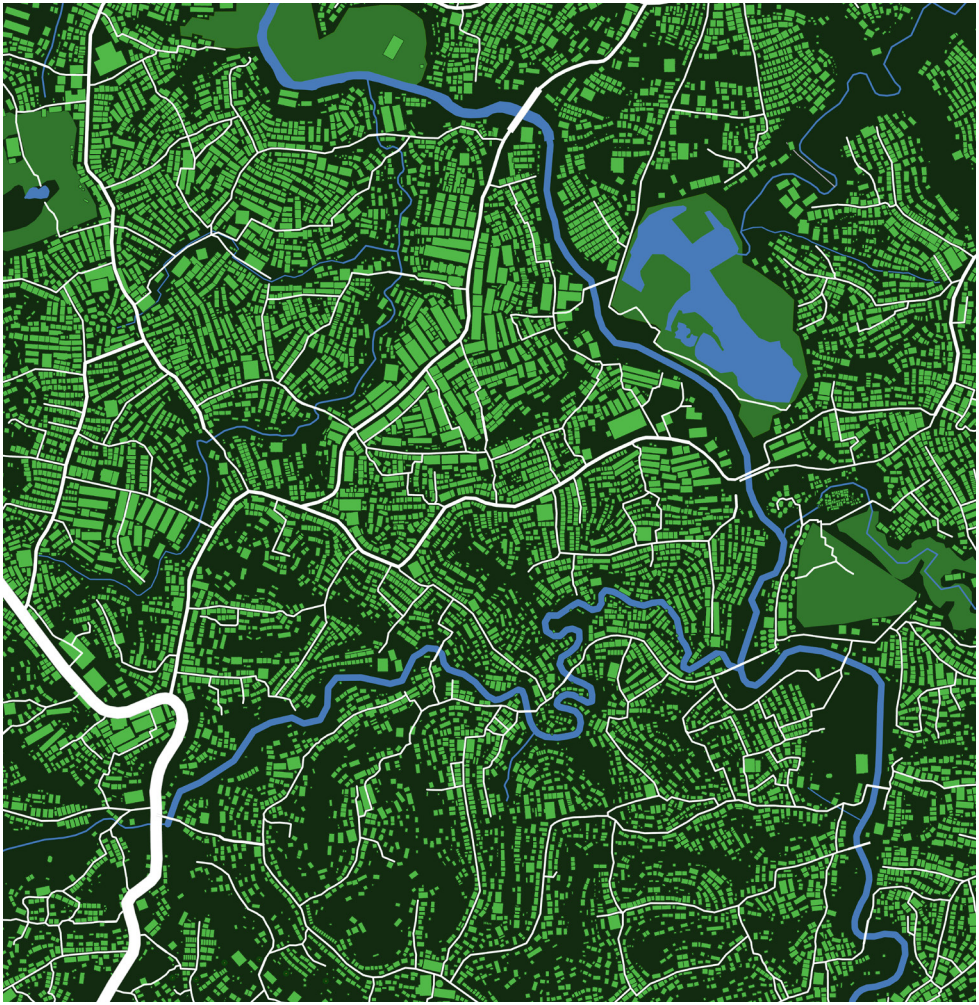
Radical Urban Lab
Volume 1 // Report 1
August 2022

Benefits and Risks of Using Biometric Technologies in Humanitarian Aid Efforts

Sofia Sanz-Kimura



Radical
Urban
Lab

The Radical Urban Lab (RUL) is part of the School of Geography and Sustainable Development, University of St Andrews, Scotland, UK.

We are: Nerina Boursinou, Chris Craig-Neil, Josh Hazelbower, Julia Lurfova, Andreas Makris, Giorgos Mattes, Rowan Milligan, Evie Papada, Vanessa Schofield, and Antonis Vradis.

Please follow us and join us in our experiment. Navigate our website to see the projects that our members are engaged in, and get in touch if you would like to find out more!

email: rul@st-andrews.ac.uk
web: rul.st-andrews.ac.uk

Cover: Map of Kutupalong refugee camp, Bangladesh.

University of
St Andrews

The research for, and writing of this report were supported by the St Andrews Research Internship Scheme (StARIS).

Contents

Foreword

Dr. Evie Papada

As a response to migration and fears regarding diminishing border controls globally, governments and international organisations increasingly experiment with digital technologies and biometrics for border and migration management. The unequivocal aim of contemporary migration management is to prevent people from reaching the global north. In this report, Sofia Sanz-Kimura spells out the risks and benefits of these technologies and their implications for humanitarian border management. Biometric border and immigration management and the widespread use of facial recognition technologies are radically transforming our traditional understanding of public spaces and freedom of movement.

The report is the final product of Sofia's engagement with the St Andrews Research Internship Scheme (StARIS) and her collaboration with Evie Papada. The Scheme offers the opportunity for undergraduate students to enhance their learning experience by working on academic research projects. Sofia's report ties into the broader aims of the Critical Understanding of Preventive Policing (CUPP) an international and interdisciplinary research project funded by Nordforsk, managed by Dr Evie Papada and Dr Antonis Vradis.

1. Introduction

Since the early 2000s, there has been a rise in the deployment of biometric technologies in humanitarian border management and refugee settings. This has come as refugee crises have exacerbated globally, with refugees, particularly from Africa, Asia and the Middle East fleeing their native countries to escape political, racial, or religious persecution, war, famine, and other disasters, and to seek safety and opportunity. In this report, I will explore the benefits and risks of the use of biometric technologies in monitoring the movement of refugees and asylum seekers. I will first briefly define biometrics and explain the history of biometrics in humanitarian aid. I will then discuss the benefits of using biometric technologies in such a context, particularly highlighting its usefulness for verification and identification, its registration speed, and its prevention of fraud. I will then consider the risks of the use of biometric technologies in humanitarian aid, particularly emphasising the issues of consent, exclusion, reliability, reusability, and data security. Finally, I will provide recommendations for future uses of biometric technologies in refugee settings.

2. What are biometrics?

Biometrics refer to any biological or physiological characteristic which is used to identify an individual or verify their alleged identity as an individual (Thomas 2005, 377). Biometric technologies are most commonly used to capture fingerprints, facial structure, and iris patterns. As technology continues to advance, however, other forms of capturing biometrics are progressing, such as voice verification, retinal scans, lip movements, and DNA (The Engine Room and Oxfam 2018, 4). As biometrics are proven to be unique to each individual, biometric systems are perceived as very reliable when determining an individual's identity.

Biometrics were first integrated into humanitarian aid efforts in the early 2000s when the United Nations High Commissioner for Refugees (UNHCR) introduced iris scans in the repatriation process of Afghan refugees in Pakistan. Since then,

biometrics have become an integral part of UNHCR's registration of refugees (Holloway, Al Masri and Yahia 2021, 14). In 2015, UNHCR officially launched its Biometric Identity Management System (BIMS) (The Engine Room and Oxfam 2018, 2). BIMS uses fingerprints as well as iris and facial recognition to identify individuals and stores all collected biometric data in a central database. The system rapidly registers and verifies the identity of refugees, ensuring that the correct individual receives aid (Lodinova 2016, 95). According to UNHCR, as of 2019, BIMS had registered over 80 percent of eligible refugees and collected 7.2 million biometric records (Kinchin 2021, 7).

Another similar system to BIMS is Eurodac, operated by the European Union (EU). Eurodac began operating in 2003 to control the mobility of refugees and asylum seekers into and within the EU. More specifically, the project sought to determine if an asylum seeker has entered the state irregularly or has asylum applications in more than one member state (Farraj 2011, 899). Under Eurodac, there is a central database which stores the fingerprints of all individuals seeking entry into any EU member state. All member states are required to send in the fingerprints of all asylum seekers to the Central Unit to determine if the fingerprint has already previously been entered into the database (Van der Ploeg 1999, 296, 298). Under the Dublin II Regulation, Eurodac is also charged with deciding which state is responsible for an asylum claim (Farraj 2011, 900). Particularly during the so-called refugee crisis, Eurodac has played a key role in identifying and classifying individuals at the EU border as well as intra-EU mobility.

Since the early 2000s, organisations and institutions such as UNHCR and the EU have relied on fingerprint scans and other biometric technologies to inform and guide their provision of humanitarian aid and mobility surveillance. As technology continues to rapidly advance, it is crucial to identify and discuss the benefits and risks of integrating such technologies into aid efforts.

3. Benefits of biometrics

As with all other technologies, there are both benefits and drawbacks of using biometric technologies. In terms of advantages, the use of biometric technologies in humanitarian settings allows for the verification and identification of refugees, a faster speed of registration, and the reduction of fraud.

Verification and identification

Verification and identification are both key to directing aid to refugees and asylum seekers. Verification involves the comparison of the biometrics of one individual to one biometric profile, which they claim will match. Identification involves when an individual's biometrics is compared to all other biometrics stored in the system to confirm their identity. Both verification and identification allow organisations to determine if a specific individual is entitled to food, housing, or whatever they claim to be entitled to.

According to The Engine Room and Oxfam, over two million refugees who flee their native countries are not identified by government documents such as passports. Thus, biometrics is often their only form of official identification. Biometrics provide them with secure identity documents, ensuring that their identities cannot be lost or stolen and giving them access to the assistance to which they are entitled. A formal ID also helps refugees get access to essential goods and services, such as food, shelter, health, education, and financial services (The Engine Room and Oxfam 2018, 6-7). The establishment of an official identity also helps establish credibility, fostering refugees' freedom of movement and independence (Kinchin 2021, 16).

Speed

Biometric technologies speed up the delivery of humanitarian assistance. The use of digital systems eliminates the time-lag which results from the authentication of paper documents (The Engine Room and Oxfam 2018, 8). Biometrics also eliminate the need for refugees and asylum seekers to register their personal information more than once. One instance when biometrics has proven especially useful in regard to speed was the process with the Common Cash Facility in

Jordan. Instead of refugees going to a bank and registering for an account in-person, UNHCR shared the data with the financial institution managing cash transfers directly. Previously, refugees also had to wait months to open an account, as they had to register with the government to obtain an identity card first (The Engine Room and Oxfam 2018, 9). The speed at which documentation and identification are provided for refugees has eliminated time-lags and sped up the registration and settlement processes.

Fraud reduction

In humanitarian aid, fraud occurs when an individual attempts to register several times with different names in order to receive more aid. Fraud puts pressure on resources and results in an inequitable and unfair distribution of essential goods and services (Farraj 2011, 915). By storing information on the unique traits of each refugee, biometrics are said to reduce the likelihood that aid goes to the wrong person or that anyone receives the incorrect amount of aid.

Though many use the claims of fraud reduction to support the use of biometrics, there is a lack of evidence regarding whether biometrics actually help to reduce fraud. One major question surrounds whether the fraud is happening by the beneficiaries receiving aid or earlier in the supply chain. Major issues in the delivery of aid tend to happen 'upstream,' with any loss or diversion of aid happening before it gets to the refugees themselves. Using biometrics only catch fraudulent attempts at the 'downstream' of the process (The Engine Room and Oxfam 2018, 8). While biometric technologies may prevent fraud on the beneficiary level to some extent, there is little data to prove that it makes any substantial difference in the greater process.

4. Risks of biometrics

Though biometric technologies have the benefits of providing fast verification and identification and working to reduce fraud, such technologies are accompanied by a myriad of risks. These risks include the lack of informed consent, the potential for exclusion, the lack of reliability, the potential of being reused by other actors,

and the risk of being lost in a security breach.

Consent

It is crucial to obtain consent throughout the process of biometric data collection. To give informed consent, an individual must be fully aware of the potential risk and understand the impact of their actions while facing no threat of harm to agree. Refugee and asylum seekers cannot be said to have given informed consent if they 1. do not know how, and for what, their biometrics will be used, protected, and shared, 2. do not understand the associated risks and consequences, and 3. are unaware of their ability to choose between participation and nonparticipation, both of which do not affect the level of aid that they receive (Holloway, Al Masri and Yahia 2021, 9). In giving consent, refugees also may fear that they will be harmed or threatened if they refuse to provide their biometrics and may also blindly agree as getting assistance is likely at the forefront of their minds (Kinchin 2021, 17).

It is often not made clear enough that having one's biometric data collected is a choice based on an adequate understanding of its use. UNHCR officers are taught how to handle individuals who are reluctant to provide biometric samples. They are told to explain why registration is important for UNHCR and discuss the consequences of refusing to register. They are not told to offer any alternative form of registration. Organisations and institutions are increasingly turning away from informed consent, instead relying on legal justifications for requiring the provision of biometrics. These legal justifications claim that data may be collected without explicit consent if handled carefully and used only for stated purposes in the best interest of the individual (Holloway, Al Masri and Yahia 2021, 30-31). It is crucial to move in the contrary and direction and require that organisations always ask for informed consent prior to collecting an individual's biometric data.

Exclusion

The use of biometric technologies also gives rise to exclusion. Sometimes, the exclusion occurs even before the technology is used. This may include when registration centres are not conveniently located or inaccessible to those with those with disabilities or when an individual has a low rate of literacy. Exclusion

may also occur depending on a refugee's religious, cultural, or social practices, such as having to wait in the same queue with both genders. Those who are already marginalized in society, such as those with diverse sexual orientations or gender identities or persecuted ethnic minorities may be reluctant to register, as they perceive it as high risk (Holloway, Al Masri and Yahia 2021, 24).

Exclusion also occurs during the process of collecting biometric data. For instance, facial recognition works better for those with lighter skin. Fingerprint scans are less reliable for those who work in hard manual or rural labour as well as the elderly, whose fingerprints are fainter. Iris scans are more accurate for those without vision impairments and those with lighter eye colour. Refugees may object to biometrics on religious grounds. In Bangladesh, there was widespread refusal by veiled Muslim women to have photos or iris scans (The Engine Room and Oxfam 2018, 10-11).

This exclusionary aspect of biometrics also raises questions about the encouragement of existing power inequalities and dehumanisation (Lodinova 2016, 97). It is difficult to gauge the effects of converting a human into a digital representation, and to assess how that may result in further discrimination. This potential for dehumanisation is risky, as most refugees are already disempowered in their relationship with humanitarian actors on who they rely on for survival (The Engine Room and Oxfam 2018, 11). Thus, biometric technologies have the capability to further foster exclusion and entrench existing power imbalances.

Reliability

Another risk of using biometric-based identification is its unreliability. Biometric technologies may return false matches. False matches are particularly prevalent in fingerprinting. False negatives occur when the system does not correctly identify a match when it should, and false positives occur when the system incorrectly identifies a match when it should not. False matches may be reduced through the increase of the pool of biometric data. Yet, this increase in data may be dangerous, as it means that more sensitive biometric data is susceptible to a breach (The Engine Room and Oxfam 2018, 9). In order to prevent false matches, the operators of the technology also require better training. Often, misidentification is a result of

the human error of the operator and their inability to match the prints of millions with complete accuracy rather than the technology itself. Yet, misidentification is very dangerous. Misidentification may pose serious harm to refugees, as they may be denied their aid or their asylum status. In extreme cases, it may also be harmful for those who are convicted of crimes based on fingerprint evidence (Farraj 2011, 936). Ultimately, biometric technologies are not always reliable and have the capacity to misidentify refugees, causing serious harm.

Reusability

The use of biometric technologies also opens up the possibility for data reusability. Data reusability refers to the re-use of biometric data by other actors for purposes other than the original intended use (Kinchin 2021, 17). It is also referred to as 'information creep.' Biometric data may be resold for profit, used by foreign governments for national intelligence and security, or used to embarrass humanitarian organisations. 'Information creep' can be especially dangerous when individuals have fled dangerous conditions in their native countries based on their political or religious beliefs, sexuality, or ethnicity (Holloway, Al Masri and Yahia 2021, 33).

Biometrics data are also sometimes used by the governments of host countries or the countries of origin for security screening. For instance, governments who host large numbers of refugees, such as Lebanon, have claimed their right to access UNHCR's central biometrics database, and other governments, such as the US, have requested the data to allegedly combat the War on Terror (The Engine Room and Oxfam 2018, 9). In order to combat data reusability, there must be more control over what data is collected and who is responsible for that data. Only necessary information should be collected, and it should be deleted once it has served its intended purpose (Holloway, Al Masri and Yahia 2021, 34).

Data security and privacy

Another major risk of using biometric technologies in a humanitarian setting is the potential for a breach in data security. Biometrics data is susceptible to being lost, stolen or sold due to hacking. Biometrics systems which rely on central databases to store biometric information, including UNHCR's BIMS, are

especially dangerous, as all biometric information could be lost with one breach.

For many refugees fleeing their native countries, privacy is of major concern. For instance, Eritrean refugees in Ethiopia and Rohingya refugees in Bangladesh have expressed concern that their biometric information would be shared with their native countries. A recent report by the Human Rights Watch claimed that UNHCR shared information with the government of Myanmar to identify individuals who would possibly be repatriated (Holloway, Al Masri and Yahia 2021, 31).

The sharing of data without consent constitutes a violation of data security. Humanitarian agencies that collect sensitive biometric data have been found to lack proper data protection, and often operate in countries which lack data protection regulations to protect data. These agencies also may prioritise the protection of different data differently based on their organisational interests. For instance, the International Organisation for Migration is more concerned with monitoring location data, and the World Health Organisation is more concerned with health data (Holloway, Al Masri and Yahia 2021, 32-33). Many organisations' promises for security remain largely untested and hypothetical.

5. Conclusion and Recommendations

In this report, I explored the benefits and risks of using biometric technologies in humanitarian border control and refugee contexts. The most notable benefits of the widespread employment of such technologies include the ability to verify and identify individuals, the speed of registration, and the alleged reduction of fraud. Risks of using biometrics to deliver humanitarian aid include the lack of informed consent, the possibility of exclusion, the potential for misidentification, the misuse of data by third parties, and the potential for a breach of privacy and data security.

From this report, it is clear that though biometric data is valuable and useful for rapid identification and subsequent delivery of aid, there is still much work to

be done. At the root is the need for further debates, analyses, and improvements on biometric technologies to ensure the security of refugees. It is important to consider on a case-by-case basis how refugees and asylum seekers would benefit from the further collection, storage, and use of their biometric information. In general, there is a greater need to put the rights and needs of refugees before that of humanitarian aid organisations and institutions and there must be greater regulations on the way in which biometric data is used to guarantee the refugees' safety and privacy. Other improvements include listening to refugees and addressing their concerns of the technologies being implemented. There should also be more discussion of inclusion and equal access, and registration methods other than biometrics should be offered as an option. Additionally, there should be more emphasis on consent and transparency regarding how data is used, where it is stored, who may access it, and with whom it is shared. As biometric technologies become more widespread and standardised in humanitarian aid efforts, it is important that those working on combating humanitarian issues find ways to improve existing systems of biometric technology while reducing the risks that they pose to refugees and asylum seekers.

References

Farraj, A. (2011). *Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers.* [online] Available at: https://iow.eui.eu/wp-content/uploads/sites/18/2013/04/07-Rijpma-Background4-Refugees-and-Biometrics.pdf [Accessed 23 May 2022].

Holloway, K., Al Masri, R. and Yahia, A. (2021). *Digital identity, biometrics and inclusion in humanitarian responses to refugee crises.* [online] Humanitarian Policy Group. Available at: https://www.calpnetwork.org/wp-content/uploads/2021/10/Digital_IP_Biometrics_case_study_web.pdf [Accessed 23 May 2022].

Kinchin, N. (2021). Technology, Displaced? The Risks and Potential of Artificial Intelligence for Fair, Effective, and Efficient Refugee Status Determination. *Law in Context*, [online] 37(3). doi:10.26826/law-in-context.v37i3.157.

Lodinová, A. (2016). Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy. *Development, Environment and Foresight*, [online] 2(2), pp.91–100. Available at: https://www.alnap.org/system/files/content/resource/files/main/34-1-101-1-10-20161201.pdf.

The Engine Room and Oxfam (2018). Biometrics in the Humanitarian Sector. [online] Available at: https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf.

Thomas, R. (2005). Biometrics, International Migrants and Human Rights. *European Journal of Migration and Law*, 7(4), pp.377–411. doi:10.1163/157181605776293255.

van der Ploeg, I. (1999). The illegal body: `Eurodac' and the politics of biometric identification. *Ethics and Information Technology*, 1(4), pp.295–302. doi:10.1023/a:1010064613240.


Radical
Urban
Lab