13 *UNHCR and Biometrics*
Refugees' Rights in a Legal No-Man's Land?

MARIE-EVE LOISELLE

Introduction

For a long time, the border was the site where states have controlled foreigners' access to their territory. In the last few decades, however, governments have increasingly sought to relocate away from their territorial limits border practices that serve to identify, filter, and, if necessary, prevent crossings into their national space. Digital innovations, including biometric technologies, are now offering new opportunities for making migrants legible from afar, miles away from "the legal gates of admission" (Shachar, 2020b: 9). For instance, it is common for states to collect travelers' biometric data at the time of application for a visa in the country of origin. Yet the turn to emerging technologies is not the preserve of governments. The United Nations Refugee Agency (UNHCR) has been using digital technologies, including biometrics, for several decades. For UNHCR, biometrics, first deployed in the Middle East, is becoming an essential tool in accounting for the populations under its protection. This chapter explores this development and the associated risks for refugees. The first part surveys the emergence of states' practices toward the deterritorialization of border controls with considerations for the enabling role of biometrics and digitization in that process. Then it demonstrates how the use of biometrics by UNHCR maps onto these states' practices. The second part considers the consequences of UNHCR's practices surrounding the biometric registration of refugees. It discusses the risks posed by the collection of biometric data in the refugee context before assessing how the institutional and structural conditions in which UNHCR operates, especially with regard to consent, accountability mechanisms, and legal safeguards, may undermine refugees' control over their data.

1 Border Control, Identification, and Digital Technologies

The assumption that the border marks the beginning and the end of a state's effective sovereignty over its territory is deeply entrenched in the Westphalian sovereignty model. This is why governments worldwide have identified borders as the locus of control over movement in and out of their respective space of authority. In that respect, the border and its associated administrative practices of admission and exclusion work like a sieve to filter beings, matters, even ideas, letting in what is good and rejecting the rest following a subjective assessment about national interests. Yet the border–control nexus is only one aspect of a larger paradigm of sovereign authority. Indeed, states increasingly opt to multiply the locations of (border) control practices at various sites beyond and within their territories. Scholars of border studies have articulated the modalities of an emerging mobility regime that aims to screen people on the move as early as possible into their journey. Ayelet Shachar explains how states, relying on legal fictions, are redrawing the spatial limits of their authority to control migration and movement through the 'shifting border' (Shachar, 2020b). As she describes, when screening migrants, states project their border practices as far outward as possible from the state territory. By contrast, when assessing the validity of rights claims, that same fictional legal border retracts back within the state territory.

Practices of "remote border control" are not new. The transatlantic visa system developed in the twentieth century was an early form of migration control at a distance (Zolberg, 1997: 308–309). What is changing is the sweeping scale at which external controls are now deployed and the granular nature of the information collected about people afforded by technological innovations. Biometric technologies are becoming the new norm for identifying and screening people. Instead of using biographic data, such as name, nationality, and gender, biometrics uses the body (e.g., fingerprints, iris scan, facial recognition, gait, DNA) as a source of information and token of identification. The data produced in such a way are distinct from other forms of personal information. They are not information about a person but from a person (Smyth, 2019: 50). They constitute the behavioral and biological material or characteristics of the individual from which they are collected.

Despite being part of someone's make-up, biometric data are severed from the body. Through its datafication, the subject is disembodied. Parts of its unique and unalterable composite travel across space unencumbered by a constructed cartography of sovereign powers. Yet if data's potential for mobility knows few limits, the "unterritoriality" of data (Daskal, 2015) does not signify the end of territoriality. On the contrary, datafication serves territorial practices of control by making possible what was before inconceivable: the assessment of someone's identity when she is at a distance, far from the state's territory. Rather than the demise of the border widely forecasted in the 1990s, data and digital technologies enabled the erection of a more insidious digital border, where only the elements of the person's identity necessary for assessing the validity of a claimed right to enter are allowed to travel.[1] These data include immutable biometric features nearly universal to all human beings yet unique to each individual, which makes them highly accurate and reliable for identification purposes. They are easily deployable, transferable, and duplicable to different contexts and localities, such as airports, land borders, and refugees' camps when needed (Smyth, 2019: 51). What's more, when combined with other forms of data, the breadth of knowledge they may impart about a person's past and present – perhaps even her future – multiply.

Hence, a key attribute of the digital border is that it makes proximity expandable without undermining legibility. The physical presence of the person seeking entry into foreign territory – a requirement of border control in an analogue world – becomes superfluous. Instead, it is the markers of one identity that travel through servers and databases to reach the authorities of the potential host country to offer a reading of the risks and benefits of her entry. This physical distance, in turn, appeases acute fears underpinned by the perceived threats posed by immigration and transnational violence – what Ronen Shamir (2005) coined the "paradigm of suspicion" – by maintaining suspect individuals at bay. Distance is compelling for another reason. Indeed, it shields a state from its obligation of nonrefoulement provided for in the

[1] Legal cartographies of rights are not only (re)drawn by sovereign and digital borders. As Anna Jurkevics notes in Chapter 11, the borders that carve out special economic zones (SEZs) from state territory constitute economic "private borders" that sever a space from a state's jurisdiction, evading democratic rule for the benefits of private interests.

1951 Refugee Convention and other protections found in international human rights law instruments, which, as Dana Schmalz explains in Chapter 4, require the refugee's physical presence or proximity to the state territory. The digital border is therefore key to foreclosing the required proximity for right's claims and becomes increasingly efficient at doing so as the number of foreigners' databases, identity management systems, and biometric identity documents increases.

For these reasons, states employ biometrics for identification purposes in ePassports. These collect the bodily attributes of foreigners in databases such as Eurodac in Europe and US-VISIT (now the Office of Biometric Identity Management) in the United States. National identity management systems using biometric and biographical data are also growing in popularity. States increasingly rely on them to ascertain welfare assistance and public service rights. When linked to travel documents, these databases have the potential to deliver on both fronts of the shifting border described by Shachar, screening those standing outside the gates of admission as well as those already in. As such, biometric technologies are allowing states to expand and rearticulate their political authority over their territory, further reinforcing their monopoly on the "legitimate means of movement" (Torpey, 2018). Yet states are not the only proponents of identity management systems. A host of international bodies have developed their own identity management architectures supported by biometrics data – or promoted their deployment – including the UNHCR.

2 UNHCR's Turn to Biometric Technologies

UNHCR was an early adopter of biometric technologies when it undertook in 2002 to collect the iris scans of all Afghan refugees returning to Afghanistan from Pakistan with its assistance to prevent multiple claims by the same person (Kessler, 2003). The Afghan experience was a precursor to UNHCR's Population Registration and Identity Management EcoSystem (PRIMES), launched in 2015. PRIMES is a digital platform that aims to bring together the host state's civil registry, UNHCR's registration identity management databases, as well as several digital tools, available or planned, to connect UNHCR, its partners, and refugees. A key component of PRIMES is its Biometric Identity Management System. This biometric database contained the fingerprints and iris scans of 15.7 million individuals at the end of

2023, up from 8.8 million in 2019 (United Nations High Commissioner for Refugees [UNHCR], 2020: 9; 2023). As the Agency explains, the biometric registration of refugees has several benefits. It facilitates UNHCR's efforts to address the needs of displaced populations worldwide. Biometrics enrolment can reduce fraud, cut down processing time, and provide a more accurate overview of the refugee populations. It also provides proof of identity for affected populations in the absence of formal identification documents and gives them timely access to services and resources in innovative ways.

Broader political and structural factors have contributed to UNHCR's turn to biometrics. As legal anthropologist Sally Engle Merry explains, the audit and performance culture typical of the corporate world has spread to global governance (Merry, 2011: S84). Since the late 1980s, a result-based management paradigm has forced organizations to demonstrate the "value for money" of their programs (Sandvik, 2016: 138). Agencies such as UNHCR must now quantify their achievements and demonstrate their efficiency to secure evidence-based funding. In that context, biometrics provides the raw material for data production and the development of statistical measures about beneficiaries, aid distribution, and other indicators of performance used to allocate funding (Madianou, 2019: 586). The importance of biometrics as a tool to measure the Agency's effective use of its budget is reflected in UNHCR's Grand Bargain commitment to "expand the use of biometrics for refugee registration to a total of 75 country operations by 2020" in order to reduce duplication and management costs. The influence of donors in the Agency's adoption of biometric technologies for registration is also evident in its statement that iris scanning was "important in securing the support and confidence of donors" (Troger & Tennant, 2008: 3).

Another factor that helps explain the development of UNHCR's digital identity architecture is the trend toward the securitization of migration, which intensified at the turn of the twenty-first century, along with the growing reliance on biometric data for filtering the movement of suspicious populations. Following September 11, 2001, suspicion and hostility against refugees rose to unprecedented levels (Betts, Loescher, & Milner, 2011: 62). This prompted northern countries to adopt a wave of measures to curb arrivals, cut down resettlement programs, and contain refugees in their region of origin. Host countries in the Global South grew equally concerned about the perceived security threats posed by large influxes of refugees (Betts et al.,

2011: 60). In this context, UNHCR has had to balance its responsibility for protecting refugees with pressure from host and resettlement countries to enhance the quality of the data it holds about refugees and share that data with them. On the one hand, UNHCR, as an "invited guest," must try to accommodate requests from host governments authorizing it to operate within their territory (Wilde, 1998: 113). On the other, the Agency cannot ignore donor states' demands for better data on refugees and spending, with voluntary contributions representing 85 percent of its budget (UNHCR, 2022a).

UNHCR's response to states' concerns has been to step up the biometric registration of refugees. It also answered the call of northern countries for improved biometric data-sharing in the resettlement process. For instance, in 2004, the US Department of State noted in a report that "assurance of positive identification via biometrics throughout the refugee assistance process and especially the resettlement process would carry enormous advantages in the post-September 11 climate" (United States Department of State, 2004). The process was officialized in a 2019 Memorandum of Understanding (MoU) between UNHCR and the US Department of Homeland Security (DHS) for the sharing of refugees' biometric data. Under the MoU, UNHCR agrees to transfer directly into the DHS Automated Biometric Identification System the biometric and associated biographic data of refugees it refers for resettlement in the United States. As the DHS recognizes, under the MoU, the United States could come into possession of data from individuals who will never set foot in the United States for various reasons (e.g., rejection or withdrawal from the resettlement process).

Finally, the adoption in 2015 of the Sustainable Development Goals and its target 16.9 calling for a "legal identity for all by 2030" has contributed to the expansion of digital identity management systems into the humanitarian space. The appeal of legal identity is premised on the assumption that the state's recognition of an individual's existence – and evidence of such recognition – is necessary to access social services and the enjoyment of rights. Since its adoption, target 16.9 has been a catalyst for technology-based solutions to legal recognition that use biometric technologies for proof of identity. This is reflected in UNHCR's Strategy on Digital Identity and Inclusion, which sets the objective of "achieving the digital inclusion and digital identity of refugees, stateless persons, and other forcibly displaced persons." With its "state of the art biometrics," the Agency explains, PRIMES can make a

meaningful contribution to target 16.9, noting that "'[l]eaving nobody behind' applies to all countries and sectors of society. Even to the digital space." The Global Compact on Refugees reflects this commitment when it provides that UNHCR "will contribute resources and expertise to strengthen national capacity for individual registration and documentation" (Sköld, 2021), including digitalization, biometrics, and the collection and sharing of quality registration data. Narratives describing these initiatives focused on digital inclusion and better services to refugees. Yet underneath these lofty goals another logic appears to be at play, which speaks to the aspiration of certain states to create a spatial distance between their shores and individuals seeking refuge without giving up on their capacities to scrutinize and screen them.

Hence the motivations – and justifications – for the use of biometric technologies are twofold. On the one hand, and perhaps most evidently, the datafication of refugees is seen by state actors as the most reliable tool for the identification of people crossing their borders. As UNHCR's identification management system evolves, it will likely become more efficient in tracing refugees' journey from registration onward. This potentiality explains why such a form of indelible identification has been compared with the tagging or tattooing of populations (Agamben, 2004). On the other hand, proponents of biometric registration are discursively constructing it as necessary for someone's recognition as a person before the law through a legal identity agenda, emphasizing values such as justice, equality, and dignity. Legal identity, supported by biometrics and digital platforms, is cast as an empowering instrument that holds the potential for opening access to humanitarian aid and services. Yet it is important not to fall prey to an instrumental use of the language of human rights. As Martin Krygier (2006: 136) warned, "hurrah words," such as democracy, the rule of law and human rights, are endowed with virtue making it difficult to challenge any proposals pertaining to secure these goals. Nonetheless, we must examine what may hide underneath the rhetoric and consider how the means proposed to achieve these goods can deliver on their promise of empowerment.

3 Challenges Posed by UNHCR's Biometric Practices

Most citizens and travelers perceive the collection of their personal data with unease about being subjected to identification practices long associated with crime control (Gilman, 2012: 1394). This said,

apprehension about data collection is soothed by the apparition of smart travelers' programs that associate biometric with privileged status. However, for refugees and other groups with precarious legal status, the collection of biometrics holds no such benefits and may result in harms that have no equivalent in different contexts. One risk refugees confront is that their country of origin may access UNHCR registration data without their knowledge or consent. The risk is not theoretical. Human Rights Watch (HRW) notes that between 2018 and 2021, the Bangladeshi government transferred the biographical and biometric data of 830,000 Rohingya refugees to the Myanmar government to assess their eligibility for repatriation. The data transferred had been collected during a joint UNHCR–Bangladeshi registration exercise. Testimonies by Rohingya refugees have since been collected to the effect that they were unaware their data could be shared with Myanmar. One individual explained to HRW that although he was informed of the potential transfer, he felt obliged to agree in order to access aid: "I could not say no because I needed the Smart Card and I did not think that I could say no to the data-sharing question and still get the card" (Human Rights Watch [HRW], 2021). Although UNHCR insists it did not violate its policy on personal data, the incident raises doubt about the feasibility of obtaining free and informed consent in humanitarian contexts.

Another risk is that biometric data be used for initially unforeseen purposes or have unexpected effects on individuals, sometimes even beyond the refugee population. In the late 2000s, UNHCR introduced the biometric registration of refugees in Kenya. In 2016, the Agency handed over the responsibility for the registration of refugees to the Kenyan government, and in the process, data from UNHCR's biometric database were integrated into the national register of persons. The operation revealed that an estimated 40,000 individuals registered with UNHCR were, in fact, Kenyan citizens. Among them, several minors at the time of registration were refused a Kenyan national identity card when reaching eighteen years old, the state claiming that they were aliens because their fingerprints were stored in the refugee database (Haki na Sheria Initiative, 2021: 31). Deprived of this document, Kenyan nationals are denied citizenship rights and privileges such as employment, freedom of movement, and education. For them, it is not the border that stands between them and the privileges of citizenship but their own biological markers.

These two examples illustrate the profound implications that may arise from UNHCR biometric registration practices. They also emphasize the importance of free and informed consent and redress mechanisms for preventing and responding to harm resulting from data processing. To be sure, this is not only true in humanitarian contexts. The collection of biometric data by states for identification purposes presents intricate legal and social challenges that are increasingly being questioned in public fora and national courts. Yet the legal environment in which UNHCR operates, as described earlier, bars most pathways for debate and contestation that would otherwise be available. The growing reliance on UNHCR to provide digital identities to refugees through biometric registration relocates data extraction and processing in an institutional and geographical space that offers an exceptionally enabling environment for such practices.

Legal scholar Julie Cohen (2019) notes that the emerging informational economy model of data extraction challenges the law and existing legal institutions. Increasingly shaped by private interests, digital practices thrive in regulatory settings that favor opacity, informality, and standard-based governance rather than legal rules. The subjugation of consent for collecting digital data sustains this model further. Considering UNHCR's accountability regime, one cannot help but notice the striking commonalities it shares with the regulatory framework idealized by digital actors in the market economy. Governance by standards rather than laws, self-regulation through codes of conduct and guidelines, and, significantly, immunity from prosecution before national courts are inherent to the Agency's regulatory environment. In short, delegating the biometric registration of refugees to UNHCR's transfer datafication practices into a jurisdictional setting where safeguard and accountability against breach to data protection are weak.

a Doubtful Consent

The issue of consent is central to discussions about new technologies and the processing of personal data in digital forms. Biometrics is data about a person's physical, physiological, or behavioral characteristics. These characteristics are unique to an individual and cannot be modified. Because of the sensitivity of these data, acquiescence or consent to the collection of biometrics is usually seen as essential to validate their processing. Individual consent gives moral legitimacy to

the collection and use of data. It reflects the agency and autonomy of the person over how their data are collected, used, and shared. From a legal standpoint, a person's consent transforms into a lawful act what would otherwise be the wrongful action of another. Indeed, collecting and processing personal data is considered an intrusion into someone's private sphere that requires her "transformative act of consent" to be lawful (Schermer, Custers, & van der Hof, 2014: 174). Consent is valid when given freely, that is, voluntarily without undue pressure or influence. The European General Data Protection Regulation, for instance, specifies that the individual consenting must have a real choice to accept or refuse the processing of her data. Consent must also be informed; to that end, the entity collecting and processing personal data must disclose who is collecting which data, for what purpose, and with whom it will be shared: "Anything less than this requires a leap of faith" (Barocas & Nissenbaum, 2014: 58).

While the legal and ethical foundations of consent remain the same in the humanitarian context, considerations specific to refugee populations complicate the issue, especially with regard to consent's voluntary element. In principle, UNHCR relies on consent as the legitimating basis for processing personal data. Yet scholars and refugee advocates have questioned whether refugees seeking UNHCR assistance can truly give their free consent when humanitarian aid is conditional on the collection of biometric data. Indeed, free consent may require not only the absence of constraint, but also the presence of enabling conditions, including basic material support for subsistence (Gould, 2019: 182).

On the issue of consent, UNHCR's policies lacks clarity. The general rule is that everywhere it is possible for the individual to exercise free and informed consent, it should be the legal basis for collecting and sharing biometrics. UNHCR's Guidance on Registration and Identity Management (2018) provides that individuals can refuse the collection of their biometrics on legitimate grounds and maintain their right to international protection using alternative methods for identification and registration. At the same time, UNHCR's 2015 Policy on the Protection of Personal Data of Persons of Concern to UNHCR (hereinafter UNHCR Policy) and its attendant 2018 Guidance on the Protection of Personal Data of Persons of Concern to UNHCR recognizes that it is not always possible to obtain refugees' free and informed consent, for instance, when a refugee seeking food or cash assistance

has no other source of income. In these situations, the UNHCR Policy provides no details about alternative modes of identification. Instead, it suggests that data processing (e.g., collection and sharing) remains valid under other legal bases such as the vital or best interests of the data subject, UNHCR's mandate, or the safety and security of refugees. On that analysis, reference to consent sounds hollow if it can be bypassed when the context makes it inconvenient to obtain.

Beyond the question of free consent, doubts remain about whether we can truly achieve informed consent in the context of new technologies. The technological complexities surrounding biometrics processing, its entanglement with big data, and unforeseen future applications make it nearly impossible to provide the information necessary to obtain informed consent – let alone in plain language. When processing someone's data involves complex data flows between diverse institutions with distinct interests, as can easily be the case when refugees' data are shared with states and implementing partners, we face what Solon Barocas and Helen Nissenbaum (2014: 58) call "the transparency paradox." That is, trying to impart the necessary information to obtain informed consent (i.e., data collected, for what purpose, with whom it is shared, following which modalities) in simple and clear terms cannot faithfully capture how data will be used. Hence, consent alone may be an inadequate basis for legitimating data use. For this reason, Carol Gould (2019) calls for the introduction of perspectives from democratic theory, bringing together principles of participation, deliberation, and representations to develop a form of "collective consent" that would apply to decision-making concerning new technologies and big data. Achieving that would be complex enough in liberal democracies. In the refugee context, this proposal will collide with the democratic boundary problem discussed by Eva-Maria Schäfferle in Chapter 16, whereby participation and representation is tightly knit to citizenship. Crucially, in the international humanitarian environment, it would require a perspective shift from seeing refugees as aid recipients devoid of agency (see Frédéric Mégret, Chapter 5), to individuals entitled to their say in decisions that affect them.

b Non-binding Standards

UNHCR's participation in collecting refugees' biometric data and the provision of digital identity is the extension of a paradigm that sees the expansion of nonstate actors' regulatory role in spheres that used to be

the preserve of states. Particularly acute since the 1990s, the phenomenon has directed attention toward how international organizations can be held accountable when their decisions or actions affect the rights or wellbeing of people under their protection or control (Benvenisti, 2018: 30). Hence, the question of accountability raised by UNHCR's biometrics practices is closely entwined with unresolved debates that emerged in the early 2000s about the responsibility of international organizations. While a number of theories are proposed to address these shortcomings, none offers a substitute for the protection found in national contexts. Several institutional characteristics undermine the Agency's answerability towards refugees and control over their own data. One is the nonbinding character of rules governing the management of refugees' data by UNHCR. The Agency's practices surrounding the processing of biometric data are primarily constituted of self-imposed policies and guidelines that inform the work of its staff. The most relevant instruments include the UNHCR Policy and two sets of guidance, mentioned earlier, for applying the Policy and guiding the registration of refugees, both adopted in 2018. Similar nonbinding standards developed by the United Nations inform UNHCR's practices.

Given the ongoing evolution and unsettled state of the law on data protection and new technologies, the adoption of standards by UN agencies is a welcome development. These policies and guidelines around basic data processing principles may promote a more uniform and right-enhancing approach to the treatment of biometric data within UNHCR. The standards also fill a gap in international law. While the right to privacy is recognized in international instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, no international instrument is dedicated to data protection. The prospect for the conclusion of an international treaty on this subject is dim. The ideological divide between the European and American approaches to data protection and the pace with which the field itself is moving makes such an agreement unlikely in the short term (Kittichaisaree & Kuner, 2015). In any event, even if adopted, an international treaty concerning data protection would be of little use to refugees owing to the difficulty in practice to apply human rights instruments to international organizations.

Still, the effectiveness of UN standards depends on implementation. An audit of the UNHCR Biometric Identity Management System

by the Office of Internal Oversight Services (OIOS) in 2016 revealed shortcomings in the application of the Policy. The OIOS found that the information communicated to refugees during biometric registration was below the standards provided for by the Policy, especially regarding the conditions of access to data by third parties and the rights and obligations of refugees. It also found that in all five country operations under review, staff knowledge of the Policy was limited. The Rohingya and Kenya cases discussed previously suggest flaws remain in applying the principles identified in UN standards in the area of concerns to the OIOS. The transfer of refugees' biometric data to the United States as per the MoU concluded between UNHCR and DHS in 2019 raises further questions about respect for UNHCR standards, especially with regard to the retention of data for longer than necessary – seventy-five years – and the use of the data for a purpose incompatible with the original reason for collection: humanitarian aid versus crime prevention (Department of Homeland Security [DHS], 2019).

c Legal No-Man's Land

With the risk of misapplying the Policy, another concern is the absence of an independent mechanism to hold the agency accountable when processing refugees' data. UNHCR's Policy on data protection establishes three supervisory roles with regard to data management: (1) a data protection officer, located at UNHCR's headquarters, with overarching responsibilities for monitoring, advising, supporting, and training personnel involved in data protection within UNHCR; (2) data controllers in each country office or operation, usually the Representative in a UNHCR country office, responsible for developing procedures for the handling of data that comply with the Policy; and (3) data protection focal points, designated by data controllers to assist them in their role. The focal point is usually the most senior UNHCR protection staff member in a country office or operation. These bodies are primarily responsible for defining institutional and country-wide procedures regarding data processing. As such, they may provide a level of oversight over decisions involving the processing of personal data. Still, (at least until recently) they were not responsible for handling individual complaints concerning breaches of the Policy. The main pathway available to refugees seeking to challenge the processing of their data is the UNHCR Inspector General's Office (IGO), an oversight mechanism

for investigating claims of misconduct by UNHCR personnel and staff. However, a number of structural deficits may prove to be severe obstacles to accountability (Johansen, 2020). This includes IGO's limited jurisdiction *ratione personae* to UNHCR staff members, not the Agency itself. Hence, the outcomes of investigations are disciplinary measures rather than remedial obligations. There are also shortcomings regarding the impartiality of the IGO owing to staffing procedures. This said, the creation of a Personal Data Protection Review Committee, envisaged in the 2022 General Policy on Personal Data Protection and Privacy to review decisions by local officials, could provide an additional and independent layer of redress once established (UNHCR, 2022).

Closely related to the latter point, the absence of an independent system of judicial review at the international level further undermined the scope for accountability within UNHCR. In a national context, judicial review has proven an efficient avenue for citizens to circumscribe the deployment of digital identity systems and population registries. In India, Mauritius, Kenya, and Jamaica, citizens and civil society have challenged the constitutionality of digital identity systems using biometrics. In these instances, judicial review afforded a space for negotiating the modalities under which governments may collect and process biometric data.[2] In three of the four cases, courts have upheld the systems but imposed limits on the type of data that can be collected and for which purpose, on who can access data, and for how long data can be retained. The Jamaican Supreme Court in *Julian J. Robinson v. The Attorney General of Jamaica* (2019) went further and struck down the National Identification and Registration Act and the National Identification and Registration System (NIDS) altogether. The Court concluded that the NIDS, which would have made it mandatory for all Jamaicans and certain residents to register their biometric data and obtain a NIDS identity card, would violate their constitutional right to privacy.

Even if judicial review operates *ex post* to the political decision, it nonetheless offers the potential for a constituency to agree or challenge

[2] *Justice K.S. Puttaswamy and Another v. Union of India and Others*, 2018; *Madhewoo v. The State of Mauritius and Another*, 2015; *Madhewoo v. The State of Mauritius and Another*, 2016; *Nubian Rights Forum and Others v. The Hon. Attorney General*, 2020; *Julian J. Robinson v. The Attorney General of Jamaica*, 2019.

governmental decisions through judicial bodies. In these four cases, national courts afforded citizens a pathway for influencing the structure and scope of national identity management systems. The binding nature of these decisions helped redress structural power inequalities between members of the public and the state. However, this crucial check designed to reign in the legislative and executive powers is lacking when UNHCR assumes responsibilities for the development of identity management systems. When conducting their mandate and functions, the immunities and privileges afforded to UNHCR and its officials shield the Agency from judicial proceedings. Indeed, Article 105 of the UN Charter and the 1946 Convention on the Privileges and Immunities of the United Nations are interpreted as providing absolute immunity to the Organization, its representatives, and officials from the jurisdiction of national courts (Rosa & Lemay-Hébert, 2019). In this context, the agency of refugees in defining the conditions under which UNHCR can collect and process their data is restricted.

Scholars have argued that the absence of checks and balances and a weak legal framework in the international migration space explains the proliferation of biometric technologies for governing the movement of refugees (Jacobsen, 2015; Molnar, 2019). On that analysis, international organizations such as UNHCR are a conduit for states to circumvent their legal responsibilities to protect human rights. Eyal Benvenisti (2018) notes that global institutions may pose a greater regulatory challenge than state institutions. Indeed, the transfer of responsibilities from states to international organizations allows powerful countries to evade democratic deliberations and respect for individual rights. This logic underpins the extraterritorialization of migration control, which, as noted by Ayten Gündoğdu in Chapter 10, often places the refugee in a "condition of rightlessness." In the present case, it is doubtful that the delegation of responsibility, if only partial, for the collection of refugees' biometric data to UNHCR is the sole product of a conscious reflection by states about evading their legal responsibilities. Foreigners' rights to data protection are generally already restricted when compared with the rights afforded by states to their own citizens (Guild, 2018). In parallel, we see a growing number of countries, especially in the Global South, adopting digital identity management systems and population registries. Most likely, the demands on UNHCR for producing ever more granular data about refugees is a consequence of the factors identified at

the beginning of this chapter. The emergence of an audit culture at the global level, the securitization of migration, and the promotion of a legal identity agenda in the UN Sustainable Development Goals all contribute to this development. But whether or not the growing pressure on UNHCR to collect and share refugees' biometric data is underpinned by a desire to evade legal obligations, this development produces a de facto transfer of biometric practices in a space of legal paucity that undermines refugees' agency over their data.

Conclusion

In 2015, UNHCR quoted Olivier Mzaliwa, a Congolese refugee, when promoting its biometric system: "I can be someone now. I am registered globally with the UN and you'll always know who I am." Perhaps Olivier is right, and we will always know who (and where) he is, but is that an inherently positive outcome? This line reflects the tension between the imperative of identification for access to aid and territory on the one hand and the right to integrity, privacy and control over one's data on the other. Kevin Haggerty and Richard Ericson (2000: 611) wrote that under a logic of technological surveillance, human bodies are abstracted from their territorial location and are reassembled into virtual "data doubles." These doubles then circulate in space and between actors in ways that condition the allocation of resources and power of (and over) those they digitally represent, without them being aware. The biometric data of refugees collected and processed by UNHCR follow a similar trajectory and purpose. While Olivier's body might well be trapped in a camp for a protracted period or stopped en route, his data, by contrast, are not only condoned but encouraged to cross national borders. In the legal no-man's land where UNHCR's biometrics practices are taking place, the risk of disenfranchising refugees, by undermining their ability to control the modalities under which their data are collected, processed, and shared, is real. It leaves them with little to no ascendance over the paths their data doubles will take, which borders they will cross, and who they will encounter along the way.