INTERNATIONAL HUMAN RIGHTS INTERNSHIP PROGRAM | WORKING PAPER SERIES

VOL. 9 | NO. 1 | SUMMER 2020

The Promise and Peril of Biometrics in Delivering Humanitarian Aid

Hanna Rioseco

McGill Centre for
Human Rights
and Legal Pluralism

Centre sur les droits de la
personne et le pluralisme
juridique de McGill

McGill FACULTY OF Law

ABOUT CHRLP

Established in September 2005, the Centre for Human Rights and Legal Pluralism (CHRLP) was formed to provide students, professors and the larger community with a locus of intellectual and physical resources for engaging critically with the ways in which law affects some of the most compelling social problems of our modern era, most notably human rights issues. Since then, the Centre has distinguished itself by its innovative legal and interdisciplinary approach, and its diverse and vibrant community of scholars, students and practitioners working at the intersection of human rights and legal pluralism.

CHRLP is a focal point for innovative legal and interdisciplinary research, dialogue and outreach on issues of human rights and legal pluralism. The Centre's mission is to provide students, professors and the wider community with a locus of intellectual and physical resources for engaging critically with how law impacts upon some of the compelling social problems of our modern era.

A key objective of the Centre is to deepen transdisciplinary collaboration on the complex social, ethical, political and philosophical dimensions of human rights. The current Centre initiative builds upon the human rights legacy and enormous scholarly engagement found in the Universal Declaration of Human Rights.

ABOUT THE SERIES

The Centre for Human Rights and Legal Pluralism (CHRLP) Working Paper Series enables the dissemination of papers by students who have participated in the Centre's International Human Rights Internship Program (IHRIP). Through the program, students complete placements with NGOs, government institutions, and tribunals where they gain practical work experience in human rights investigation, monitoring, and reporting. Students then write a research paper, supported by a peer review process, while participating in a seminar that critically engages with human rights discourses. In accordance with McGill University's Charter of Students' Rights, students in this course have the right to submit in English or in French any written work that is to be graded. Therefore, papers in this series may be published in either language.

The papers in this series are distributed free of charge and are available in PDF format on the CHRLP's website. Papers may be downloaded for personal use only. The opinions expressed in these papers remain solely those of the author(s). They should not be attributed to the CHRLP or McGill University. The papers in this series are intended to elicit feedback and to encourage debate on important public policy challenges. Copyright belongs to the author(s).

The WPS aims to meaningfully contribute to human rights discourses and encourage debate on important public policy challenges. To connect with the authors or to provide feedback, please contact human.rights@mcgill.ca.

ABSTRACT

In humanitarian situations where resources are scarce and needs are high, biometrics are useful in facilitating the secure and efficient provision of aid. However, the rapid rise and implementation of biometric technology in displacement contexts, particularly in areas of the world that lack data protection and privacy laws, raises the question: at what cost? This paper explores the tension between delivering humanitarian aid and protecting the rights of refugees by analyzing the rights implications that arise from the collection, use, and storage of Rohingya refugees' biometric data by the United Nations High Commissioner for Refugees (UNHCR) at Cox's Bazar. This paper unpacks the development and use of data-intensive systems in displacement contexts, arguing that for too long we have accepted the benefits of biometric technology without critically examining the risks it advances–which often come at the expense of already vulnerable populations. I argue that only by understanding the larger context in which a data subject is situated can we fully appreciate the particular rights at stake: for the Rohingya, understanding the precarity of their situation, as well as their relationship they have with their own identities, elucidates and a deeper awareness of the unique risks that flow from the collection of their data. In ascertaining whether the use of biometric technology truly protects and advances Rohingya refugees' rights, we must account for the surrounding legal, political, and social landscapes, and most importantly, centre our analysis on the Rohingya people themselves.

CONTENTS

Introduction

The use of biometric technology is becoming increasingly accepted. Consider, for example, the number of smart devices that can be unlocked with a person's face or fingerprint. Or the pervasiveness of facial recognition technology for purposes of security or fingerprinting for border management. Biometrics can be defined as a technique that uses biometric features to verify the identity of, or to identify, human beings.[1] Biometric characteristics include things physical characteristics, such as DNA, fingerprints, iris scans, voice print or facial geometry, and also behavioral characteristics, like handwriting.[2] Biological features that qualify as biometric have five qualities that make them desirable to be used for identification and authentication: (a) robustness; (b) distinctiveness; (c) availability; (d) accessibility, and (e) acceptability.[3] The convenience and fraud-proof capabilities of biometrics have not only revolutionized the way we design and access technology, but the way we access public and private services, too. Widely hailed as a secure, efficient, and sustainable way to verify and authenticate a person's identity, biometrics have become embedded in many of identity systems and programs operating in the world today.

At an ID2020 and Office of the United Nations High Commissioner for Refugees (UNHCR) joint workshop, the UNHCR recognized the importance of Sustainable Development Goal 16.9, which supports the goal of legal identity for all by 2030, for the world's most vulnerable people—refugees. As displaced people often lack identity documents, a spokesman from the UNHCR said: "It is not only logical to promote the digital inclusion of refugees; in the digital age, a digital identity for all is the only possible way to make sure that no one is left behind."[4] The UNHCR has been at the forefront of biometrics development, first implementing biometric technology in refugee camps in the early 2000s. However, the rapid implementation of biometric

[1] See Nancy Liu, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics* (Milton Park: Routledge 2012) at 29.

[2] See *ibid* at 20.

[3] See *ibid* at 30.

[4] "ID2020 and UNHCR Host Joint Workshop on Digital Identity" (4 December 2017), online: *UNHCR* <www.unhcr.org/blogs/id2020-and-unhcr-host-joint-workshop-on-digital-identity/> [UNHCR and ID2020 Workshop].

technology in displacement contexts, particularly in developing areas of the world that lack data protection and privacy laws, raises the question: at what cost?

As biometrics become normalized in our society as an efficient and practical identity management tool, data-intensive technologies that facilitate the mass collection and storage of biometrics are also being developed and imposed upon vulnerable populations who don't have much say as to what happens to their data thereafter. On one hand, biometric technology empowers at-risk populations by providing them with a legal identity. On the other hand, without adequate protection, it puts these people at further risk. However, the right to privacy is often overlooked in light of the benefits biometric identity management systems provide, namely, the accurate and efficient provision of aid and other essential services.

This paper will explore the tension between delivering humanitarian aid and protecting the rights of refugeed peoples. I do so by considering the experiences of the Rohingya population at Cox's Bazar, and the unique human rights and ethical implications that arise not only from the collection of their data but also from their precarious social and political situation. I argue that only by understanding the context in which a person is situated can we fully appreciate the particular rights at stake. I demonstrate that only by understanding the unique legal, political, social contexts in which biometric data is collected do we realize that UNHCR practices not only violate international norms related to privacy but encroach on the dignity of the refugeed populations they are mandated to protect. This paper is based on the idea that while human rights are universal, their relative importance and effective realization are context-specific.

To appropriately balance the rights of data subjects (in this case, the Rohingya people) with the purposes for which their data is being collected, I believe that it is imperative to understand the underlying social, political, and legal landscapes unique to the context in which data-intensive systems are deployed. In Section 2, I illustrate the purposes and aims of biometric data collection by chronicling the UNHCR's history with biometric identity management systems. In doing so, I rely on Tony Evans' thesis that the dominant human rights discourse, which supports a particular conception of rights, masks power relations. I argue that the UNHCR's deployment of biometric technologies in humanitarian aid contexts not only infringes on the rights of refugeed populations, but limits the discourse surrounding usefulness of those technologies. Section 3 explores the unique social and political contexts that underpin the precarious situation of Rohingya refugees at UNHCR camps in Bangladesh. Understanding how the history of persecution has affected their conceptions of identity elucidates and a deeper understanding of the unique rights implications that arise from the collection of their biometric data. In Section 4, I outline the contours of the right to privacy as defined in international law. I argue that privacy is not just about data protection but is fundamentally connected with human dignity. I illustrate this relationship by examining how the Supreme Court of India adopted the right to privacy in a pair of cases regarding the constitutionality of a national biometrics-based ID system.

I conclude by making recommendations for responsible data practices based on the unique social, political, and legal contexts underlying the Rohingyas' data collection. Realizing that the voices of refugees have largely been absent from the deployment and use of biometric technology, I echo the call made by Abdullahi Ahmed An-Na'im for a paradigm shift towards a people-centered model for digital rights in refugee contexts. I do so by outlining the ways in which the state-centric rights framework is failing to protect the rights of the Rohingya people and identifying opportunities for legal empowerment. In ascertaining whether the current use of biometric technology truly protects and advances Rohingya refugees' rights, we must take into account the complex legal, political, and social landscape but most importantly, centre our analysis on the Rohingya people themselves.

The UNHCR's Biometric Identity Management System

This section explores the political context behind the UNHCR's biometric identity system, illustrating how the purposes for which data is used "change according to geopolitics, technologies and market developments."[5] I begin by briefly commenting on the challenges raised by the UNHCR's traditional jurisdictional

[5] Martin Lemberg-Pedersen & Eman Haioty, "Re-assembling the Surveillable Refugee Body in the Era of Data-Craving" (2020) 24:5 Citizenship Studies 607 at 612.

immunity. Drawing upon Evans' thesis regarding power relations within the human rights framework, I argue that the UNHCR's use of biometrics in humanitarian aid contexts is problematic because it normalizes biometric collection, storage, and use, and limits critiques of data-intensive technologies.

The UNHCR's Jurisdictional Immunity

As a global administrative body, it is difficult to ascertain how the rights and obligations discussed in this paper actually apply to the UNHCR. The human rights framework is state-centric, based on the territorial sovereignty of member states who are the primary adjudicators of rights within their jurisdictions.[6] UNHCR camps are separate from the legal environment of the host state: no powers are conferred to the UNHCR by a host state, but the *de facto* power of the UNHCR reigns supreme.[7] This power is enhanced by refugees' "powerlessness and virtual complete dependence for survival."[8] It is also achieved through "discipline," a mode of social organization and power that imbues particular social norms, values, and behaviors.[9] Indeed, the scope of the UNHCR's authority and powers to administer refugee camps have evolved far beyond what was initially intended by its founding statute.[10]

The UNHCR acknowledges the importance of advancing human rights, such as ensuring the confidentiality of refugees' personal information in line with data protection principles, but the principles elaborated in official documents do not generate binding obligations.[11] Though a full discussion about the problems

[6] See Abdullahi Ahmed An-Na'im, "The Spirit of Laws is Not Universal: Alternatives to the Enforcement Paradigm for Human Rights" (2016) 21 Tilburg L Rev 255 at 271.

[7] See Stian Øby Johansen, *The Human Rights Accountability Mechanisms of International Organizations* (Cambridge: Cambridge University Press, 2020) at 179, 180.

[8] *Ibid* at 181.

[9] See Tony Evans, "International Human Rights Law as Power/Knowledge" (2005) 27:3 Hum Rts Q 1046 at 1054–55.

[10] See *Statue of the Office of the United Nations High Commissioner for Refugees*, UNGAOR, 5th Sess, Annex, UN Doc A/RES/428(V) (1951) 8; Johansen *supra* note 7 at 177.

[11] See e.g. Data Protection Handbook; United Nations High Commissioner for Refugees, *A Guide to International Refugee Protection and Building State Asylum Systems*, UNHCROR (2017) 1, online (pdf): <unhcr.org/3d4aba564.pdf> (where the importance of protecting refugees' rights are discussed as recommendations to State parliamentarians and policy

that arise from this legal void falls outside the scope of this paper, it highlights a pressing need for accountability, as refugees under the UNHCR's care often lack access to effective recourse mechanisms.[12]

For this paper, and as a subsidiary of the United Nations (UN), I will hold UNHCR to the standards elaborated in official policy guides, human rights instruments, and its mandate: "to safeguard the rights and well-being of refugees."[13]

UNHCR: A Pioneer in Biometrics

The UNHCR has been utilizing biometric technology for nearly two decades. It used iris recognition to repatriate Afghan refugees for the first time in 2002 and began developing BIMS in 2013.[14] Officially launched in 2015, BIMS is a centralized blockchain database that stores "all ten fingerprints and two irises from each individual to build a globally available biometric record."[15] According to the UNHCR, BIMS is for "protection, identity management, documentation, provision of assistance, population statistics and ultimately solutions."[16] Biometrics provide an efficient, accurate, and fraud-proof way to verify and preserve refugees' identities, a key objective in ensuring protection and targeting assistance.[17] Additionally, biometrics can "speed up cumbersome registration processes," an important advantage in

makers in adopting laws and policies to respond to the intake of asylum seekers).

[12] Anna Lise Purkey, "A Dignified Approach: Legal Empowerment and Justice for Human Rights Violations in Protracted Refugee Situations" (2013) 27:2 J Refugee Studies 260 at 261.

[13] UNHCR, Evaluation & Policy Analysis Unit, *Enhancing UNHCR's Capacity to Monitor the Protection, Rights and Well-Being of Refugees: Synthesis of Findings* at 3 https://www.unhcr.org/40d978a44.pdf

[14] See Katja Lindskov Jacobsen, "Experimentation in Humanitarian Locations: UNHCR and Biometric
Registration of Afghan Refugees" (2015) 46:2 Security Dialogue 144. at 145 [Jacobsen, "Experimentation in Humanitarian Locations"]; "Biometric Identity Management System: Enhancing Registration and Data Management" (2015) online (pdf): *UNHCR* www.unhcr.org/550c304c9.pdf [BIMS].

[15] "Guidance on Registration and Identity Management: Registration Tools" (February 2020), online: *UNHCR* <www.unhcr.org/registration-guidance/chapter3/registration-tools/>.

[16] Yaxley, Charlie, "Joint Bangladesh/UNHCR Verification of Rohingya Refugees Gets Underway" (06 July 2018), online: *UNHCR* <www.unhcr.org/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html>.

[17] BIMS, *supra* note 14.

situations where an overwhelming number of refugees need to be registered.[18] Where resources are scarce and needs are high, biometrics are useful in preventing duplication or fraud.[19] While this technology brings many benefits to refugee management, refugees appear to have little say over how their data appears in the system or what happens to it after it is collected. Further, the political context behind the UNHCR's biometric databases shows conflicting justifications and purposes for which the data is collected, raising serious questions as to what (or whose) interests are being considered in the development and deployment of these technologies.

While detailed UNHCR refugee registration policies are not publicly available, many studies have shown how private-sector partnerships and pressure from donor states can complicate the purpose of the UNHCR's biometric database.[20] In developing these data-intensive systems, private companies lend not only their expertise but the actual infrastructure and equipment the system is based on.[21] The UNHCR also justifies the development of biometrics-based systems by touting the technology's ability to facilitate inclusion and access to banking and essential services.[22] Refugee biometrics have become market opportunities, framed around narratives of aid distribution and digital empowerment. In this sense, the UNHCR legitimates the use of biometrics by adhering to "market discipline," the most predominant discipline within the current global order, which stresses economic growth and development.[23] Contextualizing BIMS within a market

[18] Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention" (2017) 11:4 J Intervention & Statebuilding 529 at 537 [Jacobsen, "Humanitarian Refugee Biometrics"]

[19] See *ibid* at 538.

[20] See *ibid* ("the UNHCR doesn't currently have a public policy on data protection. They have their own internal policies, but there's no way to know exactly what agreements they're reaching with governments or how they deal with the data they have" at 543). For studies that shed light on the political background of UNHCR's biometric projects, see e.g. Lemberg-Pedersen, *supra* note 5; Kristin Bergtora Sandvik et al, "Humanitarian Technology: A Critical Research Agenda" (2014) 893 Intl Rev Red Cross 219.

[21] See Sandvik, *supra* note 20 at 229; Lemberg-Pedersen, *supra* note 5 (BIMS was developed with the help of Accenture, a multi-national professional services company, and operates in partnership with IrisGuard, a supplier of iris recognition biometric technology at 611–12).

[22] See "UNHCR and ID2020", *supra* note 4; Lemberg-Pedersen, *supra* note 5 (the growth of technological-humanitarian-financial alliances has been facilitated by discourses of strategies of (39 in 2018).

[23] See Evans, *supra* note 9 at 1056.

discipline exerts pressure by legitimating particular customs—in this case, the use of refugees' data in developing new technologies according to donor dictates concerned with risk management and technological and financial market opportunities.[24]

The UNHCR's sharing agreements with and reliance on host and donor states elucidate another competing set of aims: national security.[25] In the past, states have requested access to the UNHCR's biometric refugee data for national security. In Kenya, the UNHCR allowed the government to crosscheck BIMS against an external database of Kenyan nationals to identify persons falsely claiming refugee status.[26] This endeavor was justified "for reasons of pressing national security… in a context of terrorist and criminal activities."[27] The United States and other Western governments have funded the development of UNHCR's refugee management technologies with a keen interest in exploring data sharing possibilities to establish the 'true' identity of a refugee through the use of biometric technology.[28] Thus, refugees' data is not just being used for refugee protection and the efficient provision of aid, but for security and anti-terror concerns. In effect, the UNHCR is forced to balance altruistic goals against the reality of being dependent upon donor state funding and serving state interests.[29] Faced with competing aims of protection and security, the UNHCR is understood as both "the gatekeeper responsible for guarding biometric data" and a "gateway for sovereign states seeking to test new technologies."[30] This is especially troubling given "the current political landscape in which refugees are increasingly being viewed with suspicion."[31]

[24] See *ibid* at 1055; Lemberg-Pedersen, *supra* note 5 at 620.

[25] BIMS has also been justified by its important role in securing the confidence and financial support of donors, signalling a tendency for the UNHCR to design its systems with donor interests in mind: see Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 537–38; Jacobsen, "Experimentation in Humanitarian Locations", *supra* note 14 at 155.

[26] See Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 541.

[27] *Ibid*.

[28] See Jacobsen, "Experimentation in Humanitarian Locations", *supra* note 14 at 155.

[29] See *ibid*.

[30] Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 531.

[31] Jacobsen, "Experimentation in Humanitarian Locations", *supra* note 14 at 155.

An overview of recent biometric projects by Privacy International shows that biometric technology is justified, for the most part, by purposes that advance economic and security interests.[32] This suggests that the UNHCR's operations are not only constrained by market discipline, but anti-terror or security disciplines, as well. Indeed, biometrics have become a "regular and routine feature" of the UNHCR's worldwide humanitarian efforts.[33] The UNHCR's status as a benevolent, authoritative institution affords a professionalized and authentic voice that justifies the use of refugees' data not only for protection but also for security and economic interests. [34] Humanitarian success stories in particular are powerful in conferring normative acceptability and influencing the routinization of new technologies.[35] In effect, the UNHCR's role in developing and deploying BIMS further limits the discourse surrounding biometrics to benefits related to the distribution of aid, security interests, and economic empowerment. This makes it increasingly difficult to critique BIMS, as the collection of biometrics in displacement contexts becomes normalized. However, recognizing the broader political context surrounding BIMS elucidates substantial risks, namely, that refugees' data will be shared and repurposed for different and competing objectives.

The Rohingya in Bangladesh

Reasons for Displacement

The Rohingya, an ethnic Muslim minority in Myanmar, have long faced conflict and persecution over their ethnic identity. Rohingya groups and historians trace their presence in Myanmar's Rakhine state back to the 12th century as inhabitants of the former Arakan Kingdom.[36] Under British colonial rule in the

[32] See "Biometrics: Friend or Foe of Privacy?" (13 December 2013) at 1–2, online (pdf): *Privacy International* <privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf>.

[33] Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 533 (alluding to statements made by the UNHCR officials about its widespread use of biometrics).

[34] See Evans, *supra* note 9 at 1058.

[35] See Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 539.

[36] See Kazi Fahmida Farzana, *Memories of Burmese Rohingya Refugees: Contested Identity and Belonging* (New York: Springer Nature, 2017) at 42; "Burma: The Rohingya Muslims: Ending a Cycle of Exodus?" (1 September 1996) online (pdf): *Human Rights Watch*

19th and 20th centuries, a significant amount of labor flows took place between modern-day India, Bangladesh, and Myanmar, prompting the arrival of more ethnic-Rohingyas to the Rakhine region.[37] The modern-day Government of Myanmar views these migration flows as a basis for refusing citizenship to the Rohingya; though this movement was intra-regional at the time, the government views it as illegal.[38] Tensions with Myanmar's government are also attributable to the Rohingya's support of the British during World War II. The British had promised the Rohingya supported a separate state in the northern Arakan region in exchange for their loyalty.[39] This alignment pitted them against the pro-independence groups who eventually came to power following Myanmar's independence. As a result, the newly independent government excluded the Rohingya from the Constitution and citizenship laws they enacted.[40] Since then, the Rohingya people have faced widespread systemic discrimination and targeted violence. In the 1970s and 1990s, the Rohingya fled to Bangladesh to escape forced labor, executions, rape, and religious persecution at the hands of Myanmar's army.[41] In each instance, the Rohingya were effectively forced to repatriate back to Myanmar by the Bangladeshi government, who withheld rations, allowed camp conditions to decline, and used physical force to get refugees to return.[42] Back in Myanmar, the systemic oppression, exclusion, and persecution of the Rohingya continued, ultimately culminating in "clearance operations" led by the Tatmadaw and other state security forces that targeted and terrorized the entire Rohingya population in 2017.[43] By August

<www.refworld.org/docid/3ae6a84a2.html> ["Cycle of Exodus"]; "Burmese Refugees in Bangladesh: Still No Durable Solution" (1 May 2000) online: *Human Rights Watch* <www.hrw.org/report/2000/05/01/burmese-refugees-bangladesh/still-no-durable-solution> ["No Durable Solution"].

[37] See Farzana, *supra* note 36 at 44–45; "No Durable Solution", *supra* note 36.

[38] See "No Durable Solution", *supra* note 36.

[39] See *ibid*; "Cycle of Exodus", *supra* note 36.

[40] See Farzana, *supra* note 36 at 47.

[41] See "No Durable Solution", *supra* note 36; "Cycle of Exodus", *supra* note 36.

[42] See "No Durable Solution", *supra* note 36; "Cycle of Exodus", *supra* note 36.

[43] See Human Rights Council, *Report of the independent international fact-finding mission on Myanmar*, UNHRCOR, 39th Sess, A/HRC/39/64 (2018) 1 at para 31–54, online (pdf): <undocs.org/en/A/HRC/39/64> [*Myanmar Report*].

2018, nearly 725,000 Rohingya fled to Bangladesh to seek safety from what is largely considered genocide.[44]

The Rohingya claim that continued government measures that deny them citizenship, and the pressure to accept National Verification Cards (NVCs), are a significant reason for their current displacement as they enabled an environment for genocide. Myanmar's government began issuing NVCs to the Rohingya in 2016.[45] The cards did not confer full citizenship rights but were necessary to hold to be eligible to apply for citizenship.[46] These cards were also mandatory for obtaining fishing and boat licenses, receiving healthcare, or registering births.[47] Many Rohingya refused to accept the NVCs not only because the cards undermined their demand for the restoration of citizenship status, but doing so would have required them to list their ethnicity as Bengali.[48] According to one community leader, the NVC process was just "the latest in a long-line of ID cards that attempt to recategorize Rohingya as foreigners, attack their group identity and remove their rights."[49] Ultimately, registration was forced upon them: the Rohingya were subjected to violence and torture if they refused to accept the cards.[50] The NVC process not only denied Rohingya access to citizenship but facilitated the erasure of their identities.

[44] See *ibid* at para 33, 84–87.

[45] See Human Rights Council, *Situation of human rights of Rohingya in Rakhine State: Report of the United Nations High Commissioner for Human Rights, Myanmar,* UNHRCOR, 40th Sess, A/HRC/40/37 (2019) 1 at para 23, online (pdf): <undocs.org/en/A/HRC/40/37> [*Human Rights in Rakhine State*]; "Tools of Genocide: National Verification Cards and the Denial of Citizenship of Rohingya Muslims in Myanmar" (September 2019) online (pdf): *Fortify Rights* <www.fortifyrights.org/downloads/Tools%20of%20Genocide%20-%20Fortify%20Rights%20-%20September-03-2019-EN.pdf> ["Tools of Genocide"]; Brinham, Natalie, "'Genocide Cards': Rohingya Refugees on Why They Risked their Lives to Refuse ID Cards" (21 October 2018), online: *openDemocracy* <www.opendemocracy.net/en/genocide-cards-why-rohingya-refugees-are-resisting-id-cards> ["Genocide Cards"].

[46] See *Human Rights in Rakhine State*, *supra* note 45 at para 23.

[47] See *ibid* at para 59; "Tools of Genocide", *supra* note 45 at 59.

[48] See *Human Rights in Rakhine State*, *supra* note 45 at para 23; "Tools of Genocide", *supra* note 45 at 68.

[49] "Genocide cards", *supra* note 45.

[50] See *ibid; Human Rights in Rakhine State*, *supra* note 45 at para 26.

Experiences in UNHCR Refugee Camps

As of November 30, 2020, 864,281 displaced Rohingya are living in UNHCR camps in Bangladesh.[51] In June 2018, Bangladesh authorities and the UNHCR began biometric registration for all refugees over the age of twelve.[52]. After providing iris scans, fingerprints, and photographs, refugees were registered and given fraud-proof identity cards that also store information about familial links. [53] Smart cards are necessary to access food and services within camps, and data is collected every time a person comes into contact with the UNHCR's services.[54] For example, a 2020 Factsheet reported that school enrollment would be linked to the BIMS database and shared with UNICEF's education information management system to avoid duplications and ensure accuracy.[55] Though the UNHCR has registered and issued smart IDs to almost all of the Rohingya refugees in Bangladesh, [56] registration was far from a smooth process.

Despite reported consultation and community awareness efforts by the UNHCR,[57] refugees have reported that they received sparse and inconsistent information about the scope and purpose of the BIMS database and smart cards before registration.[58] Based on interviews conducted in the camps, both refugees and officers from the Bangladeshi Government's Refugee Relief and Repatriation Commission (RRRC) had very different understandings as to the purpose of data collection and

[51] "UNHCR Bangladesh: Operational Update External: November 2020" (14 December 2020) online (pdf): *United Nations High Commissioner for Refugees* <data2.unhcr.org/en/documents/details/83629> ["UNHCR Operational Update"].

[52] See Yaxley, *supra* note 16.

[53] See Andrej Mahecic, "More Than Half a Million Rohingya Refugees Receive Identity Documents, Most for the First Time" (09 August 2019), online: *UNHCR* <www.unhcr.org/news/briefing/2019/8/5d4d24cf4/half-million-rohingya-refugees-receive>.

[54] Elise Thomas, "Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database" (12 March 2018) online: *Wired* <www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh>.

[55]See "UNHCR Operational Update", *supra* note 51.

[56] As of 30 November 2020, 826,758 Rohingya refugees are registered in the UNHCR-Bangladesh database: see *ibid*.

[57] See Yaxley, *supra* note 16.

[58] Madeleine Maxwell, Zara Rahman & Sara Baker, "Digital ID in Bangladeshi Refugee Camps: A Case Study" (2019) at 7, online (pdf): *The Engine Room* <digitalid.theengineroom.org/assets/pdfs/[English]%20Bangladesh%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf>.

identity documents. These understandings varied from separating Rohingya refugees from Bangladeshi nationals to establishing refugee status and becoming the responsibility of the UNHCR, to supporting repatriation efforts.[59] Additionally, refugees faced language barriers in understanding the nature of registration and identification project: the cards are issued only in English and Bengali, so those who don't speak either language or are illiterate cannot comprehend what is printed on their IDs.[60]

Initially, refugees protested against the ID system and refused to register because the cards did not specify their Rohingya ethnic identity.[61] The Rohingya are particularly sensitive about identity documents because of the history of their identity-based persecution and past experiences with the NVC process in Myanmar. However, the UNHCR recommends leaving ethnic identities off of ID cards, as it could lead to discrimination.[62] The conflict was ultimately resolved after database administrators shared more information about the reasons for data collection and explained that the database listed their Rohingya ethnic identity, despite not being shown on the cards.[63] However, the Rohingyas' registration into the Government of Bangladesh and UNHCR's shared database is precarious. The Rohingya feel that the smart cards will have the same outcome as the discriminatory NVCs.[64] Given the horrors they endured during NVC registration, the Rohingya have urged the UNHCR not to share their data. They are about their biometric data falling into the hands of the very same groups that attacked them for their identity: "We are still having doubts about one matter… they assured us that they won't share our biodata with the [Government of Myanmar], but what if they cheat us and share this data… [and] send us back to [Myanmar]?"[65]

[59] See *ibid* at 8.

[60] See *ibid* at 7.

[61] See *ibid* at 7–8; Htet Arkar, "Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps" (26 November 2018) online: *Radio Free Asia* <www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html>.

[62] See "Guidance on Registration and Identity Management: Documentation" (Feb 2020), online: *UNHCR* <www.unhcr.org/registration-guidance/chapter5/documentation>.

[63] See Engine Room, *supra* note at 8

[64] See "Genocide cards", *supra* note 45; Thomas, *supra* note 54.

[65] "Genocide cards", *supra* note 45; See also Arkar, *supra* note 61.

As there are regional regulatory frameworks to constrain the sharing of data between countries, this fear well-founded. Worse, there is strong evidence to suggest that Myanmar will receive Rohingya data through the potential repatriation process. Both the UNHCR and Bangladeshi authorities have stated that they will use biometric registrations to repatriate Rohingya refugees and issue new identification cards.[66] And in 2018, a leaked memorandum of understanding on Rohingya repatriation between the UNHCR, the United Nations Development Programme (UNDP), and Myanmar's government included a provision that gives Myanmar total control over providing identification cards to those eligible.[67] It is extremely concerning that a repatriation agreement would condone the sharing of biometric data and give Myanmar complete control over providing new identity documents, given their history with NVC registrations and exclusionary citizenship laws. While the Rohingya ultimately rejected the 2018 agreement and a final repatriation agreement has yet to be finalized, Myanmar has stated that they will issue citizenship cards that do not grant full citizenship to repatriated Rohingya.[68] Further, various reports have indicated that Bangladesh has already begun sharing lists of names with Myanmar for potential repatriation, absent a formal agreement or consent from the Rohingya. In 2018, Wired reported that Bangladesh shared a list of at least 8,000 Rohingya refugees, [69] and in 2019, Radio Free Asia reported that Bangladesh shared 25,000 Rohingya names with Myanmar for potential repatriation.[70]

Legal Issues: Understanding the Right to Privacy's Ubiquity

The right to privacy is recognised in many international and regional human rights instruments. Article 12 of the Universal Declaration of Human Rights (UDHR) states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" and that "[e]veryone has the right to the protection of

[66] See Thomas, *supra* note 54; "Genocide cards", *supra* note 45; *Myanmar Report*, *supra* note 45; Maxwell, *supra* note 58 at 8.

[67] See "Genocide cards", *supra* note 45.

[68] See Arkar, *supra* note 61.

[69] See Thomas, *supra* note 54.

[70] See Arkar, *supra* note 61.

the law against such interference or attacks."[71] A similar definition also appears in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which protects against the "unlawful" interference with or attacks on privacy.[72] The right to privacy applies not only to substantive information contained in communications but also to metadata that provides insight into an individual's behaviour and identity when analysed.[73] The mere generation and collection of data relating to a person's identity affect the right to privacy, as an individual loses control over their personal information the moment it is collected.[74]

At its core, the right to privacy protects the presumption that individuals can enjoy a "private sphere" of autonomous development, interaction, and liberty that is free from state intervention or from excessive unsolicited intervention by other uninvited individuals.[75] Privacy enables us to establish boundaries that protect ourselves from control and grants us the space to be ourselves without judgement or interference. In this sense, privacy can be understood as a right that is an essential prerequisite for both self-development and the enjoyment of other rights, such as freedom of thought and expression and freedom from discrimination.[76]

Understanding the contours of the right to privacy is an essential first step in determining whether the collection of biometric data in refugee contexts respect human rights. The collection of Rohingya's biometric data, in particular, raises serious human rights implications. In this section, I will first analyse

[71] *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, art 12 [UNDHR].

[72] See *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, art 17 (entered into force 23 March 1976) [ICCPR].

[73] Human Rights Council, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, UNHRCOR, 39th Sess, A/HRC/39/29 (2018) 1 at para 6, online (pdf): <undocs.org/A/HRC/39/29> [*Privacy in the Digital Age*].

[74] *Ibid* at para 5.

[75] *Ibid* at para 5.

[76] While an in-depth discussion about privacy's relationship with freedom of expression and freedom from discrimination falls outside the scope of this paper, see *ibid* at para 11; Paul Bernal, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" (2016) 1:2 J Cyber Policy 243 at 260; Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UNHRCOR 23rd Sess, A/HRC/23/40 (2013) 1 at para 24, online (pdf): <https://undocs.org/A/HRC/23/40>.

the right to privacy as it is understood in the digital age as the need to protect people's data. I argue that while necessary, discourse that increasingly links privacy with data protection obscures privacy as a more fundamental right that underpins many others. To illustrate privacy's ubiquity, I will highlight key takeaways from Indian jurisprudence that dealt with the rights implications of national biometrics-based ID systems. These cases not only illustrate important legal principles that biometric technologies should adhere to but demonstrate how the right to privacy can be understood not only as a safeguard for data protection, but as fundamental to the realization of dignity.

Privacy as Data Protection

Several key principles emerge from the Office of the United Nations High Commissioner for Human Rights (OHCHR) reports regarding data protection. First, data can only be processed where an individual has given their "free, specific, informed and unambiguous consent." [77] As noted in the reports from Rohingya refugees above, it is clear that the UNHCR collected refugees' data without first obtaining free, specific, and informed consent. The nature of refugees' consent can also be approached with skepticism, however, since registration is effectively mandatory to receive food and other essential services. Further, vulnerable populations in survival mode don't necessarily have the capacity to consider the long-term consequences of sharing their personal data.[78] Data collectors should also obtain consent if the purpose for which the data is being used changes. As evidenced by the Rohingyas' repeated pleas not to share their data with Myanmar authorities, and the sharing of names that have already taken place, it seems as though the UNHCR and the Government of Bangladesh are failing to obtain refugees' consent on this front, as well.

The collection and retention of data should also be limited and processed proportionately according to a legitimate purpose. [79] Function creep—namely, the expansion of a data project's scope to include cross-matching templates against other databases—is a legitimate concern of the deployment of biometric technology.[80]

[77] *Privacy in the Digital Age*, *supra* note 73 at para 29.

[78] See Maxwell, *supra* note 58 at 8.

[79] See *Privacy in the Digital Age*, *supra* note 73 at para 29.

[80] See Jacobsen, "Experimentation in Humanitarian Locations", *supra* note 14 at 156.

Thus, the type and amount of data should be limited to serving the purposes of a given project's mandate, and data should not be kept longer than it is needed. In addition, adequate security measures must be in place to safeguard against the unauthorized use, disclosure, modification, or deletion of data.[81] The Government of Bangladesh and UNHCR's track record of sharing practices, outlined above, breach this principle of proportionality and put refugees' data at risk.

Furthermore, the entities responsible for processing data must be accountable for their compliance with data protection frameworks. [82] Article 17 of the ICCPR affords rights to data subjects and implies a positive duty for states to adopt legislative frameworks to bulwark against unlawful or arbitrary interference by public or private actors.[83] Pursuant to UN guidelines, data protection legislation should specify the precise circumstances in which interference with the right to privacy is permitted to safeguard against potential misuse.[84] As for accountability, UN guidelines specify that states must ensure accountability and remedy for privacy violations by data processing entities through effective judicial or non-judicial state-based grievance mechanisms. [85] Oversight bodies tasked with safeguarding human rights should be granted the legal authority and technical resources to effectively monitor data-processing activities and impose sanctions where appropriate.[86] Entities that process data should be obligated to establish internal supervisory mechanisms, as well, and should be required to issue data breach notifications and privacy impact assessments.[87] At a minimum, individuals have a right to know when their data has been retained and processed and a right to access, rectify, or even delete data where it is unlawfully stored.[88]

The absence of domestic and regional data protection frameworks in places where the UNHCR operates, along with the UNHCR's legal immunity, raises serious concerns. Operating based on a host country agreement, the UNHCR may find itself in

[81] See *Privacy in the Digital Age*, *supra* note 73 at para 29.

[82] See *ibid*.

[83] See *ibid* at para 23.

[84] See *ibid* at para 10.

[85] See *ibid* at para 50.

[86] See *ibid* at para 33.

[87] See *ibid* at para 31.

[88] See *ibid* at para 30.

a position where it cannot easily reject a request from the host government to share biometric information on individuals who are, technically, under the jurisdiction of that government.[89] Especially where data protection laws are lacking, the private-sector companies who are allowed to test and develop these technologies on behalf of the UNHCR can do so without the risk of direct legal accountability.[90] As discussed above, while the UNHCR plays a supervisory role in refugee protection, it does not have much power in determining the protection implemented—countries establish traditional judicial and accountability mechanisms.[91] This leaves refugees without access to meaningful and effective avenues to establish any sort of control over their data.

Finally, sensitive data must be afforded a particularly high level of protection.[92] Biometric data has been recognized as an extremely sensitive type of data, as it cannot be changed and is inseparably linked to a particular person.[93] Due to biometric data's permanence, any breach that occurs extremely difficult to remedy. Thus, the collection, storage, and processing of biometric data raises significant human rights concerns and should be subject to strict scrutiny. An infringement on the right to privacy, especially where sensitive data is involved, can cascade to affect a person's dignity and can exacerbate inequality and discrimination, particularly for vulnerable groups or individuals.[94] Given these potentially lifelong effects, an analysis of the risks and rights implications involved with the mass collection, storage and use of biometric data should extend beyond the mere protection of data to a consideration of how the right to privacy is intertwined with other rights, namely, and dignity.

[89] See Jacobsen, "Experimentation in Humanitarian Locations", *supra* note 14 at 157.

[90] See Lemberg-Pedersen, *supra* note 4 at 619.

[91] See Mark Pallis, "The Operation of UNHCR's Accountability Mechanisms" (2006) 37 NYUJ Intl L & Pol 869 at 904.

[92] See *Privacy in the Digital Age*, *supra* note 73 at para 29.

[93] See *ibid* at para 14. See also EC, *Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, [2016] OJ L 119/1 art 9 (biometric data is considered a "special category" of data, the processing of which subject to strict limitations).

[94] See *Privacy in the Digital Age*, *supra* note 73 at para 11.

Privacy as Dignity

Though data protection is important for the collection of biometric information, it is but one component of the right to privacy. As defined in international law, the right to privacy also encompasses protection from attacks upon "honour and reputation,"[95] signaling that privacy rights are impacted by any activity that might infringe on a person's dignity. Understanding privacy as a basis for dignity elucidates a deeper appreciation of the importance of safeguarding privacy rights.

The preamble of the Universal Declaration of Human Rights (UDHR) recognizes that "the inherent dignity and... equal and inalienable rights of all members of the human family [as] the foundation of freedom, justice and peace in the world."[96] There are several conceptions of dignity, each tethered to particular interpretations based on context.[97] Yet dignity also "enables a dialogue to take place between judges on the interpretation of human rights norms" because "different jurisdictions share a sense of what dignity requires."[98] From these overlaps in understanding, dignity's common core can be identified. To illustrate the basic elements of dignity and how they relate to privacy in a data-intensive context, I reference recent jurisprudence from the Supreme Court of India which dealt with the rights implications of a biometrics-based national ID system.

In 2012, former Justice K. S. Puttaswamy brought forth a constitutional challenge that alleged Aadhaar, the world's largest biometric ID system, violated citizens' privacy, autonomy, and dignity and unduly limited access to essential services.[99] At the time, the Aadhaar scheme was not operating under legislation, nor did India recognize a constitutional to privacy.[100] Before

[95] See UDHR *supra* note 71 art 12; ICCPR *supra* note 72 art 17.

[96] See UDHR *supra* note 71.

[97] See Christopher McCrudden, "Human Dignity and Judicial Interpretation of Human Rights" (2008) 19:4 Eur J Intl L 655 at 730.

[98] See *ibid* at 700.

[99] See *Justice K. S. Puttaswamy v Union of India* (2018), 1 SCC 809 (India) at para 5 [*Aadhaar*].

[100] See *ibid*. See also "Initial Analysis of Indian Supreme Court Decision on Aadhaar" (26 September 2018), online: *Privacy International* <www.privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar> (implemented in 2010, Aadhaar enrollment reached 1 billion and finally received a basis in law in 2016) ["Initial Analysis of Aadhaar"].

determining whether the biometric scheme was constitutional, the Supreme Court first recognized the right to privacy in a landmark decision in 2017.[101] The following year, the Court upheld the Aadhaar scheme overall, but specified limits on its usage and demanded that a data protection law be passed immediately.[102]

In the *Puttaswamy* decision, the Court elaborated that "the sanctity of privacy lies in its functional relationship with dignity."[103] Privacy recognizes the autonomy of individuals to make personal choices and enables self-actualization by securing the inner recesses of the human personality from unwanted intrusion.[104] In the *Aadhaar* decision, the Court further defined dignity as "the core which unites the fundamental rights," which all seek to achieve the dignity of existence.[105] Dignity is made up of three elements: intrinsic value, possessed by every human by merely being human; autonomy, which recognizes that a person's intrinsic worth should be respected by others; and community value, which speaks to an individual's relationship with the state and with others.[106] Further, dignity emphasizes that the state and community must recognize that some forms of treatment might be inconsistent with respect for a person's intrinsic worth. It is only through collective decision-making that restrictions on individual freedoms can be placed.[107]

Several aspects of the *Aadhaar* decision can be distinguished from the Rohingya context. For one, there are no publicly available policy documents or regulations that govern the administration of BIMS from which a proportionality assessment could properly be performed. In the *Aadhaar* decision, the State's aim in utilizing biometric technology to deliver welfare was framed as an anti-fraud measure.[108] While the UNHCR has stated biometrics are useful for preventing fraud and duplication, the UNHCR's biometric technologies are, in practice, justified by multiple varying and competing rationales. These aims may change over time based on refugees' and the UNHCR's needs or

[101] See *Justice K. S. Puttaswamy* v *Union of India* (2017), 10 SCC 1 (India) [*Puttaswamy*].
[102] See *Aadhaar, supra* note 99.
[103] See *Puttaswamy, supra* note 101 at para 113
[104] See *ibid*.
[105] *Ibid* at para 107.
[106] See *Aadhaar, supra* note 99 at para 116; McCrudden, *supra* note 97 at 683.
[107] See *Aadhaar, supra* note 99 at para 116
[108] *Ibid* at para 266.

political and market opportunities. Further, the Court justified "minimal" intrusions on privacy in favour of economic welfare because no data on individuals' transactions are tracked. Yet this is not the case in UNHCR camps, as information is collected about refugees each time they come into contact with a service interconnected with BIMS.

A key similarity between the UNHCR's practices and the Aadhaar scheme is the balancing of two competing fundamental rights: the right to privacy, and the right to basic necessities such as food and shelter. Dignity underlies both of these rights, however, manifesting as autonomy on one hand and as an assurance of better living standards on the other. Interestingly, the economic aims that are balanced against the right to privacy seem to adhere better to a market discipline, potentially carrying heavier normative weight. In fact, the Court posited that access to essential services, the core content of social and economic rights, was a facet of autonomy.[109] Dignity's relationship with economic rights is also reflected in the UDHR. Aside from Article 1 and the Preamble, dignity is mentioned only in Articles 22 and 23: the right to social security and the right to work, respectively.[110] It thus seems that even dignity in this context is constrained by market disciplinary power. This is where dignity's workability can be appreciated: the actual components and rights that fulfil dignity change and are contingent on particular worldviews and contexts.

In the *Aadhaar* decision, the Court emphasized dignity's community value as emphasizing the establishment of collective goals.[111] Dignity implies the freedom to make personal choices, and requires respect by the state and community for an individual's self-determination and self-empowerment capabilities.[112] In the BIMS registration process, for example, the UNHCR did not demonstrate respect for the Rohingya community's desire to obtain identity documents that listed their Rohingya identity. The UNHCR does not generally print ethnicities on IDs due to avoid risks of discrimination, yet their decision favored one conception of rights (the UNHCR's) to another (the Rohingyas'). But for the Rohingya, having their identity

[109] See *ibid* at para 116.

[110] UDHR, *supra* note 71 art 22, 23(3). See also McCrudden, *supra* note 97 at 669.

[111] See *Aadhaar*, *supra* note 99 at para 116.

[112] See McCrudden, *supra* note 97 ("these are the stuff and substance of essential human dignity" at 708).

recognized is a deeply important matter, as it has been categorically denied to them by the Government of Myanmar—this level of importance seems to get lost in translation.

Moreover, upholding the right to privacy does not simply entail data protection. While strong data protection standards are a necessary bulwark against arbitrary infringements on the right to privacy, privacy is a critical foundation for the realization of many other rights. Fundamentally, privacy enables our self-actualization and preserves our dignity.

Reconciling Humanitarian Assistance with Responsible Data Practices: A New Paradigm

The urgent and important objective to quickly deliver humanitarian assistance can contradict, and often supersedes, other rights considerations. That refugees under the UNHCR's protection are obliged to agree to the collection of their biometric data, with little to no knowledge of or say in what happens to their data thereafter, raises serious implications in regard to their privacy. The right to privacy may feel relatively trivial to a displaced population fleeing genocide, or those already preoccupied with finding basic needs such as food and shelter. However, the protection of Rohingyas' biometric data is not just related to the right to privacy: respecting their right to assert control over their data recognizes their dignity. The UNHCR's mandate of facilitating the safe and dignified resettlement of Rohingya refugees cannot be realized if their dignity—as they conceive it—is not respected.

Responsible data policy can only be realized by taking into account the unique social and political contexts where the collection and use of sensitive data is taking place. Without doing so, we will fail to appreciate and mitigate against the actual risks that arise. Further, responsible data practice should not necessarily be realized through the traditional state-centric human rights framework, but rather center around and empower data subjects so that they can exert full control over themselves and their data. This is especially crucial in contexts involving stateless or refugeed populations, who face continued marginalization and additional barriers to accessing effective mechanisms for accountability and redress.

A Dignified, People-Centred Approach

The voices of Rohingya, and refugees in general, have largely been absent in the discourse surrounding the use of biometrics-based identity management systems in humanitarian contexts. In interviews with Rohingya refugees, one author noted that "[t]heir identity is very much apparent in their narratives."[113] Indeed, the Rohingya identity has been constructed and politicized through pre-colonial and colonial constructions, the formation of borders, laws, media representation, and the politics of belonging.[114] This is true for many stateless populations across the world. But now, their identities are being re-assembled by the UNHCR "according to their aid needs, but also according to donor dictates concerned with risk management, and technological and financial market opportunities."[115] Yet "in the existing voice on the Rohingya issue, the voices of the displaced Rohingya refugees themselves have not been given any space."[116]

The rights enjoyed by refugees in protracted situations are contingent upon a broad range of political and economic factors, including the level of international assistance provided and the perceived potential outcome of the refugee crisis.[117] Because the UNHCR activities usually take place in crisis situations, an "emergency mindset" permeates all areas of their operation: the need to distribute food, shelter, and other basic necessities will always prevail over other rights considerations and accountability.[118] However, this mindset perpetuates the idea of the refugee as a victim, as a recipient of aid, and an object of charity, rather than as someone to whom rights are owed.[119] Moreover, simply treating refugees better than their countries of origin does not serve to advance their rights. When it comes to the risks involved in the mass collection and storage of biometric data, understanding privacy as essential to dignity reinforces the idea that privacy (or any right) should not be surrendered merely because a person is in a protracted displacement context.

[113] Farzana*, supra* note 36 at 139.
[114] See *ibid* at 233.
[115] Lemberg-Pedersen, *supra* note 4 at 620.
[116] Farzana*, supra* note 36 at 141.
[117] See Purkey, *supra* note 12 at 261.
[118] See *ibid*; Pallis, *supra* note 91 at 905.
[119] See Purkey, *supra* note 12 at 261; Pallis, *supra* note 91 at 909.

Understanding privacy as a postulate of dignity helps to further center human rights considerations around rights-holders. Dignity's elasticity makes it difficult to apply as a legal rule, but as a concept underlying all human rights, the shell it provides offers space for consensus-building. This space is important in respecting a person or community's right and ability to make choices for themselves. An-Na'im posits that "the human dignity of every person should be upheld by his or her own agency, instead of being dependent on the goodwill of others."[120] Refugees themselves should be progressively and proactively the primary decision-makers and agents of change, rather than mere subjects or beneficiaries.[121] Further, dignity's flexibility as a rights-based principle to be informed by collective experiences and understandings allows the exact elements that fulfill it to change depending on the context. This is increasingly important in contexts where political, social, and technological forces change rapidly, and allows a more fluid balance to be struck between values such as privacy and access to food and shelter, both of which are intimately related to dignity.

Legal empowerment offers a way of increasing refugees' control over their own lives.[122] By providing refugees with the knowledge and skills necessary to mobilize and assert their rights, refugees can be empowered to challenge the dominant market and security disciplines that limit the UNHCR's biometric operations in the first place. Legal empowerment thus serves to change the paradigm in which refugees and aid providers interact and can be tailored to what refugeed populations are able to do to advance their rights and assert control over their lives.[123]

Promoting Responsible Data Practices

The practice of human rights enables us to realize the dignity that is inherent in all human beings.[124] Thus, centering dignity, as it is informed by data-subjects, as a fundamental right to be respected is crucial in developing responsible data practices in situations affected by multiple, competing interests. Adopting data standards that are responsive to the needs of refugees is important

[120] An-Na'im, *supra* note 6 at 273.

[121] See *ibid*.

[122] See Purkey, *supra* note 12 at 261.

[123] See *ibid* at 264–65.

[124] See Donnelly, Jack, *Universal Human Rights in Theory and Practice* (Ithaca: Cornell University Press, 2013) at 39.

not only to respect their dignity, but to help stabilize the complex legal landscape the UNHCR currently operates in. These standards can be used as a springboard to create flexible accountability mechanisms that create participation outside of formal, state-based judicial processes.[125]

Further, the idea of balancing privacy with security, or privacy with aid, oversimplifies the rights at stake: as outlined above, privacy is a right that affords us the ability to enjoy other rights. This speaks to the importance of taking into account the social, political, and legal forces surrounding the use of biometrics, particularly as it is questionable whether the law is ever really able to keep pace with technology or the way people use it.[126] Data-intensive systems impact not just individuals, but entire groups. Thus, in formulating responsible data practices, it is imperative to widen our conception of privacy to fully recognize its interconnectedness with other human rights and as it affects us collectively.

Necessity and Proportionality

A key principle of data protection that the UNHCR needs to adhere to is that of data minimization. Minimizing the types and amount of data collected can help to ensure that the UNHCR's biometric projects are proportionate to their aims. In balancing the UNHCR's objectives with the rights of refugees, rights that advance economic and security interests will usually outweigh rights and values, such as privacy. This is largely due to the normative force of market and security disciplines that constrain our conception of rights. However, through recognizing privacy as a right whose contents are informed by the data-subjects, a more appropriate balance can be struck.

Another key objective of BIMS is that it provides refugees with a legal identity. This is undoubtedly an important objective, as a legal identity serves as the basis for the enjoyment of many other rights and is also a facet of legal empowerment.[127] This right is so important that is enshrined in Article 27 of the refugee convention.[128] However, "Article 27 does not specify the nature

[125] See Pallis, *supra* note 91 at 876.

[126] See Bernal, *supra* note 76 at 244.

[127] See Purkey, *supra* note 12 at 276.

[128] *Convention Relating to the Status of Refugees*, 28 July 1951, 189 UNTS 150 (entered into force 22 April 1954).

of the identity papers that are to be issued… leaving each state party free to determine the particular form and content to be given to the document provided for this purpose."[129] This leaves room for refugees, the UNHCR, and the host state to negotiate a way to provide legal identities that doesn't unduly encroach on their privacy. While biometrics are an efficient and secure base for legal identities, the maintenance of a massive, centralized database that stores sensitive data generates a significant risk in the event of a data breach. Arguably, this centralized database is useful for the UNHCR in administering services and provisions within refugee camps. However, giving other entities access to that database invites opportunities for function creep and misuse. If the aim of BIMS is to provide a legal identity and distribute aid, the UNHCR should respect the principle of data minimization and consult refugees before extending the use of biometrics beyond those objectives. Refugees should be not only informed about the precise reasons for which their data is being accessed but be actively involved in decision-making about how their data is ultimately used.

Transparency and Accountability

The UNHCR's biometric systems are shrouded in secrecy.[130] With regard to the primary forces that drove and funded the development of BIMS, it seems as though the UNHCR is more accountable to political and market pressures rather than the desires of refugees. If a refugee under the UNHCR's care wanted to challenge their data practices, they would have a difficult time doing so. Refugees are subjected to multiple, over-lapping legal and quasi-legal regimes including camp by-laws, religious laws, the laws of the host state and country of origin, and international law.[131] The state-centric approach of accountability and judicial mechanisms poses a particular challenge for stateless persons who are living under the control of an international body that enjoys jurisdictional immunity. Refugees, then, are left in a precarious situation: not only do they lack control over their data and themselves, but they lack access to redress.

[129] United Nations High Commissioner for Refugees, *Identity Documents for Refugees*, UNHCROR, 35th Sess, EC/SCP/33 (1984) 1 at para 8, online: <www.unhcr.org/excom/scip/3ae68cce4/identity-documents-refugees.html>.
[130] See Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 ("there's no way to know exactly what agreements [the UNHCR] is reaching with governments or how they deal with the data they have" at 543).
[131] See Purkey, *supra* note 12 at 267

In addition to empowering refugees to assert rights claims, stronger accountability mechanisms must be put in place. Accountability in the displacement contexts means ensuring responsiveness to refugees-not partners—and ensuring the respect, protection and fulfilment of human rights obligations.[132] First, the UNHCR should be more forthcoming about the ways in which biometric technologies so that refugees know how their data is being used. In response to a question posed about the exchange of biometric data with NGO and governmental partners, the UNHCR responded: "Biometrics will be used at UNHCR's discretion. Whether or not UNHCR exchanges data with partners, is not relevant."[133] This answer invites further questions as to how the UNHCR considers its responsibilities over their massive, centralized databases of sensitive data, and signals that it is not currently considering the interests of the refugeed people under its care. And for the Rohingya, the exchange of their data can be a matter of life and death. Transparency is crucial in facilitating trust and empowering refugees to make informed decisions. Further, accountability mechanisms should provide refugees with the opportunity to participate in decision-making and exert control over their data. While a detailed discussion of what types of accountability mechanisms are best suited in this context, accountability mechanisms that are flexible and tailored to respond to the unique needs of different refugee populations should be considered. This is because the rights refugees in different contexts will assert will vary depending on their experiences and values.

Conclusion

Calling for a moratorium on the use of BIMS would help to secure the rights of refugees but overlooks the benefits that biometric technology delivers. Biometric identity management systems serve a legitimate purpose in providing people with identity documents and pathways to citizenship. Despite these positive aspects, these technologies aren't inherently positive—when the success stories behind biometric systems come out of the humanitarian context, they obscure issues relating to rights abuses and accountability.

[132] See Purkey, *supra* note 12 at 270.

[133] Jacobsen, "Humanitarian Refugee Biometrics", *supra* note 18 at 543.

Further, these systems are increasingly being deployed without strong legal footing, and without due regard for long-term implications. As the law struggles to keep pace with the rapid adoption and evolution of data-intensive systems, it's imperative for data collectors to build out internal policies that aim to mitigate the potential harms of misuse or breach. Biometrics-based systems should be designed with responsible data practices in mind, in collaboration with the people whose data they host. In addition, safeguards should not assume a global consensus on the right to privacy. Rather, accountability mechanisms and data protection standards should be tailored to meet the unique needs and values of particular communities and contexts.

As data-intensive technologies become omnipresent in our everyday lives, it is important to question the purposes that they purport to serve to appropriately mitigate against the risks of surveillance and misuse. In doing so, it is imperative to conceptualize the right to privacy as more than just an individual right to data: the right to privacy should be understood as intrinsic to dignity and self-flourishing. Only by taking into account the sociopolitical contexts in which technologies are deployed, and data is collected, can we truly appreciate the wide-ranging, fundamental rights that are at stake. We must widen the frame of privacy discourse to include considerations of dignity and other interrelated rights. Accordingly, a paradigm shift that centers data subjects and their experiences is needed to meaningfully protect the victims of rights abuses and empower them to be agents of their own change.

Bibliography

LEGISLATION: EUROPE

EC, *Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, [2016] OJ L 119/1 [GDPR].

JURISPRUDENCE: FOREIGN

Justice K. S. Puttaswamy v *Union of India* (2017), 10 SCC 1 (India) [*Puttaswamy*].

Justice K. S. Puttaswamy v Union of India (2018), 1 SCC 809 (India) [*Aadhaar*].

INTERNATIONAL MATERIALS

Universal Declaration of Human Rights, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71 [*UNDHR*].

Convention Relating to the Status of Refugees, 28 July 1951, 189 UNTS 150 (entered into force 22 April 1954).

Human Rights Council, *Situation of human rights of Rohingya in Rakhine State: Report of the United Nations High Commissioner for Human Rights, Myanmar,* UNHRCOR, 40th Sess, A/HRC/40/37 (2019) 1, online (pdf): <undocs.org/en/A/HRC/40/37>.

Human Rights Council, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, UNHRCOR, 39th Sess, A/HRC/39/29 (2018) 1, online (pdf): <undocs.org/A/HRC/39/29>.

Human Rights Council, *Report of the independent international fact-finding mission on Myanmar*, UNHRCOR, 39th Sess, A/HRC/39/64 (2018) 1, online (pdf): <undocs.org/en/A/HRC/39/64>.

International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171 at PINPOINT (entered into force 23 March 1976) [*ICCPR*].

United Nations High Commissioner for Refugees, *Identity Documents for Refugees*, UNHCROR, 35th Sess, EC/SCP/33 (1984) 1 at para 8, online: <www.unhcr.org/excom/scip/3ae68cce4/identity-documents-refugees.html>.

SECONDARY MATERIALS: MONOGRAPHS

Donnelly, Jack, *Universal Human Rights in Theory and Practice* (Ithaca: Cornell University Press, 2013).

Farzana, Kazi Fahmida, *Memories of Burmese Rohingya Refugees: Contested Identity and Belonging* (New York: Springer Nature, 2017).

Liu, Nancy, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics* (Milton Park: Routledge 2012).

Johansen, Stian Øby, *The Human Rights Accountability Mechanisms of International Organizations* (Cambridge: Cambridge University Press, 2020).

SECONDARY MATERIALS: ARTICLES

An-Na'im, Abdullahi Ahmed, "The Spirit of Laws is Not Universal: Alternatives to the Enforcement Paradigm for Human Rights" (2016) 21 Tilburg L Rev 255.

Bernal, Paul, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" (2016) 1:2 J Cyber Policy 243.

Evans, Tony, "International Human Rights Law as Power/Knowledge" (2005) 27:3 Hum Rts Q 1046.

McCrudden, Christopher, "Human Dignity and Judicial Interpretation of Human Rights" (2008) 19:4 Eur J Intl L 655

Jacobsen, Katja Lindskov, "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees" (2015) 46:2 Security Dialogue 144.

Jacobsen, Katja Lindskov, "On Humanitarian Refugee Biometrics and New Forms of Intervention" (2017) 11:4 J Intervention & Statebuilding 529.

Lemberg-Pedersen, Martin & Eman Haioty, "Re-assembling the Surveillable Refugee Body in the Era of Data-Craving" (2020) 24:5 Citizenship Studies 607.

Pallis, Mark, "The Operation of UNHCR's Accountability Mechanisms" (2006) 37 NYUJ Intl L & Pol 869.

Purkey, Anna Lise, "A Dignified Approach: Legal Empowerment and Justice for Human Rights Violations in Protracted Refugee Situations" (2013) 27:2 J Refugee Studies 260.

Sandvik, Kristin Bergtora et al, "Humanitarian Technology: A Critical Research Agenda" (2014) 893 Intl Rev Red Cross 219.

OTHER MATERIALS

Arkar, Htet, "Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps" (26 November 2018) online: *Radio Free Asia* <www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html>.

Brinham, Natalie, "'Genocide Cards': Rohingya Refugees on Why They Risked their Lives to Refuse ID Cards" (21 October 2018), online: *openDemocracy* <www.opendemocracy.net/en/genocide-cards-why-rohingya-refugees-are-resisting-id-cards>.

"Biometric Identity Management System: Enhancing Registration and Data Management" (2015) online (pdf): *UNHCR* <www.unhcr.org/550c304c9.pdf>.

"Biometrics: Friend or Foe of Privacy?" (13 December 2013) online (pdf): *Privacy International* <privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf>.

"Burma: The Rohingya Muslims: Ending a Cycle of Exodus?" (1 September 1996) online (pdf): *Human Rights Watch* <www.refworld.org/docid/3ae6a84a2.html>.

"Burmese Refugees in Bangladesh: Still No Durable Solution" (1 May 2000) online: *Human Rights Watch* <www.hrw.org/report/2000/05/01/burmese-refugees-bangladesh/still-no-durable-solution>.

"Guidance on Registration and Identity Management: Documentation" (February 2020), online: *UNHCR*

<www.unhcr.org/registration-guidance/chapter5/documentation>.

"Guidance on Registration and Identity Management: Registration Tools" (February 2020), online: *UNHCR* <www.unhcr.org/registration-guidance/chapter3/registration-tools/>.

"ID2020 and UNHCR Host Joint Workshop on Digital Identity" (4 December 2017), online: *UNHCR* <www.unhcr.org/blogs/id2020-and-unhcr-host-joint-workshop-on-digital-identity/>.

"Initial Analysis of Indian Supreme Court Decision on Aadhaar" (26 September 2018), online: *Privacy International* <www.privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar>.

Mahecic, Andrej, "More Than Half a Million Rohingya Refugees Receive Identity Documents, Most for the First Time" (09 August 2019), online: *UNHCR* <www.unhcr.org/news/briefing/2019/8/5d4d24cf4/half-million-rohingya-refugees-receive>.

Maxwell, Madeleine, Zara Rahman & Sara Baker, "Digital ID in Bangladeshi Refugee Camps: A Case Study" (2019) at 7, online (pdf): *The Engine Room* <digitalid.theengineroom.org/assets/pdfs/[English]%20Bangladesh%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf>.

Thomas, Elise "Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database" (12 March 2018) online: *Wired* <www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh>.

"Tools of Genocide: National Verification Cards and the Denial of Citizenship of Rohingya Muslims in Myanmar" (September 2019) online (pdf): *Fortify Rights* <www.fortifyrights.org/downloads/Tools%20of%20Genocide%20-%20Fortify%20Rights%20-%20September-03-2019-EN.pdf>.

"UNHCR Bangladesh: Operational Update External: November 2020" (14 December 2020) online (pdf): *United Nations High*

Commissioner for Refugees <data2.unhcr.org/en/documents/details/83629>.

Yaxley, Charlie, "Joint Bangladesh/UNHCR Verification of Rohingya Refugees Gets Underway" (06 July 2018), online: *UNHCR* <www.unhcr.org/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html>.