Cambridge International Law Journal, Vol. 8 No. 2, pp. 305–330

Technology on the margins: AI and global migration management from a human rights perspective

Petra Molnar*
University of Toronto, Canada

Experiments with new technologies in migration management are increasing. From Big Data predictions about population movements in the Mediterranean, to Canada's use of automated decision-making in immigration and refugee applications, to artificial-intelligence lie detectors deployed at European borders, States are keen to explore the use of new technologies, yet often fail to take into account profound human rights ramifications and real impacts on human lives. These technologies are largely unregulated, developed and deployed in opaque spaces with little oversight and accountability. This paper examines how technologies used in the management of migration impinge on human rights with little international regulation, arguing that this lack of regulation is deliberate, as States single out the migrant population as a viable testing ground for new technologies. Making migrants more trackable and intelligible justifies the use of more technology and data collection under the guise of national security, or even under tropes of humanitarianism and development. The way that technology operates is a useful lens that highlights State practices, democracy, notions of power, and accountability. Technology is not inherently democratic and human rights impacts are particularly important to consider in humanitarian and forced migration contexts. An international human rights law framework is particularly useful for codifying and recognising potential harms, because technology and its development is inherently global and transnational. More oversight and issue-specific accountability mechanisms are needed to safeguard fundamental rights of migrants such as freedom from discrimination, privacy rights and procedural justice safeguards such as the right to a fair decision-maker and the rights of appeal.

Keywords: *migration, migration management, new technologies, artificial intelligence, global governance, international human rights law*

1 INTRODUCTION: A LABORATORY OF HIGH-RISK EXPERIMENTS

States are increasingly turning to novel techniques to manage migration.[1] An unprecedented number of people are on the move due to conflict, instability, environmental

* I would like to thank Professor Eyal Benvenisti for his critical insights during my time at the University of Cambridge and Samer Muscati for his ongoing support.

1. Migration management is a theoretically contested term, yet is widely used in the literature on global governance of migration by various international organisations. For a broad overview of the concept, see Martin Geiger and Antoine Pécoud, 'The Politics of International Migration Management' in Martin Geiger and Antoine Pécoud (eds), *The Politics of International Migration Management* (Palgrave Macmillan, Basingstoke 2012) 1. Migration management has also been widely critiqued by various scholars and linked to broader theories such as

Journal compilation © 2019 Edward Elgar Publishing Ltd
The Lypiatts, 15 Lansdown Road, Cheltenham, Glos GL50 2JA, UK
and The William Pratt House, 9 Dewey Court, Northampton, MA 01060-3815, USA

factors and economic reasons. Receiving countries contend with the influx of large populations, straining resources and challenging border enforcement and national security. As a result, many States and international organisations involved in migration management are exploring technological experiments in various domains such as border enforcement, decision-making and data-mining. Yet all this experimentation occurs in a space that is largely unregulated, with weak oversight and governance mechanisms, driven by private-sector innovation. While discussions around appropriate regulation are emerging, the technological experimentation in migration occurs in opaque spaces where State accountability is weak.

This paper examines how technologies used in the management of migration impinge on human rights with little international regulation. I argue that this lack of regulation is deliberate, as States single out the migrant population as a viable testing ground for new technologies. The growing use of emerging technologies such as artificial intelligence (AI) and machine learning are new ways for States to create a differentiation of rights between citizens and non-citizens, exercise control over migrant populations, and externalise their responsibilities to uphold the human rights of migrants. Through agency laundering, States are able to distance themselves from suspect actions on complex and difficult decisions by outsourcing responsibility for technological innovation to the private sector, complicating the public–private accountability divide.

Technology is a useful lens through which to examine State practices, democracy, notions of power, and accountability.[2] Technology is by no means neutral[3] and can justify the differentiation of rights among citizens and non-citizens,[4] particularly regarding transparent processes, data collection, and experimentation with emerging technologies with far-reaching implications.[5] It is the normative universality of international human rights that presents a viable starting point for the global governance of migration management technologies,[6] recognising and codifying potential harms from a transnational and global perspective. However, the recognition and codification of human rights concerns have to be contextual to the unique issues around migration while simultaneously situated in the broader sphere of technological regulation. The differentiation of rights between citizens and non-citizens is not a new phenomenon. Foundational theories such as Butler's theory of State performativity and

biopower (see eg Achille Mbembe, 'Necropolitics' (2003) 15 Public Culture 11) and State performativity (Judith Butler, *Precarious Life: The Powers of Mourning and Violence* (Verso Books, London 2004)), some of which inform the analysis in this paper.

2. Ursula M Franklin, *The Real World of Technology* (House of Anansi Press, Toronto 1990).

3. Tarleton Gillespie, 'Algorithm' in Ben Peters (ed), *Digital Keywords: A Vocabulary of Information Society and Culture* (Princeton University Press, Princeton 2016) 18.

4. Nicholas P De Genova, 'Migrant "Illegality" and Deportability in Everyday Life' (2002) 31 Annual Review of Anthropology 419.

5. Petra Molnar and Lex Gill, 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System' (University of Toronto International Human Rights Program and the Citizen Lab, Munk School of Global Affairs, 2018) <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf> accessed 23 July 2019.

6. On the applicability of international human rights law (IHRL) to automated decision-making, see Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights as a Framework for Algorithmic Accountability' (2019) 68 International and Comparative Law Quarterly 309.

precarious life[7] can be expanded to State practices of technological control over populations through repeated actions and messaging around national security, border control and welfare of the State. The work of Arendt,[8] Agamben[9] and Carens[10] sheds light on the normalisation of contradictions around the differentiation of rights.

Emerging research is beginning to highlight how new technologies such as biometrics, Big Data and airport AI lie detectors by private companies such as iBorderCtrl[11] are used in the management of migration, but there is a gap in the scholarship on the disproportionate impact of technological experimentation on migrants and refugees without appropriate mechanisms of accountability and oversight.[12] This paper adds to these emerging conversations by arguing that new technologies challenge normative frameworks around decision-making and procedural protections, with the risk of creating legal black holes in which States seek to leave migrants beyond the duties and responsibilities enshrined in law. Rendering certain populations such as migrants more trackable and intelligible justifies more technology and data collection under the guise of national security, or even under tropes of humanitarianism and development. Yet technological development does not occur in a vacuum, but in fact replicates existing power hierarchies and differentials. Technology is not inherently democratic and issues of informed consent and right of refusal are particularly salient in humanitarian and forced migration contexts when, for example, refugees in Jordan have their irises scanned in order to receive their weekly rations under the justification of efficiency, while not being able to refuse biometric registration.[13] Technologies of migration management also operate in an inherently global context. They reinforce institutions, cultures, policies and laws, and exacerbate the gap between the public and the private sector, where the power to design and deploy innovation comes at the expense of oversight and accountability. Technologies

7. Judith Butler, *Precarious Life: Powers of Violence and Mourning* (Verso, London 2006).
8. Hannah Arendt, *The Origins of Totalitarianism* (Schocken Books, New York 1951).
9. Giorgio Agamben, *State of Exception* (University of Chicago Press, Chicago 2005).
10. Joseph H Carens, *The Ethics of Immigration* (OUP, Oxford 2013).
11. Robb Picheta, 'Passengers to face AI lie detector tests at EU airports' (CNN, 3 November 2018) <https://edition.cnn.com/travel/article/ai-lie-detector-eu-airports-scli-intl/index.html> accessed 23 July 2019.
12. See eg Fleur Johns, 'Data, Detection, and the Redistribution of the Sensible in International Law' (2017) 111 American Journal of International Law 57 and Raluca Csernatoni, 'Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management' (2018) 27 European Security 175. On broader theories around surveillance of migrants see Jeremy Wickins, 'The Ethics of Biometrics: The Risk of Social Exclusion from the Widespread Use of Electronic Identification' (2007) 13 Science and Engineering Ethics 45; Rebekah Thomas, 'Biometrics, International Migrants and Human Rights' (2005) 7 European Journal of Migration and Law 377; Shoshana Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Duke University Press, Durham 2011); Achraf Farraj, 'Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers' (2011) 42 Columbia Human Rights Law Review 891. On data collection, biometrics and power relations, see eg Daniel A McFarland and Richard H McFarland, 'Big Data and the Danger of Being Precisely Inaccurate' (2015) 2 Big Data and Society 1; Alice Edwards, 'A Numbers Game: Counting Refugees and International Burden-Sharing' (public lecture delivered at the University of Tasmania Law School, 19 December 2012) <www.refworld.org/docid/512c75de2.html> accessed 23 July 2019.
13. Bethan Staton, 'Eye Spy: Biometric Aid System Trials in Jordan' (IRIN, 18 May 2016) <www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan> accessed 23 July 2019.

have the power to shape democracy[14] and influence elections,[15] through which they can reinforce the politics of exclusion. Technologies also reinforce the North–South power asymmetries and concretise which locales are seen as innovation centres, while spaces like conflict zones and refugee camps become sites of experimentation under the guise of humanitarianism and empowerment of migrants through innovation.[16]

The first part of this paper (Section 2) is purposefully descriptive, laying the groundwork on how new technologies are being experimented with in migration management, highlighting some of the central problems that have been documented in border spaces, refugee camps, airports and administrative tribunals. Section 3 then analyses what few global governance mechanisms exist and takes an international human rights law perspective to situate the very real ramifications of these technologies in an opaque and discretionary space with little oversight and accountability. The unique context of migration must be the central consideration, given the very real risks to life, liberty and security, as well as heightened privacy considerations. Section 4 then queries why States are so reluctant to codify laws and regulation around migration management technologies, arguing that it is the very nature of the differentiation of rights available to migrants and non-citizens that makes migration management the perfect laboratory for technological experiments.[17] This paper takes a socio-legal approach to situate the lack of a global governance framework into wider social contexts, trends, and histories of migration management, drawing on literature from legal anthropology and discourse theory in order to make sense of the international reluctance to codify and regulate technological experimentation on migrants. Tracking, coding, surveilling and controlling migrants is nothing new; what is novel are the tools available to States in an increasingly xenophobic and sovereigntist world, prioritising innovation at the expense of almost everything else.[18]

2 KNOWN AND UNKNOWN EXPERIMENTS WITH NEW TECHNOLOGIES OF MIGRATION MANAGEMENT

The introduction of new technologies impacts both the processes and outcomes associated with decisions that would otherwise be made by administrative tribunals, immigration officers, border agents, legal analysts and other officials responsible for the administration of immigration and refugee systems, border enforcement and refugee response management. Technology also develops at a rapid pace and States are

14. Karen Hao, 'Why AI is a Threat to Democracy – And What We Can Do to Stop It' (The MIT Technology Review, 26 February 2019) <www.technologyreview.com/s/613010/why-ai-is-a-threat-to-democracyand-what-we-can-do-to-stop-it/> accessed 23 July 2019.

15. See eg Martin Russell and Ionel Zamfir, 'Digital Technology in Elections: Efficiency versus Credibility?' (European Parliamentary Research Service Briefing, PE 625.178, September 2018).

16. See eg initiatives such as 'Techfugees: Empowering the Displaced Through Technology' <https://techfugees.com/> accessed 17 March 2019.

17. See Molnar and Gill (n 5).

18. A note on methodology: in addition to its original analysis, this paper draws on various conversations, meetings and consultations with government officials, private-sector actors, activists and lawyers involved in the emerging conversations around the regulation of AI and new technologies between fall of 2018 and 2019. Under the Chatham House rules, no individuals are publicly identified but their aggregate insights inform the arguments of this paper.

engaged in an international race for AI leadership, a 'new gold rush'.[19] For example, as of 2019, there are 23 separate national or supranational AI strategies, many worth billions of dollars.[20] This influx of interest and investment has made AI and machine learning attractive and well-funded research areas for the public and private sectors alike. Technological innovations often come with the promise of increased fairness and efficiency. In response to complex issues like the global migration of millions, States are eager to see new technologies as a quick solution to what are otherwise tremendously complex and often intractable policy issues.[21] However, before analysing the particular uses of new technologies in migration, I will first explore some definitions relevant to understanding the parameters of these technological experiments.

2.1 What constitutes artificial intelligence?

Conceptual clarity in defining new technologies can be difficult. AI, machine learning, automated decision systems and predictive analytics are a series of overlapping terms and refer to a class of technologies that assist or replace the judgment of human decision-makers. These systems, which can be taught and can learn, will behave in various ways through various techniques. Different disciplines or regulatory mechanisms also use different definitions.[22] As such, delineating the limits of what constitutes AI can be difficult. For clarity, this paper will refer to all AI technologies discussed as automated decision-making. This can include technologies that automate the mining of vast stores of data as well as processes that mimic human cognition and come up with novel decisions about outcomes.

19. Aaron Shull, 'In the Global Race for AI, How Do We Ensure We're Creating a Better World?' (Centre for International Governance Innovation, 15 February 2019) <www.cigionline.org/articles/global-race-ai-how-do-we-ensure-were-creating-better-world> accessed 23 July 2019.
20. Tim Dutton, 'An Overview of National AI Strategies' (Medium, 29 June 2018) <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> accessed 23 July 2019.
21. See eg the participation of numerous States at initiatives such as refugee 'hackathons' (or a collaborative flash event in which programmers and designers endeavour to create new solutions, programs or technologies): 'Hackathon' (Techfugees, 2019) <https://techfugees.com/tag/hackathon/> accessed 25 July 2019 and 'Welcome to the 2nd Edition of the Hackathon for Peace, Justice and Security' (Data Science Initiative, 2019) <www.hackathonforgood.org/> accessed 25 July 2019. See also comments by the Government of Canada on using AI to 'help us address some of our most challenging problems': Government of Canada, 'Government of Canada Creates Advisory Council on Artificial Intelligence' (Cision, 14 May 2019) <www.newswire.ca/news-releases/government-of-canada-creates-advisory-council-on-artificial-intelligence-838598005.html> accessed 25 July 2019.
22. See eg Amnesty International and Access Now, 'The Toronto Declaration: Protecting the Rights to Equality and Non-Discrimination in Machine Learning Systems' (Access Now, 16 May 2018) <www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf> accessed 23 July 2019; Université de Montréal, 'Montreal Declaration for a Responsible Development of AI' (Université de Montréal, 2017) <www.montrealdeclaration-responsibleai.com/the-declaration> accessed 23 July 2019; or Regulation 2016/679 of the European Parliament and of the Council 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 L119/1 (General Data Protection Regulation or GDPR).

Automated decision systems process information in the form of input data, using an algorithm to generate an output. An algorithm can be thought of as a set of instructions, like 'a recipe composed in programmable steps … organizing and acting on a body of data to quickly achieve a desired outcome'.[23] Certain algorithms are 'trained' using a large, existing corpus of data, which allows the algorithm to classify and 'generalize beyond the examples in the training set'.[24] Training data can be a body of case-law, a collection of photographs or a database of statistics, some or all of which have been pre-categorised or labelled based on the designer's criteria.

Algorithms have been criticised for being 'black boxes'.[25] This is because an algorithm's source code, its training data or other inputs may be proprietary, and can be shielded from public scrutiny on the basis of intellectual property legislation or as confidential business assets. Moreover, when algorithms are used in immigration and refugee matters, and form a nexus with issues of national security, both input data and source code may also be classified.[26] However, without being able to scrutinise input data to understand how the algorithm starts to make decisions, iterate and improve upon itself in unpredictable or unintelligible ways, their logic becomes less and less intuitive to human oversight. One of the main concerns with not being able to scrutinise and critique automated decision-making is the introduction of bias. Training data can be coloured by direct or indirect human agency and pre-existing bias, or when seemingly non-discriminatory variables become 'proxies' for other categories, such as postal codes serving as proxies of race.[27] In the United States, the COMPAS algorithm used to predict the likelihood of crime recidivism has been widely criticised for falsely recommending racialised individuals for higher pre-custodial sentences than white offenders.[28]

Algorithms are vulnerable to the same decision-making concerns that plague human decision-makers: transparency, accountability, discrimination, bias and error.[29] All of these concerns are relevant to automating migration, which is already permeated by biased decision-making by human officers.

2.2 New technologies of migration management

Immigration and refugee decision-making sits at an uncomfortable legal nexus: the impact on the rights and interests of individuals is often very significant, even where the degree of deference is high and the procedural safeguards are weak. There is also a serious lack of clarity surrounding how courts will interpret

23. See Gillespie (n 3) 19.
24. Ibid.
25. See eg Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard UP, Cambridge MA 2015).
26. Molnar and Gill (n 5) 18.
27. Council of Europe, 'Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications' (Council of Europe Study DGI(2017)12, March 2018) 26 <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> accessed 12 August 2019.
28. Jeff Larson, Surya Mattu, Lauren Kirchner et al, 'How We Analyzed the COMPAS Recidivism Algorithm' (ProPublica, 23 May 2016) <www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> accessed 23 July 2019.
29. Zeynep Tufekci, 'Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency' (2015) 13 Colorado Technology Law Journal 203, 216–217.

administrative law principles like natural justice, procedural fairness and standard of review where an automated decision system is concerned.

Four major areas of concern that are emerging in the technological experimentation in migration management are data collection, biometrics and consent, criminalisation and surveillance, and automated decision-making.

2.2.1 Data-driven humanitarianism and data colonialism[30]

Automated decision-making technologies require vast amount of data on which to learn.[31] Big Data analytics require extremely large sets, which are analysed for patterns and associations to make determinations about the likelihood of future human behaviour. Multiple organs of the United Nations (UN) have begun relying on Big Data analytics to inform their policies.[32] For example, the International Organization for Migration's Displacement Tracking Matrix[33] monitors populations on the move to better predict the needs of displaced people, using mobile phonecall records and geotagging, as well as analyses of social media activity. Data analytics are also used to predict likely successful outcomes of resettled refugees based on pre-existing community links in the United States.[34] There is also the rise in the use of biometrics, or the 'automated recognition of individuals based on their biological and behavioural characteristics', in migration management. Biometrics can include fingerprint data, retinal scans and facial recognition, as well as less well-known methods such as the recognition of a person's vein and blood vessel patterns, ear shape and gait, among others.[35] The UN has been relying on populating its datasets with biometrics, collecting biodata on more than 8 million people, most of them fleeing conflict or needing humanitarian assistance.[36]

However, data collection is not an apolitical exercise, particularly when powerful Global North actors collect information on vulnerable populations with no regulated methods of oversights and accountability. The increasingly fervent collection of data

30. Nick Couldry and Ulises Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20 Television & New Media 336.
31. Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 University of California Davis Law Review 1149.
32. Olivia De Backer, 'Big Data and International Migration' (United Nations Global Pulse: Pulse Lab Diaries, 16 June 2014) <www.unglobalpulse.org/big-data-migration> accessed 23 July 2019.
33. International Organization for Migration, 'Displacement Tracking Matrix' (IOM DTM, 2019) <www.globaldtm.info/> accessed 23 July 2019.
34. Alex Shashkevich, 'Stanford Scholars Develop New Algorithm to Help Resettle Refugees and Improve Their Integration' (Stanford News, 18 January 2018) <https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/> accessed 23 July 2019.
35. 'What is Biometrics' (Biometrics Institute, 2019) <https://www.biometricsinstitute.org/what-is-biometrics/> accessed 23 July 2019.
36. These enormous datasets are notoriously hard to track and can also include the retrofitting of old data with newly collected biometrics. See eg statements publicly made by UNHCR officials at the 2018 Humanitarian Congress in Berlin, Germany: '20 Years Humanitarian Congress Berlin' (Humanitarian Congress Berlin, 17–18 October 2019) <http://humanitarian-congress-berlin.org/2018/> accessed 17 March 2019. See also N Cohen, 'Do No Digital Harm' (IRIN News, 17 October 2018) <http://www.irinnews.org/feature/2018/10/17/do-no-digital-harm> accessed 23 July 2019.

on migrant populations has been criticised for its potential to result in significant privacy breaches and human rights concerns.[37] For example, in the case of collecting biometric data on Rohingya refugees in Myanmar, the so-called datafication of refugee responses can result in oppressive governments easily identifying groups and removing them from encampments.[38] China has also been collecting facial recognition and location tracking on its Muslim minority Uighur populations in a so-called 'Muslim-tracking database'.[39]

This data collection on marginalised groups is deeply historical. For example, Nazi Germany strategically collected vast amounts of data on Jewish communities to facilitate the Holocaust, largely in partnership with the now-ubiquitous IBM.[40] Various other genocides also relied on systematic tracking of groups, such as the Tutsi registries based on ethnicity identity cards, which facilitated the magnitude of the Rwandan genocide in 1994.[41] Post 9/11, the US also experimented with various modes of data collection on suspicious populations through the US Department of Homeland Security's National Security Entry-Exit Registration System (NSEERS), which collected photographs, biometrics and even first-person interview data from over 84,000 flagged individuals coming from mostly Arab States.[42] The Trump Administration echoed these sentiments with its planned 'Muslim Registry', upheld by the Supreme Court of the United States of America,[43] or through its plans for an 'Extreme Vetting Initiative', discussed in greater detail below. All of these efforts highlight a common goal of tracking particular groups under the guise that more data is always better. Even global efforts such as the 2018 'Global Compact for Safe, Orderly and Regular Migration' foreground the preoccupation with collecting data, listing data collection as the first of its 23 objectives.[44]

In an increasingly anti-immigrant global landscape, criticisms have also surfaced that migration data has also been misinterpreted and misrepresented for political ends, for example to affect the distribution of aid dollars and resources.[45] Inaccurate

37. Jeff Crisp, 'Beware the Notion That Better Data Lead to Better Outcomes for Refugees and Migrants' (Chatham House, 9 March 2019) <www.chathamhouse.org/expert/comment/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants> accessed 23 July 2019.
38. Elise Thomas, 'Tagged, Tracked and in Danger: How the Rohingya got Caught in the UN's Risky Biometric Database' (Wired Magazine, 12 March 2018) <www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh> accessed 23 July 2019.
39. Catalin Cimpanu, 'Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online' (ZDNet, 14 February 2019) <www.zdnet.com/google-amp/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/?__twitter_impression=true> accessed 23 July 2019.
40. Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* (Dialog Press, New York 2012).
41. Zara Rahman, 'Dangerous Data: The Role of Data Collection in Genocides' (Engine Room, 21 November 2016) <www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/> accessed 23 July 2019.
42. Arab American Institute, 'National Security Entry-Exit Registration System (NSEERS)' (Arab American Institute, 2016) <www.aaiusa.org/nseers> accessed 18 March 2019.
43. *Trump v Hawaii*, No 17-965 (US Supreme Court).
44. Global Compact for Safe, Orderly and Regular Migration, UNGA Res 73/195 (19 December 2018).
45. Nature Editorial Team, 'Data on Movements of Refugees and Migrants are Flawed' (Nature, 2017) <www.nature.com/news/data-on-movements-of-refugees-and-migrants-are-flawed-1.21568> accessed 23 July 2019.

data can also be used to stoke fear and xenophobia, as seen in the characterisation[46] of the group of migrants attempting to claim asylum at the US–Mexico border. Societal fear is then used as a justification for increasingly hard-line responses that contravene international law[47] and present profound concerns around basic civil liberties and human rights.

2.2.2 Biometrics and consent

The collection of vast amounts of data on particular groups also presents issues around data-sharing and access.[48] While exchanging data on humanitarian crises or biometric identification is often presented as a way to increase efficiency and inter-agency and inter-state cooperation, benefits from the collection do not accrue equally. Data collection and the use of new technologies, particularly in spaces with clear power differentials, raise issues of informed consent and the ability to opt out. For example, when people in Jordanian refugee camps have their irises scanned in order to receive their weekly food rations in an experimental new program, are they able to meaningfully say no?[49] In an IRIN investigation inside the Azraq refugee camp,[50] most refugees interviewed were uncomfortable with such technological experiments but felt that they could not refuse if they wanted to eat. Consent cannot be truly informed and freely given if it is given under coercion, even if the coercive circumstances masquerade as efficiency and promise improved service delivery.

Further, it is unclear where all this collected biometric data is going and whether affected groups have access to their own data. In the Jordanian iris-scanning pilot project, the UN High Commissioner for Refugees (UNHCR) expressly reserved the right to collect and share data with third parties,[51] including the private sector, without clear safeguards and despite significant privacy concerns. The UN's World Food Program (WFP) was also recently criticised for partnering with data-mining company Palantir Technologies for a US$45 million contract and sharing the data of 92 million aid recipients.[52] Palantir has been heavily criticised for providing the technology that supports the detention and deportation programmes run by the US Immigration and Customs

46. Stephanie Silverman, 'The Bogus Demonization of the "Migrant Caravan"' (The Conversation, 10 December 2018) <https://theconversation.com/the-bogus-demonization-of-the-migrant-caravan-107562> accessed 23 July 2019.
47. Blake Ellis, Melanie Hicken and Bob Ortega, 'Handcuffs, Assaults, and Drugs Called "Vitamins": Children Allege Grave Abuse at Migrant Detention Facilities' (CNN, 22 June 2018) <https://edition.cnn.com/2018/06/21/us/undocumented-migrant-children-detention-facilities-abuse-invs/index.html> accessed 23 July 2019.
48. David Lyon, 'Biometrics, Identification, and Surveillance' (2008) 22 Bioethics 499, 499–508.
49. See also Johns (n 12).
50. See Staton (n 13).
51. The UNHRC also contracts its data management to the international firm Accenture. See eg UNHCR's Accenture contract: Accenture, 'UNHCR: Innovative Identity Management System Uses Biometrics to Better Serve Refugees' (Accenture, 2015) <www.accenture.com/t20161026T063323Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_15/Accenture-Unhcr-Innovative-Identity-Management-System.pdf> accessed 12 August 2019.
52. Ben Parker, 'New UN Deal with Data Mining Firm Palantir Raises Protection Concerns' (The New Humanitarian, 5 February 2019) <www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp> accessed 12 August 2019.

Enforcement (ICE) and the Department of Homeland Security (DHS).[53] It is not yet clear what data-sharing accountability mechanism will be in place during the WFP–Palantir partnership or whether data subjects will be able to opt out.

2.2.3 Criminalisation and securitisation

Autonomous technologies are also increasingly used in monitoring and securing border spaces. For example, FRONTEX, the European Border and Coast Guard Agency, has been testing various unpiloted military-grade drones in the Mediterranean for the surveillance and interdiction of migrant vessels hoping to reach European shores to facilitate asylum applications.[54] The ROBORDER project aims to create a 'fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles'.[55] The usage of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security and the increasing push towards the criminalisation of migration. Globally, States, particularly those on the frontiers of large numbers of migrant arrivals, have been using various ways to pre-empt and deter those seeking to legally apply for asylum. This normative shift towards criminalisation – or what Csernatoni terms 'dronisation'[56] – of migration works to justify increasingly hard-line and intrusive technologies such as drones and various border enforcement mechanisms like remote sensors and integrated fixed-towers with infra-red cameras to mitigate the 'threat environment' at the border.[57] These technologies can have drastic results. While so-called 'smart-border' technologies have been called a more 'humane' alternative to the Trump Administration's calls for a physical wall, studies have documented that policies of prevention through deterrence using new surveillance technologies along the US–Mexico border have actually increased migrant deaths and pushed migration routes towards more dangerous terrain through the Arizona desert.[58] Chambers et al have found that migrant deaths have more than doubled since these new technologies have been introduced,[59] creating a 'land of open graves'.[60] The use of these technologies by border enforcement is only likely to increase in the 'militarised technological regime'[61] of border spaces, without appropriate public consultation, accountability frameworks and oversights mechanisms.

53. Karen Hao, 'Amazon is the Invisible Backbone of ICE's Immigration Crackdown' (MIT Technology Review, 22 October 2018) <www.technologyreview.com/s/612335/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/> accessed 23 July 2019.
54. Csernatoni (n 12) 183.
55. Roborder, 'Aims and Objectives' (Roborder) <https://roborder.eu/the-project/aims-objectives/> accessed 23 July 2019.
56. Csernatoni (n 12) 178.
57. Ibid 188.
58. Samuel Norton Chambers, Sarah Launius, Geoffrey Alan Boyce et al, 'Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.–Mexico Border: A Geospatial Modeling of the Geography of Deterrence' (2019) 25 Journal of Borderlands Studies 1.
59. Ibid 3.
60. Jason De Leon, *The Land of Open Graves: Living and Dying on the Migrant Trail* (University of California Press, Berkeley 2015).
61. Csernatoni (n 12) 178.

2.2.4 *Individual automated decision-making in immigration and refugee decisions*

To deal with multiple complex migration crises, States are also experimenting with automating various facets of decision-making. For example, since at least 2014, Canada has been using some form of automated decision-making in its immigration and refugee system.[62] A 2018 University of Toronto report examined the human rights risks of using AI to replace or augment immigration decisions and argued that these processes 'create a laboratory for high-risk experiments within an already highly discretionary and opaque system'.[63] The ramifications of using automated decision-making in the immigration and refugee space are far-reaching. Hundreds of thousands of people enter Canada every year through a variety of applications for temporary and permanent status.[64] While the Canadian government has confirmed that currently this type of technology is confined only to augmenting human decision-making and reserved for certain immigration applications only,[65] currently there is no legal mechanism in place protecting people's procedural rights and preventing human rights abuses from occurring.

In other jurisdictions, these experiments with automation are already in full force. In the wake of the Trump administration's executive orders enforcing increasingly hard-line measures to stem immigration, a Vice Media investigation revealed that ICE has been amending its bail-determination algorithm at the USA–Mexico border to justify the detention of migrants in every single case.[66] In 2017, ICE also unveiled its 'Extreme Vetting Initiative', a process of automated assessments of immigrants to determine the probability that an applicant would be a 'positively contributing member of society' and to national interests, and 'predict whether they intend to commit criminal or terrorist acts after entering the country'.[67] Other countries such as New Zealand are also experimenting with using automated facial recognition technology based on biometrics to identify so-called future 'troublemakers' which civil society organisations are fighting against on grounds of discrimination and racial profiling.[68] As discussed above, instances of bias in automated decision-making and facial-recognition-type technology are widely documented.[69] When algorithms rely on biased data, they produce biased results.

62. Nicholas Keung, 'Canadian Immigration Applications Could Soon be Assessed by Computers' (Toronto Star, 5 January 2017) <www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html> accessed 23 July 2019.
63. Molnar and Gill (n 5) 1.
64. Ibid 4.
65. For example, temporary visa applications from India and China only: conversations with Immigration, Refugees, and Citizenship Canada with the author.
66. Daniel Oberhaus, 'ICE Modified its "Risk Assessment" Software so it Automatically Recommends Detention' (VICE, 26 June 2018) <https://motherboard.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention> accessed 23 July 2019.
67. April Glaser, 'ICE Wants to Use Predictive Policing Technology for its "Extreme Vetting" Program' (Slate, 8 August 2017) <https://slate.com/technology/2017/08/ice-wants-to-use-predictive-policing-tech-for-extreme-vetting.html> accessed 23 July 2019.
68. Lincoln Tan, 'Immigration NZ's Data Profiling "Illegal" Critics Say', The New Zealand Herald (Auckland, 5 April 2018) <www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585> accessed 23 July 2019.
69. See eg James Vincent, 'Gender and Racial Bias Found in Amazon's Facial Recognition Technology (Again)' (The Verge, 25 January 2019) <www.theverge.com/2019/1/25/18197137/amazon-rekognition-facial-recognition-bias-race-gender> accessed 23 July 2019.

These biases could have far-reaching results if they are embedded in the emerging technologies being used experimentally in migration. For example, in airports in Hungary, Latvia and Greece, a new pilot project by a company called iBorderCtrl has introduced AI-powered lie detectors at border checkpoints.[70] Passengers' faces will be monitored for signs of lying, and if the system becomes more 'sceptical' through a series of increasingly complicated questions, the person will be selected for further screening by a human officer. However, it is unclear how this system will be able to handle cultural differences in communication, or account for trauma and its effects on memory, such as when dealing with a traumatised refugee claimant.[71] Refugee and immigration claims are filled with nuance and complexity, qualities that may be lost on automated technologies, leading to serious breaches of internationally and domestically protected human rights in the form of bias, discrimination, privacy breaches, and due process and procedural fairness issues, among others. It is not yet clear how the right to a fair and impartial decision-maker and the right to appeal a decision will be upheld during the use of automated decision-making systems.

Unfortunately, government surveillance, policing, immigration enforcement and border-security programs can incentivise and reward industry for developing rights-infringing technologies.[72] Among them is Amazon's 'Rekognition' surveillance and facial recognition system, which is being marketed explicitly for use by law enforcement.[73] Using deep learning techniques, Rekognition is able to identify, track and analyse individuals in real time, recognise up to 100 people in a single image and analyse collected information against mass databases of faces. This 'person tracking' service will allow the government to identify, investigate and monitor 'people of interest', including in crowded group photos and in public places such as airports.[74]

The technology has already been criticised by the American Civil Liberties Union, which has demanded that Amazon stop allowing governments to use the technology, citing 'profound civil liberties and civil rights concerns'.[75] Amazon's own workforce has led this call, and demanded that Amazon cut its ties[76] with the controversial data analytics firm called Palantir Technologies. Palantir is responsible for providing the

70. Picheta (n 11). With Hungary and Greece being two of the crucial entry points for refugee claimants into mainland Europe, it is perhaps no accident that these locations were chosen as the site of experimentation.

71. These issues, of course, also exist with human decision-makers, and there are increasingly cogent critiques about officers misunderstanding how the psychological effects of repeated trauma can impact a person's ability to testify and appear 'truthful'. See eg the work of Hilary Evans Cameron, *Refugee Law's Fact-Finding Crisis: Truth, Risk, and the Wrong Mistake* (CUP, Cambridge 2018).

72. Natasha Duarte, 'ICE Finds Out It Can't Automate Immigration Vetting: Now What?' (CDT Blog, 22 May 2018) <https://cdt.org/blog/ice-cant-automate-immigration-vetting/> accessed 23 July 2019.

73. Matt Cagle and Nocle Ozer, 'Amazon Teams Up with Law Enforcement to Deploy Dangerous New Face Recognition Technology' (American Civil Liberties Union Northern California, 22 May 2018) <www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology> accessed 12 August 2019.

74. Ibid.

75. Ibid.

76. Kate Conger, 'Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts with Law Enforcement' (*Gizmodo,* 22 June 2018) <https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509> accessed 23 July 2019.

technology that supports the detention and deportation programs run by the ICE and the Department of Homeland Security, which Amazon workers have decried as an 'immoral U.S. policy'[77] and part of the US's increasingly hard-line treatment of refugees and immigrants.

Nevertheless, there are also some encouraging developments. For example, an automatic robotic life-raft called Emily, or Emergency Integrated Lifesaving Lanyard, has been deployed in the waters around the Greek Islands to assist with rescuing refugees.[78] The UNHCR has been experimenting with a bot examining xenophobia and racism against refugees online[79] to help with advocacy strategies. New digital verification technologies have also made analysing data coming from conflict zones more reliable, which can be beneficial for refugees requiring evidence to bolster their claims for protection.[80] A whole sector has also proliferated around creating various apps to assist refugees with accessing social services such as healthcare, banking and language acquisition, including various initiatives such as Techfugees, which foster entrepreneurship among refugee communities and whose tagline is 'empowering the displaced through technology'.[81]

However, piecemeal interventions under the guise of empowerment fail to consider that the issues around emerging technologies in the management of migration are not about the inherent use of technology but rather about how it is used and by whom. The monopolies of knowledge which are being created function to consolidate power and authority over technological development, with States and private actors setting the stage for what is possible. The unequal distribution of benefits from technological development privileges the private sector as the primary actor in charge of development, with States and governments wishing to control the flows of migrant populations benefiting from these technological experiments. Governments are the primary agents who benefit from data collection[82] and affected groups are relegated to the margins. It is therefore not surprising that the regulatory and legal space around the use of these technologies remains murky and underdeveloped, full of discretionary decision-making, privatised development and uncertain legal ramifications.

Section 3 of this paper will lay out what limited legal frameworks exist for the governance of new technologies in migration management and interrogate existing and emerging human rights obligations for States.

77. Ibid.
78. Julia Franz, 'It's a Buoy, it's a Life Raft, it's Emily – The Robotic Craft that's Saving Refugees off the Coast of Greece' (PRI, 1 May 2017) <www.pri.org/stories/2017-05-01/it-s-buoy-it-s-life-raft-it-s-emily-robotic-craft-s-saving-refugees-coast-greece> accessed 23 July 2019.
79. Rebeca Moreno, 'Teaching a "Robot" to Detect Xenophobia Online' (UNHCR Innovation Service, 2017) <www.unhcr.org/innovation/teaching-robot-detect-xenophobia-online/> accessed 23 July 2019.
80. See eg Amnesty International's Digital Verification Project: 'Digital Verification Corp' (Amnesty International, 23 November 2017) <www.amnesty.org/en/latest/news/2017/11/amnesty-international-and-trulymedia-join-forces-in-fight-against-fake-news/> accessed 12 August 2019.
81. 'Techfugees: Empowering the Displaced with Technology' (Techfugees, 2019) <https://techfugees.com/> accessed 23 July 2019.
82. Ruth Okediji, 'Does Intellectual Property Need Human Rights?' (2018) 51 NYU Journal of International Law and Politics 1.

3 REGULATORY FRAMEWORKS AND HUMAN RIGHTS IMPACTS

A number of internationally protected rights are already engaged in the increasingly widespread use of new technologies that manage migration. However, currently there is no integrated regulatory global governance framework for the use of automated technologies, and no specific regulations in the context of migration management. Much of the global conversation centres on ethics without clear enforceability mechanisms.

Various countries have begun the process of setting up piecemeal guidelines on the use of AI. For example, in April 2018, the European Commission adopted the Communication on Artificial Intelligence,[83] creating the 'European AI Alliance', and a new set of AI ethics guidelines to address issues such as fairness, safety and transparency, with its High-Level Expert Group on Artificial Intelligence tasked with establishing recommendations on future-related policy development and on ethical, legal and societal issues related to AI.[84] Countries like the Netherlands[85] and Canada[86] are leading in the establishment of certification and assessments for responsible and ethical AI. Outside of North America and Europe, India has established its inclusive AI strategy 'AIforAll',[87] while Kenya recently announced the formation of a taskforce[88] to provide guidance on Blockchain and AI-related technologies' application in the areas of financial inclusion, cybersecurity, election processes and public-service delivery.

While binding regional mechanisms that touch on the use of automated decision-making, such as Article 22 of the European Union's (EU) General Data Protection Regulation (GDPR), are being implemented and guiding principles for the development of ethical standards in engineering and design are also being explored, there are currently no legally binding international legal documents to regulate these technologies and limit their risks. However, States are already bound by the rules of customary international law that can also apply to the development of new technologies.[89]

This section will analyse some of these principles and rules, and argue that more specific regulation is required to protect against human rights infringements in the

83. European Commission, 'Communication on Artificial Intelligence for Europe' (COM (2018) 237, 25 April 2018) <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe> accessed 23 July 2019.

84. See also Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (HL 2017–2019, 100).

85. Consultancy EU, 'Deloitte Launches Certified Quality Mark for AI and Robotics' (Consultancy EU, 2018) <www.consultancy.eu/news/2043/deloitte-launches-certified-quality-mark-for-ai-and-robotics> accessed 23 July 2019.

86. Government of Canada, 'Algorithmic Impact Assessment' (Government of Canada, 2019) <https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/automated-decision-automatise/en/algorithmic-impact-assessment.html> accessed 23 July 2019.

87. Government of India, 'National Strategy for Artificial Intelligence #AIforAll' (2018) <http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf> accessed 23 July 2019.

88. Kenyan Wall Street, 'Kenya Govt Unveils 11 Member Blockchain & AI Taskforce Headed by Bitange Ndemo' (Kenyan Wall Street, 28 February 2018) <https://kenyanwallstreet.com/kenya-govt-unveils-11-member-blockchain-ai-taskforce-headed-by-bitange-ndemo/> accessed 23 July 2019.

89. Rosemary Rayfuse, 'Public International Law and the Regulation of Emerging Technologies' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP, Oxford 2018) 503.

use of new technologies, particularly given how far-reaching the ramifications can be in immigration and refugee implementations. An international human rights law (IHRL) framework is particularly useful for codifying and recognising potential harms, because technology and its development is inherently global and translational. Under IHRL, States must commit to preventing violations from occurring, establish monitoring and oversight, and provide remedy and redress for rights violations to hold violators accountable.[90] This also includes the obligations of a State to protect individuals from harms perpetrated by third parties, including private entities.[91]

However, States are willing to experiment with these new unregulated technologies in the space of migration precisely because it is a discretionary space of opaque decision-making. Moreover, much of migration management is also enacted by international organisations such as the UNHCR and various other bodies. As non-State actors operating under various legal and quasi-legal authorities and regulations globally, international organisations are 'arenas for acting out power relationships'[92] without being beholden to the responsibilities that States have to protect human rights. As Benvenisti argues, States that operate through international organisations can also 'launder' their legal responsibility for acts or omissions that are attributed to the organisation.[93] With the proliferation of technologies in what Shkabatur has termed the 'global panopticon',[94] international organisations are overly empowered to administer technology without being beholden to rights-protecting laws and principles, resulting in problems with compliance.[95] While perhaps no longer 'the harbingers of international happiness',[96] international organisations are definitely the harbingers of how power is differentially distributed when it comes to migration management technology.

What follows is a brief overview of existing rights that are already engaged in the proliferation of various migration management technologies profiled above. It is not meant as an exhaustive discussion but more as a snapshot of the far-reaching ramifications of technological experiments on migrants' lives and wellbeing, in an unregulated arena with few mechanisms of redress.

90. UN Human Rights Committee, 'General Comment No 31 on the Nature of the Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13, paras 3–8.
91. UN Human Rights Council, 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, on Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (21 March 2011) UN Doc A/HRC/17/31, principles 1–10.
92. Tony Evans and Peter Wilson, 'Regime Theory and the English School of International Relations: A Comparison' (1992) 21 Millennium: Journal of International Studies 329, 330.
93. Eyal Benvenisti, 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29 European Journal of International Law 1, 18.
94. Jennifer Shkabatur, 'A Global Panopticon? The Changing Role of International Organizations in the Information Age' (2011) 33 Michigan Journal of International Law 159.
95. See eg Kal Raustiala and Anne-Marie Slaughter, 'International Law, International Relations and Compliance' in Walter Carlsnaes, Thomas Risse and Beth A Simmons (eds), *Handbook of International Relations* (Sage, Thousand Oaks 2002) 538–539.
96. Jan Klabbers, 'The Life and Times of the Law of International Organizations' (2001) 70 Nordic Journal of International Law 287, 288.

3.1 Life and liberty

The far-reaching impact of new technologies on the lives and security of persons affected should not be underestimated. The right to life and liberty is one of the most fundamental internationally protected rights and highly relevant to migration and refugee contexts. The Convention Relating to the Status of Refugees,[97] with its accompanying Protocol,[98] enshrines the right to seek protection from persecution when life, liberty and security are threatened, including the right not to be returned to a country where persecution and risk to life is likely, under the principle of nonrefoulement. Numerous other specific legal instruments, such as the International Covenant on Civil and Political Rights (ICCPR),[99] Convention Against Torture and Other Cruel, Inhumane or Degrading Treatment or Punishment (CAT),[100] Convention on the Rights of Persons with Disabilities (CRPD),[101] Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW),[102] The Convention on the Rights of the Child (CRC),[103] and the International Convention on the Elimination of All Forms of Racial Discrimination (CERD)[104] also recognise the right to liberty and security for all persons.

Multiple technological experiments already impinge on the right to life and liberty. The starkest example is the denial of liberty when migrants are placed in administrative detention at the US–Mexico border. Immigration detention is an opaque and discretionary phenomenon,[105] and the justification of increased incarceration on the basis of algorithms that have been tampered with shows just how far the State is willing to justify incursions on basic human rights under the guise of national security and border enforcement. Errors, mis-calibrations, and deficiencies in training data can result in rights-infringing outcomes. For example, aspects of training data which are mere coincidences in reality may be treated as relevant patterns by a machine-learning system, leading to outcomes which are considered arbitrary when examined against the purpose of the governing statute. This is one reason why the GDPR requires the ability

97. Convention Relating to the Status of Refugees (adopted 28 July 1951, entered into force 22 April 1954) 189 UNTS 150 (Refugee Convention).
98. Protocol Relating to the Status of Refugees (adopted 31 January 1967, entered into force 4 October 1967) 606 UNTS 267.
99. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 9. See also Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR) art 3.
100. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85 (CAT).
101. Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 3 May 2008) 2515 UNTS 3 (CRPD) art 14.
102. Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW).
103. Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).
104. International Convention on the Elimination of All Forms of Racial Discrimination (adopted 7 March 1966, entered into force 4 January 1969) 66 UNTS 195 (CERD) art 5(b), for example.
105. Stephanie Silverman and Petra Molnar, 'Everyday Injustices: Barriers to Access to Justice for Immigration Detainees in Canada' (2016) 35 Refugee Survey Quarterly 109.

to demonstrate that the correlations applied in algorithmic decision-making are 'legitimate justifications for the automated decisions'.[106]

3.2 Equality rights and freedom from discrimination

Given the problematic track record that automated technologies have on race and gender, it is very plausible that similar issues will occur, or have already occurred, in migration. Proxies for discrimination, such as country of origin, can be used to make problematic inferences leading to discriminatory outcomes. Freedom from discrimination and equality rights are widely protected by the International Covenant on Economic, Social and Cultural Rights (ICESCR),[107] the ICCPR,[108] CERD, CEDAW, CRPD,[109] CRC[110] and the Refugee Convention.[111] The Inter-American Commission on Human Rights' (IACHR) American Declaration of the Rights and Duties of Man[112] and the Universal Declaration of Human Rights (UDHR)[113] also enshrine equality. The UNHCR has also issued guidelines specific to countering discrimination against refugees.[114]

As discussed above, algorithms are vulnerable to the same decision-making concerns that plague human decision-makers: transparency, accountability, discrimination, bias and error.[115] The opaque nature of immigration and refugee decision-making creates an environment ripe for algorithmic discrimination. Decisions in this system – from whether a refugee's life story is 'truthful' to whether a prospective immigrant's marriage is 'genuine' – are highly discretionary, and often hinge on assessment of a person's credibility.[116] To the extent that these technologies will be used to assess 'red flags', 'risk' and 'fraud', they also raise definitional issues, as it remains unclear what the parameters of these markers will be. For example, in the experimental use of AI lie detectors at EU airports, it is unclear what will constitute truthfulness and how differences in cross-cultural communication will be dealt with in order to ensure that problematic inferences are not encoded and reinforced into the system. The complexity of human migration is not easily reducible to an algorithm.

106. Lokke Moerel and Marijn Storm, 'Law and Autonomous Systems Series: Automated Decisions Based on Profiling – Information, Explanation or Justification? That is the Question!' (University of Oxford Faculty of Law Blog, 27 April 2018) <www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-automated-decisions-based-profiling> accessed 23 July 2019.
107. International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR) arts 2, 10.
108. ICCPR arts 4, 24, 26.
109. CRPD arts 3, 5.
110. CRC art 2.
111. Refugee Convention art 3.
112. Inter-American Commission on Human Rights (IACHR), American Declaration of the Rights and Duties of Man, 2 May 1948 (Bogota Declaration) art 2.
113. UDHR arts 7, 10.
114. United Nations High Commissioner for Refugees, 'Guidelines on International Protection No 9: Claims to Refugee Status Based on Sexual Orientation and/or Gender Identity Within the Context of Article 1A(2) of the 1951 Convention and/or its 1967 Protocol Relating to the Status of Refugees' (23 October 2012) UN Doc HCR/GIP/12/09.
115. Tufekci (n 29) 216–217.
116. See eg Vic Satzewich, *Points of Entry: How Canada's Immigration Officers Decide Who Gets In* (UBC Press, Vancouver 2015).

The US Government's proposed Extreme Vetting Initiative is also rife with potential discriminatory inferences, based on travel patterns, countries of origin and various other markers that can flag an individual for further surveillance and even deny them access into the country.[117] The heavy monitoring of social media sites is also contentious, as the information can often be misleading to a non-human analyst.[118] As with predictive policing, the system 'risks hiding biased, politicised, and discriminatory decision-making behind the scientific objectivity of algorithms and machine learning'.[119] Further, 'once applicants or visa holders know they are being monitored, a chilling effect could occur on their freedom of speech, forcing them to censor themselves online to avoid attracting scrutiny',[120] as well as curtail their freedom of movement,[121] association[122] and religion[123] by limiting their time in places of worship.

3.3 Privacy rights

Privacy is not only a consumer or property interest: it is a human right, rooted in foundational democratic principles of dignity and autonomy.[124] It is protected under Article 17 of the ICCPR. The UN has also explicitly recognised the impact of digital technologies on the right to privacy.[125] For example, the High Commissioner for Human Rights issued various statements on the risk surveillance poses to individuals' rights, particularly privacy and freedom of expression and association.[126] The General Assembly also adopted Resolution 68/167, which expressed concerns regarding the potential negative impacts that surveillance may have on international human rights.[127]

117. Glaser (n 67).
118. Jake Laperruque, 'ICE Backs Down on "Extreme Vetting" Automated Social Media Scanning' (Project on Government Oversight, 23 May 2018) <www.pogo.org/blog/2018/05/ice-backs-down-on-extreme-vetting-automated-social-media-scanning.html> accessed 23 July 2019.
119. Brian Root, 'US Immigration Officials Pull Plug on High-Tech "Extreme Vetting"' (Human Rights Watch, 18 May 2018) <www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting> accessed 23 July 2019.
120. Ibid.
121. ICCPR art 12; UDHR art 13; CRC art 10(2).
122. ICCPR art 22. This right is also protected by art 20 of the UDHR and art 22 of the Bogota Declaration.
123. ICCPR art 18; UDHR art 18; Bogota Declaration art 3.
124. See also Lisa Austin, 'We Must Not Treat Data Like a Natural Resource', The Globe and Mail (9 July 2018) <https://www.theglobeandmail.com/opinion/article-we-must-not-treat-data-like-a-natural-resource/> accessed 23 July 2019.
125. 'The Right to Privacy in the Digital Age' (OHCHR) <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> accessed 23 July 2019.
126. 'Opening Remarks by Ms Navi Pillay, United Nations High Commissioner for Human Rights to the Side-Event at the 24th Session of the UN Human Rights Council: How to Safeguard the Right to Privacy in the Digital Age?' (United Nations Office of the High Commissioner for Human Rights, 20 September 2013) <https://newsarchive.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E> accessed 23 July 2019; and 'Opening Remarks by Ms Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The Right to Privacy in the Digital Age' (United Nations Office of the High Commissioner for Human Rights, 24 February 2014) <www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E> accessed 23 July 2019.
127. 'The Right to Privacy in the Digital Age', UNGA Res 68/167 (21 January 2014).

With the adoption of this Resolution, the General Assembly also requested that the High Commissioner for Human Rights prepare a report on the right to privacy in the digital age.[128] In 2015, the Human Rights Council adopted Resolution 28/16, which saw the appointment of a Special Rapporteur on the right to privacy.[129] In 2016, the United Nations Committee on Social, Humanitarian and Cultural Issues adopted a new resolution on the right to privacy in the digital age, which recognises the importance of respecting pre-existing international commitments regarding privacy rights and calls on States to develop appropriate remedies.[130] It emphasises that States must address legitimate concerns regarding their national security in a manner that is consistent with these obligations and that personal data is increasingly susceptible to being sold without the individuals' consent or knowledge. The resolution also highlights the increased vulnerability of women, children and marginalised communities to these privacy right violations, and links the right to privacy with other human rights such as freedom of expression.[131] Increasingly, there is a recognition that 'the same rights that people have offline must also be protected online'[132] and that technologies should be designed and operated in a way that both respects and fulfils human rights, freedoms, human dignity and cultural diversity.[133]

However, the differential impacts of privacy infringements must be considered when analysing the experiences of migrants.[134] If collected information is shared with repressive governments from whom refugees are fleeing, the ramifications can be life-threatening. Or, if automated decision-making systems designed to predict a person's sexual orientation are infiltrated by States targeting the LGBTQ community, discrimination and threats to life and liberty are likely outcomes.[135] It is the power of pattern recognition to extract personal details from available data that is concerning, particularly given the proliferation of surveillance by authoritarian regimes.[136]

Efforts like the GDPR enshrine certain protections, particularly around the use of automated individual decision-making and the protection of personal data.[137] This is hopefully a starting point for broader global standards, but when analysing the

128. 'Opening Remarks by Ms Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar' (n 126).
129. 'The Right to Privacy in the Digital Age', UNHRC Res A/HRC/RES/28/16 (26 March 2015).
130. UNGA Third Committee (71st Session) 'The Right to Privacy in the Digital Age' (16 November 2016) UN Doc A/C.3/71/L.39/Rev.1. See also Deborah Brown, 'New UN Resolution on the Right to Privacy in the Digital Age: Crucial and Timely' (Internet Policy Review, 22 November 2016) <https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436> accessed 23 July 2019.
131. Brown (n 130).
132. 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', UNHRC Res 20/8 (5 July 2012) para 1.
133. Brown (n 130).
134. See also Johns (n 12).
135. Heather Murphy, 'Why Stanford Researchers Tried to Create a "Gaydar" Machine', The New York Times (New York, 9 October 2017) <www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html> accessed 12 August 2019.
136. Privacy International, 'Submission of Evidence to the House of Lords Select Committee on Artificial Intelligence' (Privacy International, 2017) <https://privacyinternational.org/advocacy-briefing/664/submission-evidence-house-lords-select-committee-artificial-intelligence> accessed 13 August 2019, paras 12–16.
137. GDPR art 22. The GDPR also includes mandatory provisions to make machine-made decisions explainable and transparent: see art 5(1).

protection of rights for migrants, the GDPR does not go far enough, as its protections are only available for EU citizens. The United Kingdom (UK) data protection legislation actually goes further and protects the privacy of 'anybody' in its jurisdiction,[138] presumably including migrants.

3.4 Administrative law frameworks and principles of natural justice

Any discussion of pertinent human rights in migration must also include an analysis of administrative legal frameworks and principles of natural justice that are inherent in migration management. For example, in immigration and refugee decision-making, procedural fairness dictates that the person affected by administrative processes has a right to be heard, the right to a fair, impartial and independent decision-maker, the right to reasons – also known as the right to an explanation – and the right to appeal an unfavourable decision. However, it is unclear how administrative law will handle the augmentation or even replacement of human decision-makers by algorithms. While these technologies are often presented as tools to be used by human decision-makers, the line between machine-made and human-made decision-making is not often clear. Given the persistence of automation bias, or the predisposition towards considering automated decisions as more accurate and fair, it remains unclear what rubric human decision-makers will use to determine how much weight to place on the algorithmic predictions, as opposed to any other information available to them, including their own judgment and intuition. Furthermore, when a person wishes to challenge an algorithmic decision, what will the appropriate standard of review look like? Inappropriate deference given to algorithmic decision-making has been widely documented.[139] It is unclear how tribunals and courts will assign reasonableness to automated decision-making, what standards of review will be used, and what mechanisms of redress will look like.

The unique context of migration should be the central consideration when analysing which human rights should be taken into consideration when exploring new technologies, given the very real risks to life, liberty and security, as well as heightened privacy considerations. Analysing the ramifications of new technologies on internationally protected human rights is a principled way to codify harms and think through mechanisms of redress.[140] Yet why are States reluctant to engage with this, seeing technology through the lens of IHRL? Section 4 of this paper argues that States are able to justify technological experiments in migration management precisely because migrants are not able to exercise the same rights as citizens, and because they are seen as a useful tool through which to exercise powers of sovereignty in an increasingly destabilised world.

138. Data Protection Act 2018.
139. See Michael Koliska and Nicholas Diakopoulos, 'Disclose, Decode and Demystify: An Empirical Guide to Algorithmic Transparency' in Scott A Eldridge II and Bob Franklin (eds), *The Routledge Handbook of Developments in Digital Journalism Studies* (Routledge, New York 2018) 559, 559–560; see also Michele Wilson, 'Algorithms (and the) Everyday' (2017) 20 Information, Communication and Society 137, 141, 143–144, 147.
140. See also McGregor et al (n 6).

4 MIGRATION AS TECHNOLOGICAL EXPERIMENTATION

States are able to justify increasing technological experiments in migration because migrants have been historically rendered as a population which is intelligible, trackable and manageable.[141] The very rhetoric of migration 'management' implies that refugees and migrants must be presided over and controlled, as they are construed to be a threat to national sovereignty, particularly in times when more and more States are turning inward and reifying their sovereign power. Butler's theory of State performativity is useful here. When sovereignty is under threat, the State justifies its control over populations through repeated spectacles and messaging around necessary national security and border control at the exclusion of the Other.[142] This performance is particularly cogent when the law is suspended, such as in Australia's extraterritorial – and extra-legal – immigration detention policies,[143] or, as in the case of technological development, where there simply is no law (or, as examined, very little law). Yet without law and regulation, the population affected by technological development is not able to recognise, access and enjoy rights that accrue to other groups and stakeholders. Indeed, the creation of legal black holes in migration management technologies very deliberately allows for the creation of opaque zones of technological experimentation that would not be allowed to occur in other spaces.[144] While we are able to imagine rallying around extreme issues such as the banning of killer robots in armed conflict, the grey spaces of migration management technology remain uncontested.

We are able to tolerate the contradictions inherent in the differentiation of rights precisely because the normalisation of increased surveillance, data collection, and augmentation of decision-making become ingrained in everyday actions and experiences, or the ethics of everyday actions.[145] The concept of Agamben's 'inclusive exclusion',[146] wherein the State is able to divide and separate populations based on the figure of the 'outlaw' who is outside the boundaries of the social and political life of the State further entrenches how we imagine the differentiation of rights to be natural[147] when used to justify interventions and experimentations on the margins for the so-called common good. The concretisation of migrant populations into abject

141. See eg the work of Audrey Macklin, 'Disappearing Refugees' (2005) 36 Columbia Human Rights Law Review 101; Nicholas P De Genova, 'Migrant "Illegality" and Deportability in Everyday Life' (2002) 311 Annual Review of Anthropology 419; Jan Blommaert, 'Language, Asylum, and the National Order' (2009) 50 Current Anthropology 415; Jonathan Inda, *Targeting Immigrants: Government, Technology, and Ethics* (Blackwell, Oxford 2004); Sara Ahmed, 'Affective Economies' (2004) 22 Social Text 117; Arjun Appadurai, *Fear of Small Numbers: An Essay on the Geography of Anger* (Duke University Press, Durham 2006) 49–85. See also Csernatoni (n 12).
142. Butler (n 7).
143. See eg Alison Mountz, 'The Enforcement Archipelago: Detention, Haunting, and Asylum on Islands' (2011) 30 Political Geography 118.
144. See eg the very deliberate messaging centering on border enforcement and security by the Canadian Border Services Agency and the recently announced data-sharing projects between Canada and the United States, entitled 'Keeping Our Families Safe': Government of Canada, 'Strengthening Border Management' (Connect to Canada, 2019) <https://connect2canada.com/2019/07/strengthening-border-management/> accessed 23 July 2019.
145. Arendt (n 8).
146. Agamben (n 9) 12.
147. See also Thomas Blom Hansen and Finn Stepputat, 'Introduction' in Thomas Blom Hansen and Finn Stepputat (eds), *Sovereign Bodies: Citizens, Migrants, and the States in the Postcolonial World* (Princeton UP, Princeton 2005) 17.

Others justifies unregulated technological experimentation under the guise of efficiency and security. The State justifies this experimentation through 'permanent vigilance, activity, and intervention'.[148] This also perpetuates the Global North as the locus of power and technological development, to be deployed in the Global South.

Through technology, the State control over the management of migration has extended beyond traditional sovereignty. The externalisation of borders, opacity of border zones, and transnational surveillance all work to transform migration into a site of criminality that must be surveilled and managed to root out the ever-present spectre of terrorism and irregular migration.[149] Csernatoni argues that the increased use of drones to police Europe's borders has resulted in the decentralisation of the border zone into various vertical and horizontal layers of surveillance, suspending State power from the skies,[150] and extending the border visually and virtually. This notion can be expanded to all technologies that manage migration, whether retinal scans or automated AI lie detectors at the airport, as their primary purpose is to collect data, make decisions and report to the State the necessary information on a potentially unsafe or unknown migrant body, rendering them into security objects and data points to be analysed, stored, collected, and rendered intelligible.

However, not all migration is the same. In cross-border migration management, certain mobilities are made legitimate while others are made abject.[151] An investor immigrant – or indeed, a product like an iPhone – travels across borders with relative ease, while other migrants are incarcerated, surveilled and tracked. The authority of the State and its legitimacy to make these decisions are cleverly manufactured and constantly supported,[152] and migration management spaces are particular locales where sovereignty intersects with notions of threat, security and power. Certain bodies thus become the 'agents of governmentality',[153] upon which experimentation is not only permissible but necessary, as the population must be controlled, managed and used in the performance of sovereignty and security at the border and beyond. Importantly, as Andreas reminds us, '[p]ublic perception is powerfully shaped by the images of the border which politicians, law enforcement agencies, and the media project'.[154] Coupled with the push to innovate in the global technological arms race, the theatre of conspicuous performance of power manifests in the equating of one particular group – migrants – with the necessity to manage, catalogue, experiment and innovate. There is a profound fear of mobility and of the uncontrollable migrant that motivates the proliferation of border technologies. Technology itself replicates existing power hierarchies and supports how migration continues to be differentially experienced.

148. Michel Foucault, *The Birth of Biopolitics: Lectures at the Collège de France, 1978–1979* (Graham Burchell Basing tr, Palgrave Macmillan, Basingstoke 2008) 131; Michel Foucault, 'Of Other Spaces' (1986) 16 Diacritics 22.
149. See also SITA, 'Smart Technology for Border Security' (SITA, 2019) <www.sita.aero/resources/type/infographics/smart-technology-for-border-security> accessed 23 July 2019.
150. Csernatoni (n 12). See generally also Mbembe (n 1).
151. Louise Amoore, 'Biometric Borders: Governing Mobilities in the War on Terror' (2006) 25 Political Geography 336; Matthew Sparke, 'A Neoliberal Nexus: Economy, Security, and the Biopolitics of Citizenship on the Border' (2006) 25 Political Geography 151.
152. Butler (n 7).
153. Ibid 71.
154. Peter Andreas, *Border Games: Policing the U.S.–Mexico Divide* (2nd edn, Cornell University Press, Ithaca NY 2009) 9.

Technology is far from neutral. It reflects norms, values and power in society. The development of technology occurs in specific spaces that are not open to everyone and its benefits do not accrue equally. Decision-making around implementation occurs without consultation or even sometimes without the consent of the affected groups.[155] Data ownership benefits the status quo – indeed, data is seen as quickly becoming the new currency.[156] There also appears to be deliberate confusion around the spread of technology, again to obfuscate debate and regulation, and a slowing of innovation leading to profit.[157] In what Zuboff has termed 'surveillance capitalism', reality is commodified and transformed into behavioural data for analysis and sales.[158] While Zuboff argues that all of our data is being used for profit, particular sites of experimentation centre on groups that have fewer protections available, such as people in the humanitarian and migration management space. States are seeking to leave migrants and non-citizens beyond the duties and responsibilities enshrined in law through an overreliance on the private sector to ensure technological experimentation occurs outside of sovereign responsibility.[159] The growing role of the private sector in the governance of new technologies highlights the movement away from State responsibility to create governance structures in accordance with domestic and international principles under the guise of proprietary technology, private interests and discretion.

However, the private sector already has an independent responsibility to ensure that technologies do not violate international human rights, such as the UN Guiding Principles on Businesses and Human Rights.[160] In the development of products and services, private entities also have clear legal obligations to comply with domestic law, including privacy and human rights legislation. Technologists, developers and engineers responsible for building this technology also have special ethical obligations[161] to ensure that their work does not facilitate human rights violations. However, the tension between private and public regulation highlights an overall lack of institutional capacity to effectively regulate technology and a disjuncture between those who develop migration-related technology in the private sector, and those in the public sector who deploy it on specific populations. The so-called AI divide, or the gap between those who are able to design AI and those who are not is broadening and highlights problematic power dynamics in participation and agency

155. See Molnar and Gill (n 5).
156. See eg various private-sector statements such as Natarajan Chandrasekaran, 'Is Data the New Currency?' (World Economic Forum, 14 August 2015) <www.weforum.org/agenda/2015/08/is-data-the-new-currency/> accessed 23 July 2019.
157. Benvenisti (n 93).
158. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, London 2018).
159. See eg the Canadian Government's procurement for a so-called 'Artificial Intelligence Solution' for various immigration processes, directly calling on the private sector to be the driver of migration management technologies: Public Works and Government Services Canada, 'Artificial Intelligence Solution (B8607-180311/A) Tender Notice' (13 April 2018, amended 23 May 2018) <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462> accessed 25 July 2019. See also Molnar and Gill (n 5).
160. United Nations Office of the High Commissioner for Human Rights, 'Guiding Principles on Businesses and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) 13–16 <www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> accessed 23 July 2019.
161. Kirsten Martin, 'Ethical Implications and Accountability of Algorithms' (2018) Journal of Business Ethics 1.

when it comes to the roll-out of new technologies. Most often, the viewpoints of those most affected are excluded from the discussion, particularly around areas of no-go zones or ethically fraught usages. There is a lack of contextual analysis when thinking through the impact of new technologies, resulting in great ethical, social and political harm.

Politics also cannot be discounted, as migration management is inherently a political exercise. Migration data is already being politicised to justify greater interventions in support of threatened national sovereignty.[162] The State's ultimate power to decide who is allowed to enter and under what conditions[163] is bolstered by ongoing beliefs in technological impartiality. However, there is an inherent tension between the claimed prerogative of Nation States over sovereignty and the malleable nature of technology. In its fluidity, technology is inherently oppositional to borders, and by extension sovereignty. Indeed, oftentimes it impinges on the very definition of 'humanness' in the digital era.[164] Ultimately, the primary purpose of the technologies used in migration management is to track, identify and control those crossing borders. The unequal distribution of benefits that accrue in technological development work to create monopolies of knowledge and consolidate power and authority vested in the Sovereign State. These monopolies are allowed to exist because there is no unified global regulatory regime governing the use of new technologies, creating laboratories for high-risk experiments with profound impacts on people's lives.

5 CONCLUSIONS: A PATH TOWARDS GLOBAL GOVERNANCE OF TECHNOLOGICAL EXPERIMENTS

The current global governance regime of migration management technologies is inadequate. While there are some encouraging developments in the regulation around AI and automated decision-making, there is no global way to regulate the development and deployment of new technologies in the many facets that impinge on human movement across sovereign borders. While States increasingly rely on new developments to strengthen borders, automate decision-making and collect vast amounts of data on migrants, the governance gap highlights how techno-solutionism has been allowed to proliferate without systematic analysis of the impacts and ramifications of new technologies, particularly on populations with less access to redress mechanisms and ability to exercise procedural and substantive protections. This paper has argued that this lack of regulation is deliberate, as States single out the migrant population as a viable testing ground for new technologies.

New technologies are often presented as viable solutions to complex problems. However, technological solutions do not address the underlying root causes of mass migration, border security issues, or failed policies to come to any global consensus on migration.[165] Instead, technologies replicate the problems and biases that are

162. Stephan Scheel and Funda Ustek-Spilda, 'Why Big Data Cannot Fix Migration Statistics' (Refugees Deeply, 5 June 2018) <https://www.newsdeeply.com/refugees/community/2018/06/05/why-big-data-cannot-fix-migration-statistics> accessed 23 July 2019.
163. Ibid.
164. Elia Zureik and Karen Hindle, 'Governance, Security and Technology: The Case of Biometrics' (2004) 73 Studies in Political Economy 113.
165. Csernatoni (n 12) 176, 194.

inherent in society and impinge on the very practice of democracy.[166] The ownership of information and data and the power behind development and deployment of technological experiments all operates in an opaque, discretionary and unregulated space where rights infringements already proliferate.

It is the normative universality of human rights that presents a viable starting point for the global governance of migration management technologies.[167] However, the recognition and codification of human rights concerns have to be contextual to the unique issues around migration while being situated in the broader sphere of technological regulation generally. The patchy establishment of oversight bodies and mechanisms to measure the impacts of AI and new technologies is a starting point, with countries like Canada and the UK at the vanguard. Any regional mechanisms and treaty bodies must consider the unique context of migration because technology travels, and a State's decision to develop and deploy particular technologies will set an example for other countries to follow. The role of international organisations such as the UNHCR in the proliferation of new migration management technologies must also be interrogated. There is also a unique opportunity to set clear standards and norms for States with weaker rule of law and problematic human rights records. Weak ethical standards and a lack of accounting for human rights impacts can cause a slippery slope and a race to the bottom, resulting in grave ramifications. The global community must also pay special attention to the inherent transnational dimension of technology when exporting to countries that may be more willing to experiment on non-citizens and other more vulnerable groups.[168]

A more rigorous global accountability framework is now paramount, one which recognises the necessity of regulating migration management technologies across multiple jurisdictions and bridging the public–private accountability divide. Self-regulation by the private sector is not enough to ensure that rights-infringing technological experiments are curtailed. McGregor et al[169] and others have argued that we need to go as far as drawing bright lines that prohibit the use of new technologies such as automated decision-making in certain instances that could be used to circumvent international human rights law, such as using AI to detain migrants[170] or replacing human decision-makers in refugee determinations.[171] Committing to safeguards around the use of these technologies will also ensure that principles of natural justice and administrative law are respected, including creating appropriate remedies and methods of redress.

Yet there is also a hopeful promise to the proliferation of new technologies. Policy-makers, academia and the public are being forced to reckon with fundamental normative ideas around what constitutes intelligence, how to manage and regulate new systems of cognition, and who should be at the table when designing and deploying new tools that can be used to either dismantle or reinforce the status quo. Culture,

166. Hao (n 14). See also the work of Yuval Harari, 'Why Technology Favors Tyranny', The Atlantic (Washington DC, October 2018) <https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/> accessed 12 August 2019.
167. McGregor et al (n 6).
168. For an example of this issue in another context, see the way in which Canada allows the export of internet filtering technology: Jakub Dalek, Lex Gill, Bill Marczak et al, 'Planet Netsweeper: Executive Summary' (The Citizen Lab, 25 April 2018) <https://citizenlab.ca/2018/04/planet-netsweeper/> accessed 23 July 2019.
169. McGregor et al (n 6) 335.
170. See Oberhaus (n 66).
171. Molnar and Gill (n 5).

institutions and technology all iteratively shape one another. Ultimately, technology is a social construct,[172] a mirror to reflect the positives and negatives inherent in our societies, forcing us to rethink ideas of privilege and power. It remains to be seen whether the current global push towards fervent technological innovation will result in robust global governance, centred on the experiences of those on the margins.

172. See also Ursula Franklin, *The Real World of Technology* (House of Anansi Press, Toronto 1990).