which will likely become easier and cheaper to do over time.[10]

- Greater integration of biometrics with public services like voting, as is the case in at least 42 countries worldwide from data gathered in 2016[11], or key services like purchasing mobile phone SIM cards in Bangladesh[12], allowing governments to gather biometric data on populations at large with no particular purpose.

- The development of biometrics recognition

technologies that (by design) can be done without the knowledge of the person – such as typing-based 'fingerprints'[13], facial recognition technology; gait analysis.[14]

The following factors are relevant when thinking about why biometrics, or certain types of biometrics, should be processed with greater care than other personal data: uniqueness and immutability, richness of information, and flexibility of use.

• **Uniqueness and immutability**: Unlike names, appearance or home addresses, most forms of biometric data are singularly unique to the individual involved and cannot be changed. Fingerprints, DNA samples and iris scans, for example, are constant and immutable, making them a convenient and rigorous basis upon which to base long-term identification. The same characteristics which make biometrics an optimal basis for identification also render their processing of particular concern. Because they are not only objective and irrefutable but unique, their replication, distillation, and storage creates risks for the individual concerned, who is no longer the sole possessor of their own biometric data. The non-revocability of biometrics, and the fact that they stay persistently the same over an individual's lifetime (with some important exceptions) means that biometric samples taken today could be used by and integrated into unknown and yet-to-be invented future technologies. *See section 3.2.2. for more on the risks related to the reuseability of biometric systems.*

• **Richness of information**: In addition to their highly personal nature, some biometric data such as DNA samples contain extremely sensitive information about an individual, including information about their health, that is of particular concern to both an individual and their relatives.[15] In the case of such biometric data, which can reveal a range of intimate information about an individual, the consequences of misuse, abuse, loss, or theft are much greater, and thus the threshold for its acquisition must also be higher. *See section 3.2.3. for more on the risks related to the security of biometric systems.*

• **Flexibility of use**: As technology advances, biometrics are increasingly used for surveillance and monitoring. Advancements are also permitting passive identification, for example using facial or iris recognition at a distance, without the knowledge or involvement of the individual concerned.[16] The increased speed and declining costs of such technologies permit their widespread deployment and operation.[17] Certain types of biometrics enable even more invasive types of profiling: DNA could be used to distil ethnic or racial profiles, for example. The automated design of such systems often frustrates scrutiny and accountability, rendering individuals unable to contest the decisions of biometric identification systems. *See section 3.2.4. for more on the risks related to the societal impacts of biometric systems.*

2.3. How are biometrics being used in development and humanitarian contexts?

The seminal 2013 study by Alan Gelb and Julia Clark researched 160 cases of biometrics deployment in 73 developing countries (excluding biometrics systems primarily for border control or law enforcement means), and noted two primary categories of biometrics identification systems: foundational systems and functional systems:[18]

Foundational systems are those which supply general identification for many official uses, such as national civil registries and national IDs.

Functional systems are those which are introduced in response to a demand for a particular service or transaction, such as voter IDs, health records, or financial access.

In that regard, the two largest actors in the "biometrics for humanitarianism" space are UNHCR and WFP, both of whom deploy biometrics identification both as part of beneficiary registration and in distributing assistance, as functional systems.

WFP's system is called SCOPE, and is a web-based platform that acts as a central repository for WFP beneficiary data. UNHCR's system is the Biometric Identity Management System (BIMS).

Generally speaking, biometrics systems generally permit humanitarian and development actors to conduct two different types of authentication: verification and identification.

2.3.1. BIOMETRICS FOR VERIFICATION (ONE-TO-ONE AUTHENTICATION)

Biometrics can be deployed to verify a beneficiary is who they say they are. This is also called "one-to-one" authentication, as it involves comparing the biometric data of an individual to only one biometric profile, the profile that they claim will match theirs. Using biometrics in this manner permits organisations to accurately verify, for example, that a beneficiary is entitled to the food, vaccine or housing that they claim to be entitled to, and can prevent fraudulent claims.

Technically, using biometrics for verification requires a more limited set of data to be retained and distributed. Biometrics for verification can be done by comparing a biometric sample (a person's fingerprint) with a biometric profile stored on an an ID card, or against a biometric profile stored on a device.

2.3.2. BIOMETRICS FOR IDENTIFICATION (ONE-TO-MANY AUTHENTICATION)

Biometrics can also be used to identify an individual amongst a database of biometric profiles. "One-to-many" authentication occurs when an individual presents their biometric data and it is compared against stored biometric profiles to authenticate the individual's unique identity. Organisations use biometrics for identification to prevent fraudulent enrollments and to "de-duplicate" lists of beneficiaries (by being able to detect and remove multiple enrollments). Both UNHCR's BIMS and WFP's SCOPE enable the registration of a unique identity for a beneficiary and then operate to enable staff to authenticate beneficiaires in a one-to-many comparison to biometric profiles stored in a centralised database.

One-to-many authentication systems raise more concerns than one-to-one systems. Technically, they require a larger amount of data to be stored in one place, creating a vulnerability for the organisation, and more data may be transmitted over potentially insecure channels. One-to-many systems also experience more false matches.[19] *See section 3.2.1. for more on the risks related to the accuracy of biometric systems.*

3. Benefits and risks of biometrics

In this section, we conduct an analysis of literature and stakeholder claims regarding the potential benefits and risks of deploying biometrics.

3.1. The benefits of biometrics

Literature, stakeholders and organisations align on the reasons for and benefits of integrating biometrics into development and humanitarian assistance programmes: these include that biometrics help to identify the people targeted for assistance (identifiability and traceability) reduce fraud and duplication (accuracy and integrity), and simplify registration and identification (simplicity and efficacy).

3.1.1. IDENTIFIABILITY AND TRACEABILITY

More than two million people worldwide are not identified by government documents,[20] a considerable barrier to the delivery of humanitarian assistance. Biometrics are adopted by donors and development actors to bridge the gap between unidentified beneficiaries and the targeted assistance to which they are entitled.[21] In practice, because humanitarian actors are often working in countries and situations where foundational identity systems are lacking, they deploy biometrics as a means of assigning an official identity to beneficiaries.

Biometrics can also be used to trace beneficiaries and delivery of aid. By assigning biometric identities to beneficiaries, organisations can ensure that individuals are kept within the oversight of the programme, and track better where the aid ends up.

It is clear that biometrics do facilitate more immediate traceability of aid delivery. For example, a review of cash transfers in Jordan demonstrates that the traceability benefits include real-time withdrawal data, disaggregated by ATM locations, being transmitted directly to the humanitarian organisations, enabling organisations to anticipate and respond to beneficiary problems.[22] But the traceability potential of biometrics also creates risks for individual beneficiaries. Granular data about vulnerable individuals' movements, purchases, attendance at schools and health clinics, and other access to social transfers enable precise and private inferences to be made about their lives, which inferences can be used by malevolent actors as well as benevolent ones. ***See section 3.2.3. for more on the risks related to the security of biometric systems.***

3.1.2. ACCURACY AND INTEGRITY

The most frequently-cited justification for biometrics is that they enhance the accuracy and integrity of development and humanitarian interventions by reducing fraud. Biometrics are billed as the answer to double-registrations of beneficiaries[23], with relevant literature containing claims such as "cash assistance using biometrics is close to being completely fraud-proof,"[24] and "UNHCR's monthly assistance programme uses

CAN BIOMETRICS REDUCE FRAUD?

Overwhelmingly, the strongest argument for biometrics relates to the technology being used to reduce fraud. Our interviews with stakeholders and our review of the literature revealed that upon closer examination, this argument has a problematic premise. As above, however, there is a serious lack of evidence as to whether the perceptions outlined here, drawn from interviews and anecdotes, are accurate or not.

Specifically: the biggest problems identified regarding fraud, when it comes to aid delivery, appear to happen 'upstream', as part of the supply chain of getting aid to its end point. That is, ensuring that aid is delivered through the supply chain as intended without any loss of product or diversion of aid, for example. Though duplication (ie. when one beneficiary receives aid twice) has been identified as a problem, multiple interviewees identified that quantitatively, this is less of a problem than the more systemic issues along the supply chain.

Using biometrics on beneficiaries only allows for accountability checks to be done at the 'downstream' part of the process – ie. Checking how many beneficiaries are there, checking who they are, checking that they are entitled to receive the assigned amount, and ensuring they each receive the assigned amount. This level of accountability check does not address issues along the supply chain.

While providing audit chains is a necessary part of being a transparent and accountable organisation, interviewees suggested that it was unfair to put the burden of accountability checks on the beneficiaries, when the real problems with fraud are elsewhere in the ecosystem. That said, identifying that biometrics only affect fraud at the beneficiary end rather than at the supply end, is not necessarily a reason not to engage; but rather, a point of perspective to bear in mind.

fraud-proof iris-scan technology."[25] A reduction in fraud means an increase in accuracy and verifiability, according to advocates of biometric systems.[26] It may also be key to maintaining donor support for such mechanisms.[27]

Despite the pervasiveness of this justification, there is lack of evidence as to whether biometrics could help reduce fraud, and as to whether the fraud is happening by beneficiaries or earlier on in the supply chain (*see Highlight box above*.) Certainly, a number of stakeholders interviewed by The Engine Room perceived fraud to be a real problem in humanitarian programmes, but were unable to put the problem into figures. Such anecdotes are not supported by evidence, and tend not to distinguish between the potential deterrent effect of a biometrics system and the actual fraud detection capabilities of the system. As such, it is difficult to make an informed assessment as to whether or not biometrics can detect, or reduce, double-registrations or duplications by beneficiaries.
To the best of our knowledge, there has been no publicly-available effort to compare the cost of instituting biometrics systems with the cost of fraud to the organisations. Furthermore, no organisation seems to be instituting biometrics to address the problem of fraud amongst field or partner staff, nor looking into how biometrics could be used to address issues of supply chain fraud. This could be due to organisations believing that they can control internal risk without the need of biometrics, but that behaviour of third parties including beneficiaries is harder to control.

3.1.3. SIMPLICITY AND EFFICACY

The introduction of biometrics into registration and identification has the potential to streamline beneficiary registration and speed up the delivery of humanitarian assistance.[28] The efficiency effects of biometrics are primarily due to the fact that a digitised identification system reliant on biometrics eliminates the time-lag necessary to authenticate paper identity documents.[29] Biometrics systems can free-up human resources from those purposes and thus speed up the process of delivering assistance.

There is some evidence that biometrics makes

aid provision generally more efficient. For example, the experience of the Common Cash Facility in Jordan: because UNHCR was able to export biometric data directly to the financial institution delivering cash transfers, this reduced for beneficiary enrollment times and saved beneficiaries from having to go to the bank and register for an account there. Furthermore, the bank's requirements for documentation and identification would have previously meant that individuals would have to wait months to register with the Jordanian government to obtain an identity card before opening a bank account. These times were drastically reduced through the use of the biometrics system by UNHCR and its partners.[30]

3.2. The negative impacts and risks of biometrics

Critics of biometrics generally point to the potential for false matches (reliability), the possibility that biometrics could be use by other actors and for unimagined purposes (reusability), the risks of theft, loss or misuse of biometric data (security), and the potential for exclusion (societal impacts) as factors that militate against the integration of biometrics into humanitarian work.

3.2.1. RELIABILITY

Although biometrics systems are billed as an answer to the fallible analogue systems of identification and registration, biometric-based identification can return false matches.[31] False negatives occur when the system does not identify a match when it should, while false positives occur when the system does identify a match when it should not. False matches may reflect inaccuracies in the process of recording the biometric data in the first place; fingerprinting has the highest rate of error.[32]

There are no quantitative studies or available statistics on the frequency of false matches in biometrics systems deployed by humanitarian actors, though general studies show that error rates of biometric systems reduce when the amount and type of biometric data collected increases.[33] The trade off for increasing the reliability of the system is impeding its security, by collecting and storing even more sensitive biometric data. Beyond false matches, some other studies show that biometric systems are far from infallible; aging changes the iris in ways that can impede biometric authentication,[34] fake irises can deceive the system,[35] and fingerprints and iris scans can be replicated.[36] It is reasonable to assume, too, that though some of these methods are currently difficult for the layperson to replicate, they may well become cheaper and easier to do in the future.

3.2.2. REUSABILITY

The ease with which biometric data can be shared, analysed and repurposed is both what makes biometrics so attractive to development and humanitarian actors, and what makes it so potentially dangerous, argue critics. Governments of host countries as well as countries of origin could obtain access to the biometric databases of humanitarian actors, either by request or by demand, and repurposed for law enforcement or national security screening, for example.

Data could also be sold for profit, used by foreign countries for intelligence, or used to publicly embarrass and undermine humanitarian organisations.[37] There are also concerns that biometrics systems, once in place, could be expanded to accommodate ever more intrusive data; organisations may start off using fingerprints and this could expand to include DNA analysis, for example. The probability of such use depends upon a number of factors, including cost. Similarly, future technology could be developed to gain more insights from biometric data that is gathered now.

These concerns are supported by documented examples. Governments playing hosts to large refugee populations, such as Lebanon, have claimed a right to access to UNHCR's biometric database, and donor States have supported UNHCR's use of biometrics out of their own interest in using the biometric data acquired as part of the so-called ongoing "war on terror".[38] Even outside of the development context, historical trends have shown that databases initially established for one purpose often become co-opted for law enforcement or intelligence ends.[39]

With regards to the efficiency side of arguments around reusabillity, it is not possible to know whether in total, the extra time invested at the start of the process with biometrics eventually balances out over time. Further time needs to be invested in

human infrastructure: training registration staff on how to take biometric samples, an often difficult task particularly with respect to fingerprints.[40] Interviewees with experience in biometric registration processes expressed differing views in this regard – some noting that they found the process to be much quicker, others noting they found it to take longer overall.

3.2.3. SECURITY

The most persuasive argument levied by biometrics' critics is that using biometric data places an enormous burden on organisations to constantly maintain a high level of technical and organisational security. The loss, theft or misuse of biometric data compromises an individual's legal identity in circumstances in which they have few other options for establishing that identity. Beneficiaries in humanitarian crises are fleeing persecution and have good reason to want to protect their identity, location and movements. By collecting biometric data and storing it in centralised databases, aid organisations could place beneficiaries at serious risk.

These concerns are not theoretical. Documents published by National Security Agency whistleblower Edward Snowden showed that US and British intelligence agencies targeted humanitarian organisations like UNICEF, UNDP and Medecins du Monde for surveillance.[41]

Software flaws and poor technology governance standards mean that technologies deployed by humanitarian actors might be vulnerable to compromise by a range of different actors; as the recent penetration of digital distribution platform RedRose by a rival company demonstrates.[42] The experience of establishing wifi networks in destinations for Syrian refugees is illustrative; one such network in Greece was subject to up to 80,000 hostile attacks every week.[43] Moreover, anecdotal evidence abounds of humanitarian workers losing laptops, USB keys and other digital files containing beneficiary data.

3.2.4. REPUTATION

Interviewees identified that part of the challenge for Oxfam when it comes to biometrics centres around reputational risk, conceptualised in two ways: actual risk and perceived risk. These are not Oxfam-specific, but would broadly apply to any international organisation using or setting up biometric systems.

The first would be a problem if any kind of data breach or security threat were to happen with the data that Oxfam (or any of the confederation members) held – such as a host government requesting to use the biometric database held, or an accidental leak of the database to a third party. A data breach of one of the Oxfam confederation members could affect local partners and beneficiaries trust in Oxfam at large, ultimately jeopardising Oxfam's ability to meet its mission, not to mention international trust and perception of the way in which Oxfam do their work.

The second, perceived risks, could arise in cases of misinformation spreading within camps. One interviewee noted that misinformation is a real problem in camps where Oxfam and other humanitarian organisations currently work, expressing worry that it could only take one rumour around what the purpose of the biometric data collected is being used for, for beneficiaries to become deeply suspicious of the organisation. That said, misinformation is not a risk unique to this scenario or use of data in particular, but rather one to be considered.

3.2.5. SOCIETAL IMPACTS

As with all technologies, biometrics can have unintended exclusionary aspects. Individuals may be reluctant to submit to providing biometric samples because of cultural, gender or power imbalances. Acquiring biometric samples can be more difficult for persons of darker skin colour or persons with disabilities. Fingerprinting, in particular, can be difficult to undertake correctly, particularly when beneficiaries' fingerprints are less pronounced due to manual and rural labour.[44] All of these aspects may inhibit individuals' provision of biometric data and thus exclude them from the provision of assistance.

Experts have argued that biometrics also have more intangible long-term disadvantageous societal effects and may entrench existing power disparities. Shoshana Magnet asserts that the process of capturing, decoding, and recoding the human body in biometrics is a communicative act of representation and power that reproduces social inequalities along traditional lines of

difference, such as class, race, ethnicity, gender, sexuality, and disability.[45] It is extremely difficult to measure or even perceive the long-term effects of converting individual human identity into a digital biometric representation and to assess how that may embed discrimination. Further research needs to be done in order to comprehend these impacts, and there is a strong argument for not taking irrevocable steps to deploy biometrics until such research is produced.

In the short term view, there is inconsistent evidence supporting concerns about exclusion. Some stakeholders presented anecdotal evidence of cultural rejection of biometric systems, such as the refusal by over 70 percent of veiled Muslim women in Bangladesh to submit to iris scans or have photographs taken. Aside from this, however, stakeholders interviewed by The Engine Room could not recall significant incidents in which beneficiaries objected to biometrics being taken or where disabilities or other problems had prevented registration. Stakeholders from UNHCR, reporting on the experience of running a "one stop shop" helpdesk in Jordan supporting the implementation of the IrisGuard initiative, reported insignificant numbers of rejections or refusals.

The discourse around the "identifiability" benefits of biometrics in humanitarian interventions often tends to conflate the role that biometrics play. Aid agencies cannot "give" a beneficiary an identity, they can only record identifying features and check those against other records. Treating the acquisition of biometric data as constitutive of identity risks dehumanising beneficiaries, most of whom are already disempowered in their relationship with humanitarian entities upon whom they rely for survival. This attitude is evident in the remarks of one Burmese refugee undergoing fingerprint registration in Malaysia in 2006 -- "I don't know what it is for, but I do what UNHCR wants me to do"[46] – and of a Congolese refugee in Malawi, who upon completing biometric registration told staff, "I can be someone now."[47]

Furthermore, the framing of biometrics identity systems as constitutive of beneficiaries' identity could lead to a deference to biometric identities that may cause real risks to beneficiaries. Errors in entering biometric and personal data may become entrenched in a black box system and come to determine a beneficiary's long-term access to humanitarian aid and assistance. Without appropriate adjudication processes, this could lead to adverse effects like unfair exclusion.

We are hesitant to conclude that the use of biometrics technology does not raise a significant risk of exclusion. Beneficiaries are in a relationship of asymmetric power with humanitarian organisations and may not be in a position to voice their discomfort with or opposition to the technologies used by these agencies.

Reports from interviews we conducted suggest that UNHCR has adopted the approach that refusal to submit to biometric registration amounts to refusal to submit to registration at all. If this is true, this constrains beneficiaries' right to contest the taking of biometric data, and creates a considerable disincentive to beneficiaries voicing opposition to the biometric approach.

4. Conclusion

Oxfam's approach to biometrics thus far has been innovative for its thoughtfulness and consideration, choosing to share the above, broad research findings to inform the sector. We excluded Oxfam-specific recommendations drawn from these findings, as these recommendations relate to Oxfam's internal structure and ways of working, assuming that these are less useful for the broader public.

Our research led us to appreciate Oxfam's approach not least for setting a high standard within the humanitarian sector, but for putting beneficiary rights and needs above donor pressure and technology hype. Broadly speaking, the key difference with biometrics technology in comparison to other digital technologies is that this technology has the potential for harm that humanitarian agencies engaging with biometrics would not be able to go back and fix, or adjust.

From our analysis, we conclude that the potential risks for humanitarian agencies of holding vast amounts of immutable biometric data – legally, operationally, and reputationally, combined with the potential risks to beneficiaries – far outweigh the potential benefits in almost all cases. Though systems might be sped up, or parts of processes made easier, we have identified only few situations where there are no potential alternative systems that could be instituted instead.

We suggest starting from this premise when considering whether or not biometrics are helpful, on a case-by-case basis: in which situation would the benefits of a particular biometrics system outweigh the identified risks?

As a sector, there is almost no publicly-available evidence, research or agreed-upon standard for using biometrics. Though they have been widely adopted by certain agencies, our collective understanding of their effects is still at a very early stage. We encourage humanitarian agencies exploring using biometrics, and those already implementing biometric systems, to consider filling that evidence gap in a way that contributes to better sector-wide understanding of the implications of biometrics, and we look forward to contributing to this in the future.

Notes

1. For notes on why the moratorium was instituted, see internal Oxfam GB biometrics position paper.

2. WFP, "WFP introduces iris scan technology to provide food assistance to Syrian refugees in Zaatari," 6 October 2016, available at https://www.wfp.org/news/news-release/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu.

3. UNDP Yemen, "Biometric voter registration kit testing provides glimpse into future of elections in Yemen," 2013, available at http://www.ye.undp.org/content/yemen/en/home/ourwork/democraticgovernance/successstories/biometric-voter-registration-kit-testing-provides-glimpse-into-f.html.

4. Heidi Gilert & Lois Austin, Review of the Common Cash Facility approach in Jordan, UNHCR and the Cash Learning Partnership, October 2017, available at http://www.cashlearning.org/downloads/calp-ccf-jordan-web.pdf.

5. This regulation is underpinned by a number of international instruments: UN Security Council Resolution 137 and the Convention for the Suppression of the Financing of Terrorism, which imposed on State obligations to prevent and suppress the financing of terrorist acts and to criminalise terrorism-related activities; The Convention Against Transnational Organized Crime and the Convention against Corruption, which, inter alia, require regulation in the area of financial institutions and money laundering; and the Financial Action Task Force on Money-Laundering ("FATF") Recommendations, which are a set of 40 recommendations and 9 special recommendations designed to provide a comprehensive set of measures for a legal and institutional regime against money laundering and the financing of terrorism.

6. Eric M. Johnson, "Red Cross launches first U.S. drone program for disasters," Reuters, 7 September 2017, available at: https://www.reuters.com/article/us-storm-harvey-redcross-drones/red-cross-launches-first-u-s-drone-program-for-disasters-idUSKCN1BI2X9; Swiss Foundation for Mine Action & CartONG, Drones in Humanitarian Action - guide to the use of airborne systems in humanitarian crises, 2 December 2016, available at: https://reliefweb.int/report/world/drones-humanitarian-action-guide-use-airborne-systems-humanitarian-crises.

7. Woodward, J. D., Orlans, N. M., & Higgins, P. T., Biometrics: Identity Assurance in the Information Age (McGraw-Hill Osborne Media: 2003).

8. Alex Perala, "BRIEF: The New Artificial Intelligence Explosion," Mobile ID World, 11 October 2017, available at: https://mobileidworld.com/artificial-intelligence-explosion-010114/.

9. Battista Biggio, Giorgio Fumera, Paolo Russu, Luca Didaci & Fabio Roli, "Adversarial Biometric Recognition : A review on biometric system security from the adversarial machine-learning perspective," IEEE Signal Processing Magazine, 12 August 2015, available at: http://ieeexplore.ieee.org/document/7192841/.

10. Taylor Armerding, "Vocal theft on the horizon," CSO Online, 16 May 2017, available at: https://www.csoonline.com/article/3196820/security/vocal-theft-on-the-horizon.html.

11. IDEA, "Is the biometric data used in voter identification at polling stations," available at: https://www.idea.int/data-tools/question-view/739.

12. Zara Rahman, "Bangladesh Will Demand Biometric Data From All SIM Card Users," Global Voices, 22 December 2015, available at: https://globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users/.

13. Lucian Constantin, "AI-based typing biometrics might be authentication's next big thing," PC World, 27 January 2017, available at: https://www.pcworld.com/article/3162010/security/ai-based-typing-biometrics-might-be-authentications-next-big-thing.html.

14. "The future of biometrics technology: Convenience or privacy," Reuters, 2 June 2017, available at: https://blogs.thomsonreuters.com/answerson/biometrics-technology-convenience-data-privacy/.

15. S and Marper v United Kingdom, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, 4 December 2008, at [72].

16. Anne-Marie Oostveen & Diana Dimitrova, "Iris scanners can now identify us from 40 feet away," The Conversation, 21 May 2015, available at: http://theconversation.com/iris-scanners-can-now-identify-us-from-40-feet-away-42141.

17. Edin Omanovic, "Biometrics knows no borders, it must be subject to extreme vetting," Privacy International, 25 October 2017, available at https://privacyinternational.org/node/1538?PageSpeed=noscript.

18. Alan Gelb & Julia Clark, "Identification for Development: The Biometrics Revolution", Center for Global Development Working Paper 315 January 2013, available at: https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315, p. 1.

19. Privacy International, Biometrics: Friend or Foe of Privacy?, September 2017, available at: https://www.privacyinternational.org/node/24, p. 6.

20. Charlie Ensor, "Biometrics in aid and development: Game changer or trouble-maker?" The Guardian, 22 February 2016, available at www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology.

21. UNHCR, "Biometric Identity Management System," 2015, available at: http://www.unhcr.org/550c304c9.pdf.

22. WFP, "First Cash Assistance to Secondary Girl Students Using Biometrics in Fata," 24 May 2017, available at: https://www.wfp.org/news/news-release/first-cash-assistance-secondary-girl-students-using-biometrics-fata.

23. See, for example, Dina Fine Maron, "Eye-Imaging ID Unlocks Aid Dollars for Syrian Civil War Refugees," Scientific American, 18 September 2013, available at https://www.scientificamerican.com/article/eye-imaging-id-unlocks-aid/.

24. Heidi Gilert & Lois Austin, Review of the Common Cash Facility approach in Jordan, UNHCR and the Cash Learning Partnership, October 2017, available at http://www.cashlearning.org/downloads/calp-ccf-jordan-web.pdf.

25. UNHCR Innovation, "Using biometrics to bring assistance to refugees in Jordan," UNHCR Innovation Service, 30 August 2016, available at: www.unhcr.org/innovation/using-biometrics-bring-assistance-refugees-jordan/.

26. Ibid.

27. According to a UNHCR spokesperson: "[I]f a rejected asylum seeker tries to reapply for refugee status, the system will automatically discover this. The system will also discover if a person is fraudulently claiming to be someone she, or he, is not. Such a security measure will certainly enhance the credibility of UNHCR's registration system in the eyes of the [...] government and other partners. Yante Ismail, "Fingerprints mark new direction in refugee registration," UNHCR, 30 November 2006, available at: http://www.unhcr.org/uk/news/latest/2006/11/456ede422/fingerprints-mark-new-direction-refugee-registration.html.

28. Charlie Ensor, "Biometrics in aid and development: Game changer or trouble-maker?" The Guardian, 22 February 2016, available at www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology.

29. Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," Journal of Intervention and Statebuilding, 2017, available at: http://www.tandfonline.com/doi/pdf/10.1080/17502977.2017.1347856?needAccess=true.

30. A UNHCR review of a biometrics pilot in Malawi demonstrated that 30 percent of registration staff found fingerprints difficult to use, and overwhelmingly preferred iris scanning and facial recognition technologies, from Heidi Gilert & Lois Austin, Review of the Common Cash Facility approach in Jordan, UNHCR and the Cash Learning Partnership, October 2017, available at http://www.cashlearning.org/downloads/calp-ccf-jordan-web.pdf.

31. Alan Gelb & Julia Clark, "Identification for Development: The Biometrics Revolution", Center for Global Development Working Paper 315 January 2013, available at: https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315, p. 9.

32. Privacy International, Biometrics: Friend or Foe of Privacy?, September 2017, available at: https://www.privacyinternational.org/node/24,p. 11.

33. For example, a study of India's Aadhaar biometric identity system, which requires twelve pieces of biometric data (ten fingerprints and two iris scans) found that the probability of a false negative was estimated at only 0.035 percent, and the probability of a false positive at 0.057 percent. Alan Gelb & Julia Clark, "Identification for Development: The Biometrics Revolution", Center for Global Development Working Paper 315 January 2013, available at: https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315.

34. Kevin W. Bowyer & Samuel P. Fenker, Analysis of Template Aging in Iris Biometrics. Paper presented at the IEEE Computer Society Biometrics Workshop, June 17, 2012, available at: https://www3.nd.edu/~kwb/Fenker_Bowyer_CVPRW_2012.pdf.

35. Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., & Ortega-Garcia, J., From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems. Paper presented at the Black Hat USA, Las Vegas, 2012, available at: https://media.blackhat.com/bh-us-12/Briefings/Galbally/BH_US_12_Galbally_Iris_Reconstruction_WP.pdf.

36. Divij Joshi, "India's Biometric Identificiation Programs and Privacy Concerns," The Centre for Internet and Society, 31 March 2013, available at: https://cis-india.org/internet-governance/blog/indias-biometric-identification-programs-and-privacy-concerns.

37. Data which have been stolen or leaked from insufficiently secure medical databases have been repurposed in a similar way: Gus Hosein & Aaron Martin, "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations," London School of Economics, December 2010, available at: http://personal.lse.ac.uk/martinak/eHealth.pdf.

38. Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," Journal of Intervention and Statebuilding, 2017, available at: http://www.tandfonline.com/doi/pdf/10.1080/17502977.2017.1347856?needAccess=true.

39. For example, the European Commission promised that its EURODAC database of asylum applications would be protected from other uses, until 2012 when it agreed to allow Europol and other law enforcement agencies access to it Paul Currion, "Eyes Wide Shut: The Challenge of Humanitarian Biometrics," Irin News, 25 August 2015, available at: http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics.

40. Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," Journal of Intervention and Statebuilding, 2017, available at: http://www.tandfonline.com/doi/pdf/10.1080/17502977.2017.1347856?needAccess=true.

41. James Ball & Nick Hopkins, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU Chief," The Guardian, 20 December 2013, available at http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

42. Lisa Cornish, "New security concerns raised for RedRose digital payment systems," Devex, 28 November 2017, available at https://www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619.

43. Carleen Maitland & Rakesh Bharania, Balancing Security and Other Requirements in Hastily Formed Networks: The case of the Syrian Refugee Response, 31 March 2017, available at https://ssrn.com/abstract=2944147.

44. Keith Breckenridge, "The Biometric State: The Promise and Peril of Digital Government in the New South Africa," Journal of Southern African Studies, June 2005, available at: https://wiser.wits.ac.za/sites/default/files/Breckenridge%20-%202005%20-%20The%20Biometric%20State%20The%20promise%20and%20peril%20of%20digi.pdf, p. 275.

45. Shoshana Amielle Magnet, When Biometrics Fail: Gender, Race, and the Technology of Identity (Durham, NC, Duke University Press: 2011).

46. Yante Ismail, "Fingerprints mark new direction in refugee registration," UNHCR, 30 November 2006, available at: http://www.unhcr.org/uk/news/latest/2006/11/456ede422/fingerprints-mark-new-direction-refugee-registration.html.

47. Tina Ghelli, "UNHCR pilots new biometrics system in Malawi refugee camp," UNHCR, 22 January 2014, available at: http://www.unhcr.org/52dfa8f79.html.

Annex A Methodology

This report is based on a review of the ways in which humanitarian agencies are currently using biometric technologies; relevant literature and resources, and interviews with key informants from humanitarian agencies with experience of using biometrics; biometric tech providers; and internal stakeholders within Oxfam. The research was complemented by desk research throughout the process, and took place from December 2017-March 2018.

The external interviewees were identified through The Engine Room's networks, Oxfam's suggestions, and those of the consultant we worked with on this project, Carly Nyst. A total of 24 interviewees were completed; 9 of which were Oxfam staff, and the rest external stakeholders.

Annex B Acknowledgements

We offer our sincere thanks to the many people who generously offered their time to us during this project, including people we interviewed, and those who offered feedback.

People who were interviewed for this report, and gave their consent to be included in this list, are: Rosa Akbari; Max Baldwin; Helen Bushell; Mike Clayton; Alex Pirlot de Corbion; Amos Doornbos; Dr Ted Dunstone; Diana Isiye; Sam Jefferies; Tiwonge R Machiwenyika; Mohammed Samer.

Many internal Oxfam staff gave us feedback and guidance, and Anna Kondakhchyan worked with us throughout this process and was our main point of contact at Oxfam.

Annex C
Bibliography

Taylor Armerding, "Vocal theft on the horizon," CSO Online, 16 May 2017, available at: https://www.csoonline.com/article/3196820/security/vocal-theft-on-the-horizon.html.

James Ball & Nick Hopkins, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU Chief," The Guardian, 20 December 2013, available at http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

Battista Biggio, Giorgio Fumera, Paolo Russu, Luca Didaci & Fabio Roli, "Adversarial Biometric Recognition: A review on biometric system security from the adversarial machine-learning perspective," IEEE Signal Processing Magazine, 12 August 2015, available at: http://ieeexplore.ieee.org/document/7192841/.

Kevin W. Bowyer & Samuel P. Fenker, Analysis of Template Aging in Iris Biometrics. Paper presented at the IEEE Computer Society Biometrics Workshop, June 17, 2012, available at: https://www3.nd.edu/~kwb/Fenker_Bowyer_CVPRW_2012.pdf.

Keith Breckenridge, "The Biometric State: The Promise and Peril of Digital Government in the New South Africa," Journal of Southern African Studies, June 2005, available at: https://wiser.wits.ac.za/sites/default/files/Breckenridge%20-%202005%20-%20The%20Biometric%20State%20The%20promise%20and%20peril%20of%20digi.pdf.

Lucian Constantin, "AI-based typing biometrics might be authentication's next big thing," PC World, 27 January 2017, available at: https://www.pcworld.com/article/3162010/security/ai-based-typing-biometrics-might-be-authentications-next-big-thing.html.

Lisa Cornish, "New security concerns raised for RedRose digital payment systems," Devex, 28 November 2017, available at https://www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619.

Paul Currion, "Eyes Wide Shut: The Challenge of Humanitarian Biometrics," Irin News, 25 August 2015, available at: http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics.

Charlie Ensor, "Biometrics in aid and development: Game changer or trouble-maker?" The Guardian, 22 February 2016, available at www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology.

Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., & Ortega-Garcia, J., From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems. Paper presented at the Black Hat USA, Las Vegas, 2012, available at: https://media.blackhat.com/bh-us-12/Briefings/Galbally/BH_US_12_Galbally_Iris_Reconstruction_WP.pdf.

Alan Gelb & Julia Clark, "Identification for Development: The Biometrics Revolution", Center for Global Development Working Paper 315 January 2013, available at: https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315.

Tina Ghelli, "UNHCR pilots new biometrics system in Malawi refugee camp," UNHCR, 22 January 2014, available at: http://www.unhcr.org/52dfa8f79.html.

Heidi Gilert & Lois Austin, Review of the Common Cash Facility approach in Jordan, UNHCR and the Cash Learning Partnership, October 2017, available at http://www.cashlearning.org/downloads/calp-ccf-jordan-web.pdf.

Gus Hosein & Aaron Martin, "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations," London School of Economics, December 2010, available at: http://personal.lse.ac.uk/martinak/eHealth.pdf.

IDEA, "Is the biometric data used in voter identification at polling stations," available at: https://www.idea.int/data-tools/question-view/739.

Yante Ismail, "Fingerprints mark new direction in refugee registration," UNHCR, 30 November 2006, available at: http://www.unhcr.org/uk/news/latest/2006/11/456ede422/fingerprints-mark-new-direction-refugee-registration.html.

Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," Journal of Intervention and Statebuilding, 2017, available at: http:///www.tandfonline.com/doi/pdf/10.1080/17502977.2017.1347856?needAccess=true.

Eric M. Johnson, "Red Cross launches first U.S. drone program for disasters," Reuters, 7 September 2017, available at: https://www.reuters.com/article/us-storm-harvey-redcross-drones/red-cross-launches-first-u-s-drone-program-for-disasters-idUSKCN1BI2X9.

Divij Joshi, "India's Biometric Identificiation Programs and Privacy Concerns," The Centre for Internet and Society, 31 March 2013, available at: https://cis-india.org/internet-governance/blog/indias-biometric-identification-programs-and-privacy-concerns.

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

Carleen Maitland & Rakesh Bharania, Balancing Security and Other Requirements in Hastily Formed Networks: The case of the Syrian Refugee Response, 31 March 2017, available at https://ssrn.com/abstract=2944147.

Dina Fine Maron, "Eye-Imaging ID Unlocks Aid Dollars for Syrian Civil War Refugees," Scientific American, 18 September 2013, available at https://www.scientificamerican.com/article/eye-imaging-id-unlocks-aid/.

Edin Omanovic, "Biometrics knows no borders, it must be subject to extreme vetting," Privacy International, 25 October 2017, available at https://privacyinternational.org/node/1538?PageSpeed=noscript.

Anne-Marie Oostveen & Diana Dimitrova, "Iris scanners can now identify us from 40 feet away," The Conversation, 21 May 2015, available at: http://theconversation.com/iris-scanners-can-now-identify-us-from-40-feet-away-42141.

Alex Perala, "BRIEF: The New Artificial Intelligence Explosion," Mobile ID World, 11 October 2017, available at: https://mobileidworld.com/artificial-intelligence-explosion-010114/.

Privacy International, Biometrics: Friend or Foe of Privacy?, September 2017, available at: https://www.privacyinternational.org/node/24.

Zara Rahman, "Bangladesh Will Demand Biometric Data From All SIM Card Users," Global Voices, 22 December 2015, available at: https://globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users/.

"The future of biometrics technology: Convenience or privacy," Reuters, 2 June 2017, available at: https://blogs.thomsonreuters.com/answerson/biometrics-technology-convenience-data-privacy/.

S and Marper v United Kingdom, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, 4 December 2008.

Swiss Foundation for Mine Action & CartONG, Drones in Humanitarian Action - guide to the use of airborne systems in humanitarian crises, 2 December 2016, available at: https://reliefweb.int/report/world/drones-humanitarian-action-guide-use-airborne-systems-humanitarian-crises.

UNDP Yemen, "Biometric voter registration kit testing provides glimpse into future of elections in Yemen," 2013, available at http://www.ye.undp.org/content/yemen/en/home/ourwork/democraticgovernance/successstories/biometric-voter-registration-kit-testing-provides-glimpse-into-f.html.

UNHCR, "Biometric Identity Management System," 2015, available at: http://www.unhcr.org/550c304c9.pdf.

UNHCR Innovation, "Using biometrics to bring assistance to refugees in Jordan," UNHCR Innovation Service, 30 August 2016, available at: www.unhcr.org/innovation/using-biometrics-bring-assistance-refugees-jordan/.

WFP, "First Cash Assistance to Secondary Girl Students Using Biometrics in Fata," 24 May 2017, available at: https://www.wfp.org/news/news-release/first-cash-assistance-secondary-girl-students-using-biometrics-fata.

WFP, "WFP introduces iris scan technology to provide food assistance to Syrian refugees in Zaatari," 6 October 2016, available at https://www.wfp.org/news/news-release/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu.

Woodward, J. D., Orlans, N. M., & Higgins, P. T., Biometrics: Identity Assurance in the Information Age (McGraw-Hill Osborne Media: 2003).