The biometric assemblage: surveillance, experimentation, profit and the measuring of refugee bodies

Mirca Madianou
Department of Media, Communications and Cultural Studies
Goldsmiths, University of London
New Cross, London
SE14 6NW
UK
m.madianou@gold.ac.uk

Article in press: *Television and New Media*, vol. 20, September 2019
DOI: 10.1177/1527476419857682

Abstract

Biometric technologies are routinely used in the response to refugee crises with the United Nations High Commissioner for Refugees (UNHCR) aiming to have all refugee data from across the world in a central population registry by the end of 2019. The article analyses biometrics, AI and blockchain as part of a technological assemblage, which I term the biometric assemblage. The article identifies five intersecting logics which explain wider transformations within the humanitarian sector and in turn shape the biometric assemblage. The acceleration of the rate of biometric registrations in the humanitarian sector between 2002 and 2019 reveals serious concerns regarding bias, data safeguards, data-sharing practices with states and commercial companies, experimentation with untested technologies among vulnerable people, and, finally, ethics. Technological convergence amplifies risks associated with each constituent technology of the biometric assemblage. The paper finally argues that the biometric assemblage accentuates asymmetries between refugees and humanitarian agencies and ultimately entrenches inequalities in a global context.

Keywords

biometrics, artificial intelligence, blockchain, refugees, humanitarian organisations, technological convergence.

The biometric assemblage: surveillance, experimentation, profit and the measuring of refugee bodies

> A few times a month, Bassam pushes a shopping cart through the aisles of a grocery store stocked with bags of rice, a small selection of fresh vegetables, and other staples. […] The Tazweed Supermarket, where he's shopping, is on the periphery of a 75,000-person refugee camp in the semi-arid Jordanian steppe, six and a half miles from the Syrian border. At the checkout counter, a cashier tallies the total, but Bassam doesn't pay with cash or a credit card. Instead he lifts his head to a black box and gazes into the mirror and camera at its center. A moment later, an image of Bassam's eye flashes on the cashier's screen. Bassam collects his receipt—which reads "EyePay" and "World Food Programme Building Blocks" across the top—and walks out into the noonday chaos of the Zaatari refugee camp (Juskalian 2018).

Bassam is one of the 100,000 Syrian refugees living in refugee camps across Jordan who receive aid through the United Nation's World Food Programme (WFP). Unlike traditional food distributions, or cash transfers, Bassam receives aid through a blockchain application combined with biometric technology that constitutes the WFP's *Building Blocks* scheme. Before visiting the supermarket, Bassam receives an SMS message informing him that his aid entitlement is ready to be collected. At the registered grocery store, by scanning his iris, Basam verifies his identity on a United Nations High Commissioner for Refugees (UNHCR) database, which releases an electronic payment from WFP to the merchant. WFP aims to use Blockchain to reach the 500,000 Syrian refugees in Jordan by early 2019.

Blockchain applications for humanitarian aid are part of wider developments in the field of humanitarianism. In the above example blockchain is combined with developments in biometric technologies which are now commonly used for the registration of refugee populations. Blockchain, biometrics and artificial intelligence (AI) are part of the wider trend towards digital innovation and data practices in the humanitarian field, leading practitioners to claim that big data and digital developments have catalyzed a new era of 'humanitarianism in the networked age' (UNOCHA 2013). This article raises critical questions about the introduction of biometric and blockchain applications in humanitarian operations. Rather than analysing these technologies as distinct entities I argue that they need to be understood as a technological assemblage, which includes biometrics, blockchain and AI. Instead of assuming the unalloyed benefits of biometrics and blockchain, the article observes serious risks associated with these developments are amplified as a result of technological convergence. Specifically, I argue that the technological convergence of biometrics, blockchain and AI into what I term the 'biometric assemblage' amplify the risks associated with each constituent technology. These risks, which have direct implications for the security, privacy and dignity of refugees, reproduce asymmetries between refugees and humanitarian agencies and ultimately entrench inequalities in the north – south context.

Biometric technologies have become the standard method for refugee registrations with UNCHR aiming to have all refugee data from across the world in a central population registry by the end of 2019. What the opening example suggests is that biometric data have wider applications – in this case they function as the currency for food distributions. Biometrics converge with other innovations to advance the 'digital identity' and financial inclusion of refugees (UNHCR 2018) revealing the increasing collaboration between humanitarian agencies, states and the private sector. After defining biometrics, AI and blockchain as an assemblage, the article will discern the distinct, yet overlapping logics which drive the adoption of these technologies. The paper will then review the implementation of biometric registrations in the humanitarian sector from the early 2000s until 2019. The acceleration of the rate of biometric registrations among refugee populations takes place despite the significant risks which are heightened as a result of technological convergence. After outlining the serious risks associated with the biometric assemblage, the paper will consider who benefits from biometric registrations and related 'digital identity' initiatives. The article highlights the logics of capitalism and solutionism as key forces shaping the biometric assemblage. This is illustrated in the idea of the refugee camp as a testing site for new technologies. In so doing the biometric assemblage depoliticises displacement and heightens power inequalities between refugees and humanitarian agencies.

The article is primarily based on the analysis of recent policy documents and industry reports including internal UN audit reports, which reveal the current discourses about biometrics in the humanitarian sector. The analysis of the secondary material is supplemented by ongoing empirical research on the broader topic of digital innovation and data practices in the humanitarian sector which includes 35 interviews and ethnographic fieldwork (conducted between July 2016 and January 2019) with humanitarian officers, donors, volunteers, consultants, software developers, private entrepreneurs as well as other stakeholders.[1] The purpose of the article is not to fully report on this research: the interview material is used to illustrate the notion of the biometric assemblage, the associated heightened risks, the reasons driving these developments and their implications.

The identification assemblage: biometrics, blockchain and artificial intelligence

Biometrics is a technology for measuring, analysing and processing a person's physiological characteristics, such as: fingerprints, iris, facial patterns, voice, hand geometry and DNA among others. Contemporary biometrics use digital technology, but despite the popular view that biometrics is a recent phenomenon, the desire to read identity from human bodies has a long history which can be traced to the now discredited subjects of anthropometry, phrenology and bertillonage in the nineteenth century (Magnet 2011). The biometric industry grew out of the US prison-industrial complex in the mid- to late twentieth century, which reveals the close association between biometrics and the control and disciplining of marginalized populations (Magnet 2011). The biometric industry boomed after 9/11, which represented a tremendous business opportunity (Magnet 2011, 120), signalling a 'realignment of national security interests with the profit of private companies' (Monahan 2010, 37). The sector has continued to grow and was valued at $14.4bn in 2017 with expectations to almost triple by 2023.[2]

Biometric data are used for identification and verification purposes. Identification checks a biometric record against a large database of biometric profiles (one-to-many comparison) while verification checks a live record against the entry already in the system (one-to-one authentication). Identification processes entail a higher risk of false matches than verification (The Engine Room and Oxfam 2018). Humanitarian agencies commonly use biometric data for identification purposes. One of the reasons UNHCR embraced biometric technologies was to address fraud, which requires checking a refugee biometric profile against an entire database of refugee profiles (UNHCR 2002).

Biometric identification depends on automated systems of algorithmic sorting. Biometric identification occurs largely through artificial neural networks (ANN) which employ machine learning algorithms in order to process complex data inputs and learn to imitate the function of the human brain, for example in recognising patterns or shapes (Bowyer et al. 2008; Bowyer and Burge 2016). Recognition results vary depending on the type of algorithms used for processing (e.g., segmenting), or indexing the iris scan, as well as the algorithms and input data used for training the neural networks (Bowyer et al. 2008). While it is beyond the scope of the article to include a technical discussion of neural networks, machine learning and AI are neither neutral nor objective, but depend on human decisions as well as the quality of datasets, which are always inherently incomplete (Buolamwini and Gebru 2018; Caliskan et al. 2017). AI is not just involved in the identification process, but also in the actual capturing and processing of biometric data (for example in the segmenting of the iris scan). It is for all these reasons that I argue that AI is integral to biometrics – there cannot be biometrics without AI – and why they both need to be understood as part of an assemblage which cannot be reduced to any of the constituent components.

Recently, as illustrated by the example which opened this article, biometrics have been combined with developments in blockchain, which is known as the technology behind bitcoins, but has a wider set of applications. Blockchains are distributed ledgers, or shared databases. Any participant on a blockchain network can submit and review 'blocks' of information in real time. For example, when a participant in the *Building Blocks* scheme records a new transaction, this is automatically replicated on all system nodes following biometric and algorithmic verification. The network constantly reconciles information so that all users access the most up-to-date version of the blockchain. The distributed nature of information means that even if one node is shut down, the network will not be affected. This also means that no single user can control the whole network (GSMA 2017). At the same time information cannot be deleted – new blocks can only be added. This – often praised – immutability of blockchain can have negative consequences if data entries are erroneous.

While public blockchains are better known (as they are used in cryprocurrency systems), private blockchains are also common and often preferred by humanitarian organisations as they only allow access to information to those granted permission. The WFP *Building Blocks* scheme was initially launched on a public blockchain, but scalability problems relating to speed and cost shifted the project to a permissioned blockchain (Juskalian 2018).[3]

While most existing analyses of biometrics have focused on different biometric methods (fingerprints vs iris recognition), or the biometric sector on its own (Magnet 2011; Ajana 2013) I argue that it is impossible to separate biometrics from AI, machine learning, big data and additional developments such as blockchain. I conceptualize these intersecting technologies as a biometric assemblage. Assemblage here refers to the constellation of technologies and socio-material practices that are interconnected, but not reducible to a single logic. As such the term is only loosely connected to the original meaning by Deleuze and Guattari (1987) and others across the humanities and social sciences (Anderson and McFarlane 2011; Marcus and Saka 2006). The biometric assemblage results from the convergence of a number of constituent technologies (biometrics, AI, machine learning, big data, blockchain, cloud computing as well as others) and associated practices. The notion of assemblage doesn't imply a stable or durable entity (Anderson and McFarlane 2011; Marcus and Saka, 2006). The biometric assemblage constantly evolves and is never reducible to a single technology. At the same time, we can only understand each constituent technology in relation to all other elements in the assemblage. Machine learning algorithms amplify existing risks associated with biometric measurements, storage and identification processes. Big data are used to train ANN algorithms. Blockchain-enabled cash transfers use biometric verification, which depend on algorithms. The replicability and public nature of blockchain ledgers raise questions about the privacy and protection of sensitive data, while blockchain's immutability can make an erroneous record permanent which can have severe consequences for displaced people.

The biometric assemblage does not exist in a vacuum. It is shaped and re-shaped through practices in the humanitarian and private sectors. Part of the attractiveness of the notion of the assemblage is that it encompasses material and social, human and non-human elements and processes (Anderson and McFarlane 2011). The biometric assemblage is not just a result of technological convergence; it equally depends on the social, political and economic factors in which technologies are developed and used. The next section dissects the transformations taking place in the humanitarian sector by identifying five distinct logics which are also constitutive of the biometric assemblage.

The structural transformation of the humanitarian sector: five logics

The humanitarian field has undergone significant transformations in recent years. With more than 135 million people across the world needing humanitarian assistance in 2018[4] and over 68.5 million displaced people worldwide[5] the sector faces tremendous challenges. To understand the reasons behind the enthusiastic adoption of biometric and other digital technologies and computational methods, we need to understand the developments within the sector. This section outlines five logics that represent the parallel and often conflicting agendas of different stakeholders within the aid field: humanitarian organisations, donors (typically national governments), host states and the private sector. This is one of the first attempts to develop an account that encompasses all stakeholders including the private sector, which has not received much attention in the literature despite its increasingly central role in humanitarian operations. While the following paragraphs discuss each logic separately, in practice these intersect and overlap giving rise to dynamics that contribute to the shaping of the biometric assemblage and its consequences.

The logic of accountability

The first logic concerns the ongoing demand for humanitarian reform. For years humanitarianism has been criticized for a lack of accountability to affected people and for reproducing the power asymmetries on which it is based. Interactive technologies are seen as empowering refugees to voice their concerns and hold aid organisations into account (Madianou et al. 2016). The demand for reform has driven the adoption of interactive technologies and has ultimately legitimated digital developments, including biometrics, within the sector. Biometrics are increasingly justified in the name of refugee protection and dignity in addition to improving the quality of assistance (for example, by freeing aid workers from time-consuming refugee registrations thus allowing them to focus on improving services). The logic of humanitarian reform also drives the use of biometrics in humanitarian cash transfers, which increasingly replace aid in-kind. Digital cash transfers are seen as empowering beneficiaries by giving them choice. Recent reports recommend the digital distribution of cash, which typically depend on biometric verification, for the added benefit of encouraging the financial inclusion of refugees.[6] These developments are enshrined in UNHCR's policy on 'digital identity' for all displaced people. 'Digital identity' is based on biometric data and is portable across borders in order to be used for access to jobs, remittances and banking (UNHCR 2018).

The logic of audit

One of the important structural transformations of the humanitarian sector has been the transformation of states into donors which demand evidence for the effectiveness of interventions (Krause 2014). Given the huge growth of the humanitarian sector with the global aid economy estimated at $156 billion, the pressure for audit is enormous. At the same time, the increasing marketization of humanitarianism coupled with the short cycle of funding mean that agencies constantly compete for funding, or renewal of funding for which they have to supply evidence of impact. Digital technologies – including biometrics – provide instant metrics regarding beneficiaries, distributions and other audit trails and this is one of the reasons why donors, such as the US government, actively encourage the uses of biometrics (The Engine Room and Oxfam 2008, 2). Iris scans were first introduced by UNHCR in order to address low-level fraud. A related factor is the pressure for savings and efficiency. Biometric scans are claimed to speed up registrations, which in the past involved lengthy interviews and paperwork (UNHCR 2002), while cash transfer programmes such as *Building Blocks* reduce third-party costs.

The logic of capitalism

One of the most interesting developments in recent years is the dynamic entry of the private sector in the humanitarian space. Technology companies, such as Facebook and Google, have been keen to apply some of their products during emergencies while private-public partnerships are increasingly popular. In February 2019, WFP announced a $45 million partnership with Palantir, the CIA-backed software firm known for its work in intelligence and immigration enforcement (including advanced biometrics) and alleged implication in the Cambridge Analytica scandal.[7] The WFP has been at the forefront of such partnerships through its Innovation Accelerator, which launched the *Building Blocks* programme. Biometric registrations are often outsourced to private vendors, part of the multimillion, rapidly expanding biometric industry. Private-public partnerships compel aid agencies to adopt biometric-based systems in order to integrate their systems with those of their commercial partners (The Engine Room and Oxfam 2018, 2). For private companies the involvement in humanitarian causes represents excellent branding opportunities with further potential benefits, such as increased visibility, access to data and opportunities to pilot new technologies (Jacobsen 2015). The 'digital identity' policy by UNHCR (2018) discussed earlier has been largely driven by the private sector, which explains the emphasis on entrepreneurialism and web-based business opportunities (GSMA, 2018).

The logic of solutionism

The logic of solutionism refers to the desire to find technological solutions to complex social problems. The logic of solutionism is closely linked to the logic of capitalism and the involvement of technology companies in the aid sector. The uses of data and digital technology in humanitarianism have been normalised to the extent that innovation has become synonymous with digital innovation (Madianou, in press). Given the complexity of humanitarian challenges, the desire to find solutions isn’t surprising. Problems emerge when solutions are put before the understanding of the actual problems. Technological hype, often stirred by technology companies keen to promote their latest innovation, takes precedence over the meticulous assessment of situations which may not be suited to digital interventions. The desire to find solutions may be one of the factors driving experimentation with technology in the context of emergencies (Jacobsen 2015).

The logic of securitization

States are inevitably involved in the response to displaced people. States host refugees and are keen to secure their borders as has been evident in the so-called European refugee crisis (Anderson 2014). Biometric technologies are one method through which governments aim to control borders, detect ‘anomalies’ and ensure security (Aradau and Blanke 2017) by making populations legible (Scott 1998). The logic of securitization reduces refugees to a security threat (Anderson 2014, 68). In the humanitarian context, host governments often put pressure on intergovernmental agencies such as UNHCR to share data collected in a state’s territory (Jacobsen 2015). On some occasions UNHCR conducts biometric registrations together with host states, or in some cases simply supports the hosts to carry out registrations. Such practices raise concerns about ‘function creep’, which refers to the way in which data collected for one purpose (e.g., to address fraud in aid delivery) may end up being used for an entirely different purpose (e.g., surveillance in order to combat terrorism) (Ajana 2013).

These five logics are vital for understanding the development of the biometric assemblage in the humanitarian response to displaced people. In fact, the logics are part of the assemblage, which is not only the result of technological convergence, but situated in a particular social, political and economic context. The following section, which provides a brief historical account of biometrics in the humanitarian sector, will illustrate how the intersecting logics have shaped past and contemporary developments.

Measuring refugee bodies: biometrics in the humanitarian sector

The use of biometrics has been championed by two UN Agencies, UNHCR and WFP. UNHCR began biometric registrations in 2002 when it piloted iris scans in the repatriation of over 1.5 million Afghan refugees from Pakistan (UNHCR 2002). Iris scans were introduced in order to identify 'two-timers' who sought funds 'more than once' (UNHCR 2002). If an algorithm detected that a new entry matched an already existing iris record, the claimant was refused aid. The UNHCR representative in that mission declared his trust in iris technology when he stated that as a result decisions could no longer be disputed: 'How can [refugees] argue now, *the machine can't make a mistake*.' (UNHCR 2002, emphasis added)

UNHCR turned away more than 396,000 'recyclers' between March and October 2002 out of a total 1.8 million refugees (UNHCR 2002). However, a 2-3% error rate in iris identification (which would have been common in 2002 for such a large database – see Bowyer et al 2008) suggests that up to 11,800 claimants out of the alleged 396,000 'recyclers' might have been denied aid due to an error thus questioning claims about the infallibility of machines. As Jacobsen remarks no

UNHCR report refers to the risks of false matches and the fact that error rates increase with the size of the database (2015, 64).

Following the initial pilot, UNHCR introduced biometric registrations in a number of responses. In 2010, UNHCR adopted the 'Policy on Biometrics in Refugee Registration and Verification Processes' which states that biometrics 'adds value to UNHCR identity, registration and documentation processes by providing reliable identity authentication and preventing risks of false claims, fraud and identity theft' (OIOS 2016, 1). In 2015, UNHCR launched a new Biometric Identity Management System (BIMS), in partnership with the global consulting firm Accenture,[8] to capture and store all fingerprints and iris scans from registered refugees (UNHCR 2015). By the end of 2015, BIMS was rolled out in 11 countries with 593,000 refugee enrolments and a budget of $9.6 million (OIOS 2016, 1). In 2016, the Office for Internal Oversight Services (henceforth OIOS), the UN's Internal Audit Division, conducted an audit of BIMS focusing on five locations: Chad, the Democratic Republic of Congo (DRC), India, the Republic of Congo (ROC) and Thailand (OIOS 2016). The report included interviews with key personnel, observation of the actual registrations, review of biometric data collected and other relevant documentation (OIOS 2016, 2). I will draw on the report's conclusions in the following sections.

In 2017-8, UNHCR undertook the biometric registration of the 900,000 Rohingya people who arrived in Bangladesh fleeing persecution in Myanmar.[9] This registration was conducted jointly with the Bangladesh government via a private vendor raising questions about data safeguards and function creep (Madianou, in press; Rahman 2018). In 2017, UNHCR launched a new system, PRIMES, which stands for 'Population Registration and Identity Management Ecosystem' (UNHCR 2019). PRIMES represents a clear acceleration of the rate of biometric registrations.

By 2018 more than 7.1 million people (8 out of 10 refugees registered by UNHCR) were biometrically enrolled in 60 countries. PRIMES hosted the biometric data of more than 2.4 million refugees by January 2019 while UNHCR aims to have all refugee data from across the world in a central registry by the end of 2019 (UNHCR 2019). Parallel to these developments, WFP has also intensified the use of biometrics, often in collaboration with UNHCR.

Recent industry reports on biometric enrolments highlight the benefits to refugees such as protection, dignity and economic opportunities (UNHCR 2018) compared to earlier reports which emphasized the logic of audit (fraud prevention and increased efficiency) (UNHCR 2002; OIOS 2016). PRIMES is part of the ‘digital identity and inclusion’ policy that has three objectives: a) empowering refugees through ‘web-based economic activities’ b) ‘strengthening state capacity’ and c) improving ‘the delivery of aid’ through ‘efficiency gains’, which in turn will increase ‘client satisfaction’ (UNHCR 2018). Equating identity with biometric data and financial opportunity signals that the humanitarian field has adopted the discourse of the private sector. This is particularly evident in the WFP’s interventions and notably the *Building Blocks* programme.

Risks

The risks associated with biometric technologies have been documented in the existing academic (Ajana 2013; Jacobsen 2015) and policy literature (The Engine Room and Oxfam 2018). This section argues that existing risks are amplified as a result of the technological convergence which underpins the biometric assemblage.

Bias

Although biometrics are celebrated as the perfect identification technologies, there is significant evidence against their reliability. Literature has pointed out failures at the levels of biometric enrolment (the actual measurement of body parts), data processing and data matching. For example, research confirms that fingerprints are unreliable biometric data. Elderly people, Asian women, manual workers as well as workers in the care, health or beauty sectors are reported to have faint fingerprints – the latter due to manual labour or the handling of chemicals (Nanavati, Thieme and Nanavati 2002). Even iris scans, which are hailed as one of the most reliable biometrics, are known to be affected by age and other factors (Bowyer and Burge 2016; Hollingsworth, Bowyer and Flynn 2008). Recent studies demonstrate that machine learning algorithms discriminate based on race and gender as facial recognition AI systematically fails to recognise African and female faces (Buolamwini and Gebru 2018). The above examples show that there is body discrimination in technology design (Monahan 2010). Drawing on Fanon (1986) whose term 'epidermalization' describes the internalization of inferiority as a result of racism, Browne argues that the prototypical whiteness underpinning biometrics constitutes a form of 'digital epidermalization': an imposition of race on the body through digital means (2015). Race, gender, ethnicity, class, disability and age are produced through biometric technologies. Despite the assumption that biometrics are impartial and scientific, biometric data codify existing forms of discrimination (Magnet 2011) while the discourse of science masks racist, sexist and classist practices.

Biometric errors occur not just in the enrolment and processing of refugee data, but also at the level of matching biometric records. Because neural networks run on algorithms trained on data which contain human biases (Caliskan et al 2016) biometric identifications reproduce and therefore legitimate racial, gendered and other forms of discrimination. The probability of erroneous matches increases with large samples (Jacobsen 2015, 64). While blockchain is mainly used for verification (rather than identification), which lessens the degree of algorithmic bias, its indelibility can accentuate any erroneous records as data are immutable once entered on blockchain. This can have devastating consequences for the individual concerned as their claims to aid, asylum, family reunification and safety depend on their biometric records. Although bias is not inherent to refugee biometrics, because these technologies are routinely deployed to identify 'suspect' bodies, 'the impact of technological failure manifests itself most consistently in othered communities' (Magnet 2011, 50).

Lack of safeguards

The vulnerability of biometric databases is one of the most recognised risks in the debates on biometric data in humanitarian emergencies. Potential data breaches are, of course, inherent to all digital systems. The difference with refugee biometric data is their sensitive nature: the consequences could be devastating if they end up in the wrong hands. A data breach increases the vulnerability of displaced people and the risks of their data being used for discrimination, involuntary repatriation, resettlement or further persecution. There is ample evidence of data breaches in the humanitarian sector. A connectivity project in a refugee camp in Greece was subjected to up to 80,000 malware events every week during 2015 (Maitland and Bharania 2017). In December 2017, the cloud server of 11 humanitarian agencies was hacked, potentially compromising the personal data of tens of thousands of vulnerable people (Raymond, Scarnecchia and Campo 2017). Here cloud computing is added to the biometric assemblage as the remote storage of data increases the risk of data breaches.

Perhaps most damning are the criticisms from within the humanitarian sector regarding data security practices. An internal UN audit report identified serious breaches (e.g., leaving workstations unsupervised whilst publicly accessible) in the deployment of biometric registrations across five countries in 2016, which could ‘lead to the loss or misuse of personal data of persons of concern’ (OIOS 2016, 9). Despite conversations across the sector regarding responsible data practices, there’s a conspicuous absence of clear policy on data practices and data security. The lack of policy is also reflected in wider issues regarding data sharing with governments and commercial partners.

Data sharing and function creep: surveillance and profit

A key feature of all digital data is their replicability and retrievability. Biometric records can be reproduced, shared and reused with great ease and these features are heightened by technological convergence (e.g., replicability is inherent to blockchain). Given the sensitivity of refugee data and the fragile political contexts in which biometric registrations take place, the risk of data misuse can have grave consequences. This isn’t necessarily the result of data breaches, but linked to the logic of securitization. Humanitarian organisations routinely share data with states under their cooperation agreements. All agencies including UNHCR operate under the jurisdiction of host nations, which put pressure to comply with data sharing requests (Jacobsen 2015). The internal UN audit report not only reveals the routine nature of data sharing, but also an astonishing lack of safeguards. For example, not only did the UNHCR missions share the personal data of refugees with the governments of the Central African Republic, India and Thailand, they did not ‘assess the level of data protection applied by the respective governments' nor did they obtain 'transfer agreements' (OIOS 2016, 11).

Once data is shared, UNHCR or other agencies have no power over how the data may be stored or used in the future under different governments. Biometric data sharing can facilitate surveillance and function creep whereby the original purpose of data collection is different from subsequent uses (Ajana 2013). Such concerns are heightened by the increasing interoperability of databases (Ajana 2013) and the technological convergence which underpins the assemblage. The absence of legal frameworks for data and privacy further compounds these risks.

Data sharing does not just occur with governments; private companies, which have been routinely involved in registrations since 2002, may also have access to data. As we saw earlier, the 2017-8 UNHCR-Bangladesh government Rohingya registration was outsourced to a private vendor (Rahman 2017). The agreements between UNHCR, WFP and private companies are not publicly available which precludes any meaningful accountability. UNHCR (2019) states that partners can access the PRIMES database, without details about what access is granted to commercial partners and contractors including those that provide the software or hardware for biometric measurements. On the announcement of its $45 million partnership with Palantir in 2019, WFP issued a statement 'that no access to data that provide beneficiary participation would be granted'[10] but did not mention access to metadata, which are equally sensitive and can have deleterious consequences if they end up in the wrong hands (ICRC and Privacy International 2018). In the research fieldwork which informs this article, two of my participants involved in private-public partnerships acknowledged that they were aware that data-sharing took place in the context of certain partnerships. Given the lack of public policy regarding data sharing practices opacity governs.

Ethics

Questions of ethics underpin almost every aspect of the discussion on risks so far. This section scrutinizes questions of informed consent and the protection of refugee personal data. Informed consent is particularly problematic in biometric refugee registrations as opting out isn't a realistic option. Refusing to register with a humanitarian agency is to refuse aid – something displaced people can hardly afford. Only those registered can be on distribution lists. The lack of alternatives for displaced people (as work and other opportunities are typically closed to them) can turn consent into coercion. The UN audit report confirms that the level of information provided to refugees was inadequate (OIOS 2016). The report is particularly critical with regards to whether persons of concern had been informed about the use of their data by government or third parties (for example, the vendor companies).

> In four out of the five country operations reviewed, OIOS observed that the level of information provided to persons of concern during the biometric registration was below the standards required by [UNHCR] policy. There were also inconsistencies in the information provided, particularly regarding the access to the data by third parties. […] There was no evidence that persons of concern were informed of their rights and obligations […] (OIOS 2016, 10).

The infinite replicability of data through blockchain raises further concerns about data ownership and people's 'right to be forgotten'. It is not clear whether

Building Blocks users are made aware how their data are replicated in the blockchain system. Given bias, data breaches and function creep are heightened as a result of the assemblage, the imperative for meaningful consent is stronger than ever.

Digital identity: who is it for?

The above discussion confirms that the already existing risks are amplified as a result of the technological convergence which underpins the assemblage. So what explains the acceleration of the rate of biometric registrations? Recall that UNHCR aims to have all refugee data from across the world in PRIMES by the end of 2019.

If we return to the five logics outlined earlier in the chapter, we see that in combination they all explain the present acceleration of biometric registrations. Some logics prevail over others. The introduction of iris scans by UNHCR in 2002 in order to identify low-level fraud by ‘recyclers’ was driven by the logic of audit. This was compounded by the demand of clear audit chains by donors (states). However, in reality the real problems with fraud are ‘elsewhere in the system’ and typically in the supply chain of aid distribution where potential gains can be greater (The Engine Room and Oxfam 2018, 8). One of my interviewees wondered if identifying a proportionately small number of ‘two-timers’, justified the enormous investment in biometric technologies. Although there are legitimate questions regarding fairness to other persons of concern, dealing with ‘two-timers’ doesn’t seem a compelling explanation for the sweeping scale of biometric registrations. The fact that the OIOS report found that only one of the five missions where BIMS was deployed in 2016 actually used biometrics for identification during distributions suggests that audit trails aren’t strictly observed (8). Biometric registrations carried on regardless of the fact that they weren't needed for aid distributions. If biometrics weren't used for audit what purpose did they serve?

Although UNHCR reports increasingly promote the value of biometric registrations for the benefit of refugees, it is hard to see how the biometric assemblage is driven by the logic or humanitarian accountability. References to refugee empowerment linked to 'digital identity' policies appear in the late 2010's, well after the generalized adoption of biometric registrations. It appears that the logic of accountability justifies biometrics, rather than explains their widespread implementation. The logics of securitization and capitalism on the other hand are certainly strong drivers. The OIOS and other reports discussed in previous sections confirm that data sharing occurs with host states and other parties. The proliferation of private-public partnerships and the involvement of the lucrative biometric sector suggest the presence of strong business interests. The logic of capitalism acquires further momentum when examined in combination with the logic of solutionism. Technological hype is a powerful force behind the rise of the biometric assemblage.

Solutionism, Technological Hype and Experimentation

The logic of solutionism is particularly evident in the *Building Blocks* example which runs on blockchain – the most hotly anticipated technological innovation during my 2018 fieldwork. This illustrates how the assemblage results from both technological convergence and particular social, political and economic logics. New technologies such as blockchain are added to the assemblage because of the prevailing hype, while in turn the renewed assemblage generates further enthusiasm and strengthens the logics of capitalism and solutionism. Listen to one of my interviewees from the humanitarian sector:

> 'Two years ago nobody in the sector was talking about blockchain. […] Now you go to meetings and you get people saying we want to try something with blockchain. And then you probe it a little bit and they don't really understand what blockchain is. […] They just know it's an innovation […] so they want to give it a try. So this is a case when a specific technology is perceived as innovative, it becomes a cover for things that don't necessarily need that technology to be done. There are a lot of ways in which you can use a blockchain, but blockchain isn't the only way of doing those things. There are other distributed databases. There are other modes of encryption. You don't have to use blockchain to get the benefit of those. But because blockchain has a high profile, because blockchain is at the peak of the Gartner hype cycle, that's what people focus on'.

This comment is echoed by Robert Opp, head of Innovation at WFP who admitted that the *Building Blocks* distribution 'could also be carried out with a simple spreadsheet. [*Building blocks*] is not the endpoint; this is the beginning for us'.[11] This quote begs the question: what was the purpose of building a biometric verification system for half a million people and have it run on a little tested technology such as blockchain? If this was nothing but a massive experiment or pilot to test technological solutions for potential efficiencies, what were the safeguards for the 500,000 refugees whose data were used as currency? What if the untested technology suffers a major data breach? If *Building Blocks* was a pilot why wasn't the sample smaller and the project tested on a less sensitive population – such as European citizens who are normally not in fear of persecution if their data are leaked? But then, such a pilot would not have been permitted in Europe under GDPR legislation.

Treating the refugee camp as a laboratory has a long history that can be traced back to colonial regimes. Elsewhere I argue that digital innovation in emergencies is a form of value extraction, which I term technocolonialism (Madianou, in press). Jacobsen similarly highlights the experimental character of biometric registrations where 'the risk of experimentation failure is outsourced to the global periphery' (Jacobsen 2015, 31). The discourse of experimentation is evident in article headlines such as Wired's 'How refugees are helping create Blockchain's brand new world'[12]. As one of my interviewees remarked: 'No one would write an article about a well-written database, whereas Blockchain can make the biggest impact'. Whilst several of my humanitarian interviewees were critical of the prevalence of solutionism, that didn't stop the drive for experimentation. As one interviewee put it: 'refugees shouldn't be the first population to experiment on, they should be the last'.

It becomes apparent that 'digital identity' policies aren't about refugees after all; they are part of an experiment for the ultimate benefit of technology companies and other stakeholders. Digital identity is a neoliberal project that promises freedom and economic development, whilst contributing to systems of migration control and the accumulation of capital. Biometrics were already widespread as a result of the logics of audit and securitization. The logics of capitalism and solutionism have accelerated the implementation of the biometric assemblage while the logic of accountability provides a cloak of legitimacy: who doesn't want identity after all? The contrast here is between 'digital identity' as a neoliberal project and the actual constitution of biometric subjectivities.

Conclusion

The rate of biometric registrations has accelerated with UNHCR aiming to have all refugee data collected in the PRIMES registry by the end of 2019. Biometric technologies are here understood as part of a larger technological assemblage that includes AI, machine learning, blockchain among others. Technological convergence amplifies risks associated with each technology: for example, the immutability of blockchain, which in other contexts may be a desirable feature, can have disastrous consequences in volatile situations if records are erroneous. AI and machine learning can amplify the existing bias within biometric measurements. Such mistakes can have devastating consequences for displaced people, who are already living in precarity. While biometrics are deployed in the name of transparency – to make populations legible and traceable, their operations remain opaque. Just like in all forms of automation (Eubanks 2018) algorithms and AI resemble a black box (Pasquale 2015). Their operations are concealed, but their consequences, when mistakes are made, are felt in very tangible ways.

The biometric assemblage isn't just a result of technological convergence; it equally depends on the social, political and economic contexts in which technologies are developed and used. The article has identified five intersecting logics which reflect wider transformations within the humanitarian sector and explain the enthusiasm behind the biometric assemblage. The analysis of biometric registrations between 2002-2019 revealed that the *logic of humanitarian accountability*, whilst contributing to the legitimation of biometrics, is often trumped by other logics such as the *logic of audit.* The latter results from the increasing pressure by donors to demonstrate the effectiveness of interventions through clear audit trails. While biometric registrations were initially implemented to combat low-level fraud, our analysis showed that audit trails were often ineffective. Still the logic of audit explains the pervasive demand for efficiencies, which are claimed to be enabled by biometric registrations.

States also champion biometrics as part of the desire to make populations legible to them and to control the border from perceived 'undesirables'. The *logic of securitization* is evident in the data-sharing between UNHCR and host governments. Further, biometrics reveals the privatization of the humanitarian sector as registrations are typically outsourced to vendors. The biometric assemblage is part of a lucrative industry sector driven by the *logic of capitalism* and profit. The logic of capitalism is also present in the branding opportunities humanitarian emergencies offer as well as the conflation between biometric registrations, digital identity and economic opportunity, which has now trickled into humanitarian policy documents. By reframing political problems in line with business objectives (as is evident in the neoliberal logic of the camp as a place of opportunity), private sector initiatives depoliticize displacement. Crucially, the logic of capitalism is combined with the *logic of solutionism* as is evident in the ways in which the biometric assemblage is used to experiment with new technologies and platforms among the most vulnerable populations. The logics of audit, securitization and capitalism override the logic of humanitarian reform which appears merely to legitimate the acceleration of biometric registrations through 'digital identity' policies.

The risks are significant and accentuated as a result of the technological convergence behind the assemblage. Biometric data and algorithms codify discrimination and compound existing inequalities. Further risks include the lack of data safeguards and ethical concerns given the lack of meaningful consent when refugees are essentially asked to choose between aid or their data privacy. The replicability of data is heightened as a result of technological convergence while data reusability through sharing agreements with states raises concerns about function creep whereby subsequent uses exceed the original remit of 'registration'. Risks include surveillance, discrimination and forced repatriation among others. There are finally ethical concerns about experimentation and the potential monetization of biometric data.

Ultimately, the biometric assemblage accentuates power inequalities in the global context. 'Digital epidermalization', the imposition of race through algorithmic practices of measuring and matching (Browne 2015), contributes to the enduring legacies of colonialism through which we can understand contemporary migration crises (De Genova 2016). While power asymmetries are immediately visible in refugee registrations, I argue that they are also present in the seemingly more empowering experience of 'shopping' through biometric data. The *Building Blocks* case can be seen as a gamified version of the logic of the camp – whereby the refugee submits their data – without knowing how these will be used and without the option to refuse – in order to be eligible for aid. The *Building Blocks* example exemplifies neoliberal humanitarianism as refugees are imagined as entrepreneurs with 'digital wallets', 'digital identities', ready to start a business, while the camp is rebranded as a place of opportunity.

Yet the reality is rather different. Whilst acknowledging refugee agency, the persistence of power asymmetries is impossible to ignore. The biometric assemblage is part of the digital systems of migration management, which control refugee mobility by constituting new types of traceable, 'digital bodies' which are open to additional forms of intervention and surveillance (see also Jacobsen 2015). While refugee digital body parts travel through digital systems and databases, the actual physical bodies are stuck in camps for years. If refugee data are reused or otherwise exploited, this contrasts with any actual benefits for the data owners. The digital, traceable body is a liminal body as it invites the intervention of the border in perpetuity. Despite acts of resistance, these power asymmetries are hard to reverse. Rather than being a solution, the biometric assemblage becomes part of the problem of displacement and inequality.

References

Ajana, Btihaj. 2013. *Governing through Biometrics*. London: Palgrave.

Anderson, Ben and Colin McFarlane. 2011. "Assemblage and Geography." *Area*, 43(2): 124-127.

Anderson, Ruben. 2014. *Illegality Inc. Clandestine Migration and the Business of Bordering Europe*. Berkeley: University of California Press.

Aradau, Claudia and Tobias Blanke. 2017. "Governing Others: Anomaly and the Algorithmic Subject of Security." *European Journal of International Security*, 3 (1): 1–21. doi:10.1017/eis.2017.14

Bowyer, Kevin and Mark Burge, eds. 2016. *Handbook of Iris Recognition*. London: Springer-Verlag.

Bowyer, Kevin, Karen Hollingsworth and Patrick Flynn. 2008. "Image Understanding for Iris Biometrics: a survey." *Computer Vision and Image Understanding,* 110 (2): 281-307.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC.: Duke University Press.

Buolamwini, Joy and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning*, 81: 1-15.

Caliskan, Aylin, Joanna Bryson, and Arvind Narayanan. 2017. "Semantics Derived Automatically from Language Corpora Contain Human-like Biases". *Science*, 356 (6334): 183–186.

De Genova, Nicholas. 2016. "The European Question: Migration, Race and Postcoloniality in Europe." *Social Text* 34 (3): 75-102

Deleuze Gilles and Felix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

Eubanks, Virginia 2018. *Automating Inequality. How High-tech tools Profile, Police, and Punish the Poor.* New York: St Martins Press.

Fanon, Frantz. (1952) 1986. *Black Skin, White Masks*. Translated by Charles Lam Markmann. London: Pluto Press

GSMA. 2017. Blockchain for Development. London: GSMA.

Hollingsworth, Karen, Kevin W. Bowyer and Patrick J. Flynn 2008. "Pupil dilation degrades iris performance." *Computer Vision and Image Understanding*, 113: 150-157.

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

International Committee of the Red Cross (ICRC) and Privacy International (2018) The Humanitarian Metadata Problem: Doing No Harm in the Digital Era. Last accessed 23 February 2019 https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

Juskalian, Russ. 2018. Inside the Jordan Refugee Camp that Runs on Blockchain. *MIT Technology Review*. 12 April 2018. Last accessed 3 February 2019 https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

Krause, Monika. 2014. *The Good Project*. Chicago, IL: Chicago University Press.

Madianou, Mirca. in press - 2019. "Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises". *Social Media and Society*

Madianou, Mirca, Jonathan Ong, Liezel Longboan and Jayeel Cornelio. 2016. "The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery." *Journal of Communication* 66 (6): 960-981. DOI:10.1111/jcom.12258

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

Maitland, Carleen and Rakesh Bharania. 2017. "Balancing Security and Other Requirements in Hastily Formed Networks: The Case of the Syrian Refugee response." Last accessed 20 February 2019 SSRN: http://dx.doi.org/10.2139/ssrn.2944147

Marcus, George E. and Erkan Saka. 2006. "Assemblage." *Theory, Culture & Society,* 23 (2-3): 101–9

Monahan, Torin. 2010. *Surveillance in the Time of Insecurity*. New Brunswick, NJ: Rutgers University Press.

Nanavati, Samir, Michael Thieme and Raj Nanavati. 2002. *Biometrics: Identity Verification in a Networked World*. New York: Wiley

Office for Internal Oversight Services (OIOS). 2016. Audit of the Biometric Identity Management System at the Office of the United Nations High Commissioner for Refugees. Report 2016/181. Geneva: United Nations.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA.: Harvard University Press.

Rahman, Zara. 2017. Irresponsible Data? The Risks of Registering the Rohingya. Irin, 23 October 2017, last accessed February 23rd 2019 https://www.irinnews.org/opinion/2017/10/23/irresponsible-data-risks-registering-rohingya

Raymond, Nathaniel, Daniel Scarnecchia and Stuart Campo. 2017. Humanitarian Data Breaches: The Real Scandal is Our Collective Inaction. *Irin*. Last accessed 20 February 2019 https://www.irinnews.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction

Scott, John. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

The Engine Room and Oxfam 2018. *Biometrics in the Humanitarian Sector*. Last accessed 14 February 2019 https://theengineroom.org

United Nations High Commission for Refugees [UNHCR]. 2019. *Data of Millions of Refugees now Securely Hosted in PRIMES.* Last accessed 23 February 2019 https://www.unhcr.org/blogs/data-millions-refugees-securely-hosted-primes/

United Nations High Commission for Refugees [UNHCR]. 2018. *UNHCR Strategy on Digital Identity and Inclusion.* Geneva: UNHCR. Last accessed 23 February 2019 https://www.unhcr.org/blogs/wp content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

United Nations High Commission for Refugees [UNHCR]. 2015. *Biometric Identity Management System: Enhancing Registration Data Management.* Geneva: UNHCR. Last accessed 14 February 2019 https://www.unhcr.org/550c304c9.pdf

United Nations High Commission for Refugees [UNHCR]. 2002. *Afghan Recyclers Under Scrutiny of New Technology.* https://www.unhcr.org/news/latest/2002/10/3d9c57708/afghan-recyclers-under-scrutiny-new-technology.html

United Nations Office for the Coordination of Humanitarian Affairs [UNOCHA]. 2013. *Humanitarianism in the Network Age*. OCHA policy and studies series. New York: OCHA

Notes

[1] Fieldwork for this ongoing project has taken place in London, New York, Athens and Berlin with further interviews planned in Geneva and the US. Several participants in overseas missions were interviewed via videocalling platforms. All interviews were anonymized.

[2] https://www.grandviewresearch.com/industry-analysis/biometrics-industry

[3] The *Building Blocks* scheme uses the parity Ethereum proof-of-authority (PoA) consensus algorithm (Juskalian 2018).

[4] UN OCHA Global Humanitarian Overview 2018 https://interactive.unocha.org/publication/globalhumanitarianoverview/

[5] "UNHCR figures at a glance" https://www.unhcr.org/figures-at-a-glance.html

[6] See the recommendations of the High Level Panel on Humanitarian Cash Transfers: https://www.odi.org/projects/2791-high-level-panel-humanitarian-cash-transfers

[7] "New UN deal with data mining firm Palantir raises protection concerns". https://www.irinnews.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp

[8] https://www.accenture.com/us-en/success-unhcr-innovative-identity-management-system

[9] https://www.unhcr.org/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html

[10] https://insight.wfp.org/a-statement-on-the-wfp-palantir-partnership-2bfab806340c

[11] https://www.forbes.com/sites/astanley/2018/06/09/u-n-official-defends-refugee-voucher-program-even-though-it-doesnt-require-blockchain/#51b83e071f66

[12] https://www.wired.com/story/refugees-but-on-the-blockchain/