Amnesty International is a movement of 10 million people that mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law, and are held to account. We are independent of any government, political ideology, economic interest, or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.
# TABLE OF CONTENTS

**INDEX**

Key Terminology A-Z  
Introduction  

1. HOW INEQUALITY DRIVES MIGRATION AND FORCED DISPLACEMENT  
   Technology, Inequality, Forced Displacement, and Migration  
   Technology, Inequality, and Migration: Human Rights Implications  

2. HOW TECHNOLOGY ENABLES THE CRIMINALIZATION OF MOVEMENT  
   Externalization and Internalization of Borders  

3. BEFORE THE BORDER  
   Predictive Forecasting Tools  
   Border Deterrence Technology  

4. AT THE BORDER  
   Immigration Surveillance  
   Biometrics  
   Algorithmic Decision Making  

5. AFTER THE BORDER  
   Technology-Enabled Detention and Alternatives to Detention  
   Economic, Social and Cultural Rights  
   Social Security and Welfare  
   Work, Migration, and Technology  

**CONCLUSION AND RECOMMENDATIONS**
ALGORITHMS

An algorithm is a list of mathematic rules which solve a problem. The rules must be in the right order –think of a recipe. Algorithms are the building blocks of Artificial Intelligence (AI) and Machine Learning (ML). They enable AI and ML technologies to train on data that already exists about a problem so that they are able to solve problems when working with new data.

ALGORITHMIC MANAGEMENT

The use of computer programmed procedures for the coordination of labor input in an enterprise or organization, which can take the form of a diverse set of technological tools and techniques to remotely manage workforces.¹ These methods rely on data collection and surveillance of workers to enable automated or semi-automated decision-making.² However, when algorithmic management is used in situations in which companies are able to avoid legally classifying workers as employees, and therefore avoid the legal protections afforded to them, workers are at risk of more precarious and dangerous working conditions, and have little recourse to restitution or the ability to opt out, particularly in scarce and competitive labor markets.³

ARTIFICIAL INTELLIGENCE (AI)

There is no widespread consensus on the definition of AI because the term does not refer to a singular technology and rather encapsulates myriad technological applications and methods. Most formal definitions will refer to a range of data-driven processes which enable computers to execute very specific or more general tasks, such as decision-making or solving problems, in place of or to assist humans. Amnesty International intentionally takes a broad definition of AI in order to adequately and holistically interrogate the human rights impacts of the various components, practices and processes that underlie AI technologies. Broadly speaking, AI is any technique or system that allows computers to mimic human behavior.

BIOMETRIC DATA

Data that is based on physical/biological features of individuals for example fingerprints, iris prints, facial imagery, and other highly personal characteristics. This data is often collected and stored for the purposes of identifying an individual or authenticating their identity.⁴

BORDER-INDUSTRIAL COMPLEX

This concept (also sometimes referred to as the border surveillance industry or immigration-industrial complex), refers to the closely intertwined relationships between governments and the private sector, including tech companies in asylum and migration management systems.⁵

EXTERNALIZATION

A range of migration management policies that focus on shifting the responsibility of providing international protection to refugees and asylum seekers to other countries, or on enlisting source or transit countries in tightening control over their borders. Externalization policies share the objective of preventing or punishing irregular border crossings by refugees, asylum seekers and migrants, often mobilizing and leveraging international financial aid.

GPS TECHNOLOGIES

Global Positioning System: a navigational system used to identify the longitudinal and latitudinal position of people, objects and places across the planet.

INTERNALIZATION

A series of increasingly common migration practices, carried out in coordination with externalization of borders, in which border policing mechanisms and practices are brought inward from a nation’s physical border. This may take the form of increased interior policing of immigrants, including methods of surveillance with the goal of detecting, detaining, and deporting migrants.6

INTEROPERABILITY

The ability of one system or database to seamlessly exchange or find information within another system or database.

INTERSECTIONAL DISCRIMINATION

When discrimination on different grounds operates together to produce compound or distinct disadvantages. For example, if a Black or Muslim asylum seeker is more likely to experience migration-related detention, the discrimination and violation of their human rights is due to a combination of their perceived or real race, national origin, immigration or citizenship status.

NON-REFOULEMENT

The legal obligation for states not to return or transfer anyone to a place or jurisdiction where they would be at real risk of persecution or other serious human rights violations or abuses.

“SMART” BORDERS

The use of technological systems in reinforcing borders, for example biometric identification and registration, the automated detection of human movement and object recognition, automated entry/exit systems at the border, and/or apps used to govern asylum applications, to name a few.

TECHNOCOLONIALISM

How some researchers have referred to the data-hungry nature of many of today’s information and communications technologies, particularly when they are leveraged in humanitarian contexts and/or with the personal data of highly marginalized populations. Technologies that make use of data of highly marginalized populations often play a role in entrenching inequalities between the Global Majority and Global Minority, and ultimately, reflect the historical inequalities of extraction and colonialism.²

A midst human rights violations around the world, many of which are fueled by growing global inequality, technology has continued to permeate into more areas of daily life. Racial, economic, and social inequities around the world have shaped and driven the movement of persons across municipal and international borders, many of whom are fleeing the effects of conflict, intractable poverty, political oppression, or the climate crisis. 2023 recorded the highest ever number of forcibly displaced people—an estimated 110 million. Many governments and political movements around the world have weaponized xenophobic rhetoric about refugees and migrants, often blaming domestic instability on migrants and refugees or otherwise mobilizing support for externalization and privatization of borders.

Human rights organizations around the world have documented grave and escalating rights violations against refugees, asylum seekers, internally displaced people, and migrants. At the same time, the role of new forms of digital technology in and around international borders has continued to grow. Many states and international organizations have increasingly integrated new technologies into the systems that process and manage movement of persons. Some forms of digitization at and around borders may be considered a form of pushback against refugee and migrant rights. Such technology-enabled security practices also justify and undergird the expansion of discriminatory tools in policing, social services, and beyond, which impact not just migrants and refugees, but a range of racialized and marginalized groups.

This briefing will provide an overview of how migration fits into an intersectional framework of technology, inequality, and human rights. Building upon previous work by Amnesty International and others, this briefing will outline how uses of new technology are central to a trend of violations of human rights at borders around the world, and provide a broad outline of forms of technology used by states and non-state actors in migration management and asylum systems. The second of a series of four briefings by Amnesty International USA on technology and inequality, this report will demonstrate how concerns around digital rights and the rights of asylum seekers, refugees and migrants are increasingly interrelated, and must be considered within a broader trend of criminalization of marginalized peoples’ lives that is often enabled and facilitated by new forms of technology.
The United Nations High Commissioner for Refugees (UNHCR) recorded a 21 percent increase in 2022 alone in the number of displaced persons, which accounts for the single largest yearly increase recorded since the UNHCR began keeping such records.21 Because of escalating threats from insecurity and conflict, the scale of displacement around the world shows no sign of slowing. Meanwhile, many states around the world have long experimented with increasingly punitive border management and asylum policies that effectively criminalize those seeking asylum or moving across borders.22 In addition, many political actors and parties around the world have continued to weaponize xenophobic and racist rhetoric about immigrants and asylum seekers.23 Asylum seekers themselves often do not receive adequate protection while they are in the process of seeking a status determination, including in the form of dangerous or unhealthy living conditions at borders, or within camp settings.24 Forcibly displaced people are often forced to seek asylum in part because of underlying structures of inequality they experience in their home context that lead to discrimination and persecution, including ethnic and religious minorities,25 and LGBTQI+ people.26 Many people who experience forced displacement are from countries or populations who have experienced the impacts of historical colonialism and ongoing economic extraction.27 Forced displacement itself is often a modern manifestation of the aftermath of violent and extractive systems of colonialism, both past and present.28 States often experiment with new technologies in the asylum or immigration process on those who, for a variety of underlying reasons, have the least ability to protect their rights, or seek redress when harmed.29 The use of new technologies is increasing in the migration and asylum fields across the world, particularly in the arenas of policing and security, personal identification, and communication and movement of information.

Many of these systems pose threats to the rights of people seeking to move across borders, in ways that exacerbate underlying racial, economic, and


social inequalities. Further, many of the digital tools being used in the processing of movement of persons are developed, sold, and deployed by private companies, whose very business model is often rooted in and structured by the extraction and accumulation of data for profit. As the right to seek asylum is under increasing threat by states and governments who are using the human, the adoption of undertested and experimental technologies at the border must be examined carefully alongside other technology-enabled human rights concerns.

Alongside the digitally-enabled rights violations of asylum seekers, refugees and migrants, there are also increasing threats to the rights and concerns of migrants moving across borders for work opportunities. The rights of migrant workers are protected under additional legal instruments, and are increasingly an issue of concern, particularly alongside growing violations of workers’ rights more broadly. Amnesty International has increasingly sounded the alarm about the exploitation and rights violations of migrant workers, who are often subject to serious rights violations, including vulnerability to trafficking in persons and wage theft. Finally, migrant workers and other people with insecure citizenship status, including undocumented immigrants, are often subject to the same forms of digitally-enabled surveillance, monitoring, and exploitation, particularly in the context of the workplace, and are similarly vulnerable to these tools because of their inability to opt out or seek redress when such tools are used in harmful ways.

Across all stages of movement, including in countries of origin, transit, and destination, all migrants have the right to equality and non-discrimination, privacy, and access to social protection. Technologies that contribute to discouraging people on the move from exercising these rights can be considered part of a broader system of what some researchers have termed “technocolonialism,” entrenching inequalities of already marginalized groups. The use of such technologies often helps to facilitate both the externalization and internalization of borders, in which various forms of technology provide the pretext by which states and regions justify the undermining or weakening of human rights by extending systems of criminalization and surveillance into more areas of daily life for more types of people. Borders increasingly operate both internally and externally, and an approach which analyzes the growing influence of technology on migration helps shed light on how affected populations are subject to rights violations across different stages of their movement.

THE DIGITAL BORDER: MIGRATION, TECHNOLOGY, AND INEQUALITY

---

31 Amnesty International, Digitally Divided (previously cited) p. 6.
33 Refugee Studies Centre, Automating Immigration and Asylum, p. 5.
35 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
36 See, for example, Amnesty International, They Think That We’re Machines: Forced Labour and Other Abuse of Migrant Workers in Qatar’s Private Security Sector (Index: MDE 22/388/2022), 7 April 2022, https://www.amnesty.org/en/documents/mde22/388/2022/en/
38 International Covenant on Civil and Political Rights (ICCPR), Article 24, Article 26.
39 The right to privacy is protected under a number of international human rights instruments, including Article 17 of the ICCPR which provides that no one should be subject to “arbitrary or unlawful interference” with their privacy, family, home or correspondence, and this should be protected by law, Universal Declaration of Human Rights, Article 12; International Covenant on Civil and Political Rights, Article 17. The UN Human Rights Committee has long recognized that such protection includes regulating “the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies. See UN Human Rights Committee (HRC), General Comment 15: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), UN Doc. HRI/CES/R/Rev.3 (Vol. I), 8 April 1998, para. 10. See also Amnesty International, Automated Apartheid: How Facial Recognition Fragments, Segregates, and Controls Palestinians in the OPT (Index: MDE 15/6701/2023), 2 May 2023, https://www.amnesty.org/en/documents/mde1567012023/32671
30 The right to social security is recognized and protected by international human rights law. Article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) and Article 22 of the Universal Declaration of Human Rights (UDHR) recognize the right of everyone to social security. According to ICESCR, states are responsible for ensuring that social support is adequate in amount and duration so that everyone can realize their rights to family protection and assistance, an adequate standard of living and adequate access to healthcare. See: See UN CESCR, General Comment 19, 4 February 2008, para. 22; ICCPR, Article 23, European Social Charter (Revised) 1996, Articles 12, 23, and 30.
32 Refugee Studies Centre, Automating Immigration and Asylum (previously cited), p. 5.
Various forms of technology implemented at borders threaten the right to seek asylum, as well as the rights to non-refoulment, equality, and non-discrimination. Digitized securitization and surveillance measures may have the effect of discouraging people from exercising their right to claim asylum. Information management systems use datasets and algorithms that may exacerbate underlying inequalities in the lives of people on the move by threatening the rights to non-discrimination and equality. These technologies frequently replicate previously existing racial, economic, and social biases, including by replicating historical biases based on an individual’s real or perceived ethnicity, race, national origin, descent, religion, and other characteristics. Such security technologies are often implemented on the premise that individuals of certain nationalities or possessing certain characteristics pose a threat with respect to national security concerns. These assumptions are based on and justified by racist and xenophobic ideologies, discourses and structures.

People on the move also have the right to liberty and freedom from arbitrary detention, which may be under threat when technologies are used to make decisions about migrants’ ability to move freely. Under international law, the enjoyment of personal liberty and freedom of movement should be any individual’s default condition. Migrants, refugees and asylum seekers, like anyone else, must benefit from a legal presumption of liberty and, as a consequence, any restrictions to their liberty must be clearly prescribed by law, strictly justified by a legitimate purpose, necessary, proportionate and non-discriminatory.

Finally, people crossing borders for reasons other than seeking asylum, also have the right to privacy, which is often threatened by forms of technology including increased biometric data collection, surveillance technology, and the collection and sharing of personal data at and around borders, as well as further surveillance by means of social media. While interference with an individual’s right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful, people on the move—with precarious immigration status; refugees, asylum seekers, and undocumented communities alike—are often obligated to compromise on their human rights, in exchange for possible passage. International human rights law and standards set out a three-part test to determine whether an interference with the right to privacy is legitimate or amounts to a violation: firstly, any interference must be prescribed by and in accordance with the law (legality); secondly, it must be pursuant to a legitimate aim; thirdly, it must be strictly necessary to meet a legitimate aim, such as protecting national security or public order (necessity) and be conducted in a manner that is proportionate to that aim and non-discriminatory, which means balancing the nature and the extent of the interference against the reason for interfering (proportionality).

43 Convention Relating to the Status of Refugees.
44 Universal Declaration of Human Rights (UDHR), Article 14.
45 Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Article 3. “No State Party shall expel, return (“refouler”) or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture.”
46 Non-discrimination and equality are fundamental components of international human rights law and essential to the exercise and enjoyment of economic, social and cultural rights.” – UN CESCR, General Comment No. 20: Non-discrimination in economic, social and cultural rights, UN Doc. E/C.12/GC/20 (2009), Para. 2. “Non-discrimination, together with equality before the law and equal protection of the law without any discrimination, constitute a basic and general principle relating to the protection of human rights.” – UN Human Rights Committee, General comment No. 18, UN Doc. HRI/GEN/1/Rev.9 Vol. I (1989), Para. 1
47 Refugee Law Lab, Technological Testing Grounds (p. 19).
46 Digitized securitization
47 Information management systems
48 Such security technologies are often implemented on the premise that individuals of certain nationalities or possessing certain characteristics pose a threat with respect to national security concerns.
49 These assumptions are based on and justified by racist and xenophobic ideologies, discourses and structures.
50 People on the move also have the right to liberty and freedom from arbitrary detention, which may be under threat when technologies are used to make decisions about migrants’ ability to move freely. Under international law, the enjoyment of personal liberty and freedom of movement should be any individual’s default condition. Migrants, refugees and asylum seekers, like anyone else, must benefit from a legal presumption of liberty and, as a consequence, any restrictions to their liberty must be clearly prescribed by law, strictly justified by a legitimate purpose, necessary, proportionate and non-discriminatory.
51 Finally, people crossing borders for reasons other than seeking asylum, also have the right to privacy, which is often threatened by forms of technology including increased biometric data collection, surveillance technology, and the collection and sharing of personal data at and around borders, as well as further surveillance by means of social media. While interference with an individual’s right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful, people on the move—with precarious immigration status; refugees, asylum seekers, and undocumented communities alike—are often obligated to compromise on their human rights, in exchange for possible passage. International human rights law and standards set out a three-part test to determine whether an interference with the right to privacy is legitimate or amounts to a violation: firstly, any interference must be prescribed by and in accordance with the law (legality); secondly, it must be pursuant to a legitimate aim; thirdly, it must be strictly necessary to meet a legitimate aim, such as protecting national security or public order (necessity) and be conducted in a manner that is proportionate to that aim and non-discriminatory, which means balancing the nature and the extent of the interference against the reason for interfering (proportionality).
52 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para 7.
54 ICCPR, Article 9.
56 See, for example: Universal Declaration of Human Rights (UDHR), Article 12; ICCPR, Article 17; UN Human Rights Committee (HRC), General Comment 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), 8 April 1988, para. 10; UN High Commissioner for Human Rights, Report. The Right to Privacy in the Digital Age: 3 August 2018, UN Doc. A/HRC/39/29, para. 5.
The rights of people moving across borders are protected under various legal instruments of international law. Refugees, asylum-seekers, and migrants are also entitled to other rights protections, which are applicable at every stage of their journey and regardless of national origin or background.

**RIGHT TO SEEK AND ENJOY ASYLUM**

Everyone has the right to seek and enjoy asylum from persecution in other countries. Access to territory is a necessary requirement for realizing the right to seek asylum. Once asylum-seekers have been able to access territory, they must also be able to present their claims by accessing refugee status determination procedures that contain certain basic safeguards.

**THE UNHCR HAS STATED THAT, “WHILE IT IS LEFT TO EACH STATE TO ESTABLISH THE PROCEDURE MOST APPROPRIATE TO THAT STATE’S CONSTITUTIONAL AND ADMINISTRATIVE STRUCTURE, ASYLUM PROCEDURES MUST BE CONDUCTED IN FULL RESPECT OF DUE PROCESS STANDARDS.”**

This means that technologies deployed at or around borders must not directly or indirectly impede access to the asylum process, impede due process, or have the effect of criminalizing movement across borders by excessively monitoring, tracking and intercepting asylum seekers on their journey.
PRINCIPLE OF NON-REFOULEMENT

All states are entitled to regulate access and residence of foreigners on their territory and return people who are irregularly present on their territory to their country of origin. However, states around the world are bound by the principle of non-refoulement, which is the cornerstone of refugee law and enshrined in customary international law, meaning it is binding on all states irrespective of which treaties they have ratified. Under this principle, “no State Party shall expel, return (“refouler”) or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture” or other serious human rights violations.

THE PRINCIPLE OF NON-REFOULEMENT MUST BE OBSERVED IN RESPECT OF ANYONE IN REMOVAL, EXPULSION OR EXTRADITION PROCEDURES, IRRESPECTIVE OF WHETHER A PERSON HAS FORMALLY REQUESTED OR OBTAINED INTERNATIONAL PROTECTION.

Therefore, any technology that facilitates or creates the conditions for ‘pushbacks,’ or forced return of asylum seekers or refugees without consideration of individual circumstances or the potential for an appeal may be considered a violation of the principle of non-refoulement, particularly where there are substantial grounds to believe there is a risk of serious human rights violations or abuses.

---

63 Convention and Protocol Relating to the Status of Refugees; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Article 3
64 Convention Relating to the Status of Refugees; Protocol Relating to the Status of Refugees.
65 Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Article 3.
67 Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Article 3.
The principles of equality and non-discrimination are among the key concepts of international human rights protection, protected in various human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and others. Under these instruments, all persons are guaranteed equal protection of the law, and discrimination “on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status” is prohibited, as well as discrimination against persons with disabilities. Some people, including migrants, refugees, and asylum seekers, experience additional or unique forms of discrimination because of multiple characteristics that are part of their identity, or perceived in that context, such as race and social origin. This is referred to as intersectional discrimination.

Such discrimination and other forms of xenophobia disproportionately impact people on the move, including refugees, asylum seekers, and migrants, and is of particular concern amidst rising xenophobic rhetoric by governments around the world. International law obliges states to take measures to eliminate all forms of discrimination.

---

68 International Covenant on Civil and Political Rights (ICCPR), Article 4, Article 26.
70 Convention on the Rights of Persons with Disabilities (CRPD)
74 International Convention on the Elimination of All Forms of Racial Discrimination, Article 2(1); International Covenant on Civil and Political Rights, Article 26.
MIGRANT WORKERS’ RIGHTS

Migrants who cross international borders for the purpose of work opportunities, as with all persons, are guaranteed the rights to life, liberty, privacy, and freedom from compulsory labor, as well as the right to freedom from arbitrary detention, regardless of where or under what circumstances a person crosses a border. The right to safe and fairly compensated work is protected by a number of different instruments under international law. Under Articles 6 and 7 of the International Covenant on Economic, Social and Cultural Rights, states are obligated to protect individuals’ right to “just and favorable conditions of work,” including “equal wages and equal remuneration,” as well as “safe and healthy working conditions” and “rest, leisure, and reasonable limitation of working hours.” Furthermore, the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families provides further specific protections for migrant workers, including, notably, protection from arbitrary or unlawful interference with one’s privacy, family, home or correspondence. Amnesty International has recommended that the UN Committee on the Protection of the Rights of All Migrant Workers and Members of their Families (CMW) requests States Parties to the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families to provide detailed information on, inter-alia, several aspects of their labor migration policies, as well as measures taken to ensure that all migrant workers are able to gain a living by work which they freely choose or accept, as well as measures to ensure that workers are able to report instances of labor violations and obtain an effective remedy for human rights violations.

---

75 ICCPR Article 6
76 ICCPR, Article 8.
77 International human rights law restricts the use of both custodial and non-custodial measures i.e. detention and measures short of detention, also known as “alternatives to detention” for migration control. As with the use of detention, these “alternatives” must still comply with the principles of legality, necessity, proportionality, and non-discrimination.
78 International Covenant on Economic, Social and Cultural Rights, Articles 6-7
79 ICCPR, Article 19; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14
STATE OBLIGATIONS AND PRIVATE SECTOR RESPONSIBILITIES

MANY STATES AND REGIONS NOW RELY IN PART ON PRIVATE CORPORATIONS TO MANAGE THE MOVEMENT AND RECEPTION OF PEOPLE CROSSING INTERNATIONAL BORDERS.81

The term “border industrial complex” has been used to describe the nexus between border policing, militarization, and financial interest,82 and often manifests as the multiplying83 partnerships between state and international bodies and private companies.84

According to the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), States’ international human rights law obligations require that they respect, protect and fulfill the human rights of individuals within their territory and/or jurisdiction, including non-citizens.85 This includes the duty to protect against human rights abuse by third parties, including business enterprises. Because the State duty to protect is a standard of conduct, States themselves are not per se responsible for human rights abuse by private actors.86 However, States may breach their international human rights law obligations in the case that “such violations can be attributed to them, or where they fail to take appropriate steps to prevent, investigate, punish and redress private actors’ abuse.” Although it is the case that States “generally have discretion in deciding upon these steps, they should consider the full range of permissible preventative and remedial measures, including policies, legislation, regulations and adjudication.” Furthermore, States also have the duty to protect and promote human rights, including by enacting concrete measures to ensure “equality before the law, fairness in its application, and by providing for adequate accountability, legal certainty, and procedural and legal transparency, as well as the duty to ensure remedy.”87 In addition, States should “clearly set the expectation that all businesses enterprises within their territory or jurisdiction respect human rights throughout their operations.”88 State guidance to businesses may include advice on human rights due diligence, including how to recognize the specific challenges that may be faced by Indigenous peoples, women, national or ethnic minorities, religious and linguistic minorities, children, persons with disabilities, and migrant workers and their families.89

81 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para. 18
86 UN Guiding Principles (previously cited), Principle 1 and Commentary
87 UN Guiding Principles (previously cited), Principle 25
88 UN Guiding Principles (previously cited), Principle 2
89 UN Guiding Principles (previously cited), Commentary to Principle 3
STATE OBLIGATIONS AND PRIVATE SECTOR RESPONSIBILITIES

CORPORATE RESPONSIBILITIES

Companies have a responsibility to respect all human rights wherever they operate in the world and throughout their operations. This is a widely recognized standard of expected conduct as set out in international business and human rights standards including the UN Guiding Principles on Business and Human Rights (UN Guiding Principles) and the OECD Guidelines for Multinational Enterprises (OECD Guidelines).  

This corporate responsibility to respect human rights is independent of a state’s own human rights obligations and exists over and above compliance with national laws and regulations protecting human rights.  

This principle is particularly relevant for businesses operating in countries where laws not only fall short of international human rights law but actually contradict it in key respects. In these situations, the UN Guiding Principles indicate that business enterprises “are expected to respect the principles of internationally recognized human rights to the greatest extent possible in the circumstances, and to be able to demonstrate their efforts in this regard.”  

The responsibility to respect human rights requires companies to avoid causing or contributing to human rights abuses through their own business activities, and address impacts in which they are involved, including by remediating any actual abuses. It also requires companies to seek to prevent or mitigate adverse human rights impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.  

(Continued on Next Page)
The UN Guiding Principles establish that to meet their corporate responsibility to respect, companies should have in place an ongoing and proactive human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights. When conducting human rights due diligence, a company may identify that it may cause or contribute to – or already be causing or contributing to – a serious human rights abuse. In these cases, companies must cease or prevent the adverse human rights impacts.94

WHEN BUSINESSES HAVE DETERMINED THAT THEIR PRACTICES HAVE CAUSED OR CONTRIBUTED OR ARE CAUSING OR CONTRIBUTING TO ADVERSE HUMAN RIGHTS IMPACTS, THEY HAVE A RESPONSIBILITY TO PROVIDE FOR OR COOPERATE IN THEIR REMEDIATION PROCESSES.95

Where impacts are outside of the business enterprise’s control but are directly linked to their operations, products or services through their business relationships, the UN Guiding Principles require the company to seek to mitigate the human rights impact by exercising leverage, or seek to improve leverage where leverage is limited, including through collaboration if appropriate.

Under the UN Guiding Principles, “business relationships” include “relationships with business partners, entities in its value chain, and any other non-State or State entity directly linked to its business operations, products or services.”96

An important element of due diligence is transparency and publicly accounting for how a company has identified, prevented, or mitigated potential or actual adverse impacts on human rights. As the UN Guiding Principles make clear, companies “need to know and show that they respect human rights.”97 In this case, “showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders.”98
According to the UN Guiding Principles on Business and Human Rights:

“States should take additional steps to protect against human rights abuses by business enterprises that are owned or controlled by the State, or that receive substantial support and services from State agencies, including, where appropriate, by requiring human rights due diligence.”

States individually are the primary duty-bearers under international human rights law, and collectively they are the trustees of the international human rights regime. Where a business enterprise is controlled by a State or where its acts can be attributed to the State, a failure to respect human rights by the business enterprise may constitute a violation of the State’s own obligations under international law. Furthermore, the closer a business enterprise is to the State, or the more it relies on statutory authority or taxpayer support, the stronger the State’s rationale becomes for ensuring that the enterprise protects human rights. In addition, States have a heightened responsibility to ensure the human rights best practices of enterprises in the context of conflict-affected areas, a definition which may include border zones of various regions around the world, particularly where such zones and regions have a heightened risk of human rights violations and abuses, including both gender-based and sexual violence.

As stated above, an important element of due diligence and fulfilling the responsibility to respect human rights is transparency and publicly accounting for how a company has identified, prevented, or mitigated potential or actual adverse impacts on human rights, however there is often a lack of transparency in relation to the partnerships between States and private companies with regard to technology products or services used in border management.

---

99 UN Guiding Principles (previously cited), Principle 4
100 UN Guiding Principles (previously cited), Commentary to Principle 4
101 UN Guiding Principles (previously cited), Commentary to Principle 4
102 UN Guiding Principles (previously cited), Principle 7 and Commentary
104 UN Guiding Principles (previously cited), Principle 7b.
Border externalization is an increasingly common method by which States evade their obligations under international law to protect people on the move, including with the assistance of various security and migration management technologies. Amnesty International defines externalization as a broad spectrum of actions implemented outside of the territory of the State that people are trying to enter, usually through enhanced cooperation with other countries. These policies may consist of formal, stand-alone legal agreements, or they may comprise a variety of informal arrangements or actions contained within broader cooperation agreements, diplomatic dialogues, projects, compacts or programs established between States which include – but go beyond – migration issues.

In practice, border externalization often takes the form of practices that shift the responsibility of providing international protection for refugees and asylum-seekers to other countries or which enlist host and transit countries in tightening control over their borders. These policies are often punitive, or preventative and in most instances, the primary goal of externalization is to reduce the number of people arriving to a destination country. Externalization policies can include, but are not limited to: the relocation of border enforcement zones, the outsourcing of border enforcement to other countries, as well as increased use of military grade security mechanisms at borders, increasingly enabled by digital technology. All of these policies are made possible by the deployment of various forms of new technology, including surveillance technology, biometric data capture, and unregulated data sharing agreements between federal and international agencies and state and local law enforcement bodies, as well as between countries. Many of these practices are also made possible by products and services of the booming border security market, which has been predicted to reach a $65-68 billion dollar valuation by 2025, with particular expansion expected in biometrics and artificial intelligence sectors. While “measures to keep people from reaching sanctuary are as old as the asylum tradition itself,” the involvement of corporations in this area of state function is relatively new. As a result of the experimental nature of many migration management tools, as well as the absence of regulation of their use, the use of technology as a form of border externalization often exacerbates inequality and injustice for people on the move.

---

110 Refugee Law Lab, Technological Testing Grounds (previously cited), p. 34.
Although externalization policies are not unlawful per se, Amnesty International has noted that the externalization of border control and asylum processing, in particular, pose significant human rights risks, including the right to seek asylum, and the principle of non-refoulement, among others. These policies generally have a disproportionate impact on persons from Africa, Central and South America, the Caribbean, the Middle East, and South Asia, and are often fueled by racialized, xenophobic, and ethnonationalist politics that seek to exclude certain groups from regions on discriminatory bases.

Meanwhile, other technology-enabled policies impacting people on the move can be framed as the “internalization” of borders, a process in which the infrastructure of immigration control follows a person once they have crossed a border, layering discrimination or presumption of criminality into a person’s life on the basis of their association or history with migration or asylum. Examples of internalization measures include unregulated information sharing of migrants’ personal data between State and local policing agencies, unchecked surveillance of immigrant and undocumented communities, and the use of digitized surveillance and decision-making in welfare and social protection systems, which often disproportionately impacts people with insecure citizenship status and other marginalized groups.

In each of these instances, technology-enabled policies and procedures extend the reach of the border to within the lives of more groups of people, blurring the line between border enforcement and interior policing.

Internalization of borders also impacts people besides migrants and refugees, including racialized people and economically insecure people. This is of particular concern when enormous and technologically-enabled security regimes developed by States ostensibly for the management of borders can be appropriated to curtail human rights for citizens as well, as in the case of the U.S. Customs and Border Patrol (CBP), being deployed by the U.S. government to crack down on Black Lives Matter protesters in 2020. Other security practices that may ‘internalize’ borders include the U.S. government’s suspension of constitutional protections within the so-called 100-mile zone, whereby border patrol authorities are granted exception to conduct warrantless searches and seizures anywhere within 100 miles of a U.S. border, normalizing a lesser expectation of privacy for roughly two thirds of the U.S. population. The spread of border internalization often coincides with the spread of new data intensive technologies used at and around borders.

---

128 Amnesty International considers that external migration policies include: 1) Externalization of border control: Enlisting other countries to engage in punitive or preventive policies aiming at stopping irregular border crossings by refugees, asylum-seekers and migrants; 2) Externalization of asylum-processing: Shifting to other countries the responsibility for providing protection to those seeking asylum; 3) READMISSION AGREEMENTS: Arrangements that facilitate the forcible return to their countries of origin of people with no right to remain – for example irregular migrants or people whose asylum claims were unsuccessful; 4) International assistance: Positive incentives that attempt to address the perceived causes of migration and displacement by improving living conditions and access to rights and protection in countries of origin and transit, including through the deployment of development aid, trade measures and foreign direct investment; 5) SAFE AND REGULAR PATHWAYS OF ENTRY – Policies enabling regular access to destination countries for people in need of protection (for example: resettlement, family reunification, protected entry, community sponsorships, etc.) – as well as for migrants (for example: labor migration schemes, student visas, etc.). From the perspective of international law, external migration policies – which often simply entail cooperation between States on migration issues – are not unlawful per se. However, Amnesty International considers that several types of external migration policies, and particularly the externalization of border control and asylum-processing, pose significant human rights risks. For further reading, see: Amnesty International, The human rights risks of external migration policies, (previously cited), pp. 4-6.


132 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para. 49.
Some technology-enabled forms of border externalization occur before affected groups have begun their journey. States are increasingly utilizing big data analytics and other forecasting tools to inform policymaking around asylum and movements of persons and, in some cases, to justify the utilization of more heavily militarized border surveillance and policing tools. These tools use data analysis to predict movement of persons across borders and are being adopted and utilized across a variety of contexts. The European Asylum Support (EASO), for example, has developed the Early Warning and Preparedness System (EWPS), which uses data, including weekly online search patterns through Google Trends, to develop a machine learning-based algorithm that claims to analyze events that might cause future large-scale displacement in selected regions. Other such projects include the Global Conflict Risk Index (GCRI), developed by the European Commission’s Joint Research Centre (JRC), which calculates the statistical risk of an armed conflict in any selected country, reportedly for up to four years, as well as initiatives like the Foresight Project, a partnership between the Danish Refugee Council and IBM using 25 years of historical data to predict forced displacement.

Data-driven predictive analytics in migration and humanitarian management, which mimics similar technologies that have long been a feature of military and security agencies, may have some promise for helping to stretch the capacity of overtaxed humanitarian agencies. However, the accuracy of these models has been shown to be highly variable. And while migration forecasting tools are likely not discriminatory per se, the vast majority of these predictive models are built on open source data, including information available on social media, TV news, and such sources as internet search trends. These data sources are inherently limited in scope, geography, and time, and reflect the biases and gaps of open source data more broadly, especially with the consideration of racial, class, and gender gaps in internet access where online sources are concerned. Overall, the threat of bias and error and the lack of safeguards to protect against potential discrimination in use requires consistent human intervention and rigorous human rights assessments of such tools to identify and mitigate their potential to result in adverse outcomes for people on the move, including by justifying the increase of border securitization and surveillance.

133 Refugee Studies Centre, Automating Immigration and Asylum (previously cited), p. 15.
134 Refugee Studies Centre, Automating Immigration and Asylum (previously cited), p. 15.
138 Refugee Studies Centre, Automating Immigration and Asylum (previously cited), p. 16-17
139 Refugee Studies Centre, Automating Immigration and Asylum (previously cited), p. 16-17

States around the world are increasingly enacting highly militarized security infrastructure at their borders,\(^{144}\) in ways which are often designed to deter or discourage potential entry by migrants and asylum seekers even before travel begins.\(^{146}\) These infrastructures also impact communities living in territories near borders in destination countries, increasing police and surveillance infrastructure in regions where populations may already be subject to high levels of poverty as well as racialized or unequal policing.\(^{147}\) Many of these border security and surveillance measures are enabled by technology, and may threaten the right to seek asylum by threatening people on the move with violence, detention, or other inhumane treatment.\(^{148}\) States often justify the legitimacy of border securitization\(^ {149}\) measures as essential to national security, in ways which may frame migration and seeking asylum itself as a criminal activity.\(^ {150}\)

Technology-enabled early detection tools are increasingly used in monitoring and securing border zones, including in the form of military-grade drones and “unmanned mobile robots” in the European Union (EU) context.\(^ {151}\) Other such detection technologies include radar, high-tech cameras, satellite data, and electro-optical sensors,\(^ {152}\) all of which may constitute forms of migration deterrence. The U.S. border, for example, has been similarly reinforced with militarygrade technologies of surveillance and deterrence, including a network of 55 security towers equipped with cameras, heat sensors, motion sensors, and other so-called “smart” border technologies.\(^ {153}\) Other border security technologies appear to serve very little practical purpose other than as methods of deterrence and intimidation, such as the case of the “robotic patrol dogs,” equipped with attached sniper rifles, tested at the border by the US in 2022.\(^ {154}\)

By pushing back potential migrants or forcing them to take alternative routes to the border, these militarized border technologies may contribute to an increase in migrant deaths by pushing people on the move to take more dangerous routes to avoid detection or interception.\(^ {155}\) Many of these technologies are untested and experimental by nature,\(^ {156}\) operating outside regulation and having been put into operation without human rights impact assessments having been conducted,\(^ {157}\) thus forcing migrants and asylum seekers to serve as test subjects. Other forms of technology that impact the lives and rights of people on the move before their journey starts include information and intelligence sharing programs between countries.\(^ {158}\) These information sharing tools, which often take the form of interoperable databases,\(^ {159}\) are a form of technological infrastructure that allows predominantly global minority countries to collect and share enormous quantities of private data about people on the move.\(^ {160}\) This information may reflect underlying biases and inaccuracies that are common to biometric data\(^ {161}\) such as the misrecognition of Black people by facial recognition technologies or the de facto exclusions

\(^ {144}\) UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, “Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para. 54.


\(^ {156}\) Article 19, When Bodies Become Data: Biometric Technologies and Free Expression, April 2021, https://www.article19.org/10.1093/hrlr/ngaa057
This information can also be used to form the basis of algorithmic risk assessments for migrants in the processing of their migration or asylum status determination. Limited or inaccurate data can lead to profiling of high risk groups, including refugees and asylum seekers from racialized groups or countries in the Global Majority, as in the case of unreliable “gang-member affiliation databases” whose information is shared between the U.S. and other countries, as well as between U.S. domestic police departments and federal agencies. Increased data sharing and interoperability of data between countries can serve as an accelerator of inequality in access to the global migration and asylum system, exacerbating pre-existing marginalization of groups who already have a heightened risk of discriminatory outcomes. This is exemplified by, for example, the biometric identity databases developed jointly between destination and origin countries to aid in the facilitation of tracking and deporting refugees. In a variety of instances around the world, data sharing without firewalls or regulation opens the door to unequal and discriminatory policing of people moving across borders.

Other forms of surveillance prior to interaction with a physical border may include social media monitoring of people on the move, as in the case of a Texas National Guard operation that infiltrated a private communication channel for migrants on WhatsApp. The International Organization for Migration (IOM) has also developed the Displacement Tracking Matrix, which monitors people on the move, including their social media activity and mobile phone records. In some cases, such social media monitoring may extend outward to others, including human rights defenders and journalists who may be working with or adjacent to migrant or refugee communities. Monitoring of private communications and social media threatens the right to privacy for people on the move, particularly when this monitoring is used in the process of issuing asylum or immigration status decisions.

---

168 “In another example, DHS is developing the Homeland Advanced Recognition Technology System (HART) to replace its current centralized biometric database. ICE will enable DHS to aggregate and compare biographical and biometric data on hundreds of millions of people across the globe. This includes so-called encounter data from police stops, facial recognition, DNA, iris scans, and voice prints—usually gathered without the individual’s knowledge or consent. The massive HART database draws from widespread biometrics collection in all realms—for example, the US DOS INL’s development of integrated DNA databases in Mexico and Central America in the name of combating trafficking or the proposed national biometric digital ID in Mexico. In this way, multiple state initiatives merge, and the power of the state to police, track and control migrants and all people under their watch grows exponentially.” For more, see: The Transnational Institute, The Everywhere Border (previously cited), pp. 6-7.
171UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para. 17.
Systemic racism is embedded in migration and border control policies and practices, resulting in direct and indirect forms of racial discrimination. The principles of equality and non-discrimination run throughout international human rights law and standards and aim to achieve formal equality in law and in practice. However, as the former Special Rapporteur on contemporary forms of racism has noted, immigration laws and policies are not race-neutral and reinforce racial inequalities and discrimination. Thus, digital technologies have and exacerbate racially discriminatory impacts on migrants and refugees on the basis of race, ethnicity, national origin, descent, citizenship status, religion, and other characteristics.

As highlighted by the former Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance in her 2020 report on emerging digital technologies and racial discrimination:

“THERE CAN NO LONGER BE ANY DOUBT THAT EMERGING DIGITAL TECHNOLOGIES HAVE A STRIKING CAPACITY TO REPRODUCE, REINFORCE AND EVEN TO EXACERBATE RACIAL INEQUALITY WITHIN AND ACROSS SOCIETIES. A NUMBER OF IMPORTANT ACADEMIC STUDIES HAVE SHOWN CONCRETELY THAT THE DESIGN AND USE OF TECHNOLOGY ARE ALREADY HAVING THIS PRECISE EFFECT ACROSS A VARIETY OF CONTEXTS.”
Several forms of technology-enabled interventions at and around physical borders are being used in the reception of people on the move.\textsuperscript{175} Many states have deployed digitally-enabled surveillance and policing tools at their borders. This infrastructure often relies on technologies originally built for military or national security purposes, often subjecting migrants and asylum seekers to the presumption of criminality,\textsuperscript{176} and further applying a national security lens to an arena that should be fundamentally rights-based. As previously discussed, these digitally-enabled surveillance and policing tools also often include interoperable databases that share fingerprints and biometrics between police agencies and international humanitarian organizations.\textsuperscript{177}

In many cases, these digitized interventions at the border form what some have termed “immigration surveillance,”\textsuperscript{178} wherein expanded capabilities for identifying individuals, controlling mobility, and sharing information, has the effect of weakening human rights protections for migrants and asylum seekers, both while interacting with border authorities and for long after.\textsuperscript{179}
Over the past several decades, there has been an unprecedented increase in global inequality and extreme wealth disparity, with the world’s poorest now owning just 2% of the world’s wealth and the world’s richest owning 76%. This has also resulted in a rapid rise in poverty as a root cause and facilitator of human rights violations around the world, as well as increasing adoption of policing and governing tools that effectively criminalize poverty itself. Amnesty International and other organizations have argued that meaningful efforts at mitigating structural inequality must be rooted in an acknowledgement of its material and historical roots, most of which are directly linked to colonial systems of oppressive and violent economic extraction. In so doing there is a need to engage an intersectional approach that acknowledges how various forms of marginalization (racial, gender, socio-economic, disability, etc.) do not function separately, but are exacerbated by one another. These intertwined forms of inequality are often exacerbated by seemingly neutral systems of power that are increasingly digitally-enabled, or which are extensions of existing inequalities outside of the digital realm.

(Continued on Next Page)
Today’s global crisis of inequality is reflective of decades of policymaking that has deliberately prioritized the interests of the powerful against the needs of the Global Majority – the digital sphere merely mirrors and extends this power imbalance. Such imbalances are also directly linked to recent history; global inequalities of race, gender, disability, and income are explicitly rooted in historical systems of oppression and extractive political economies, including “racist economic extraction and exploitation that occurred during the colonial era.”  

Broadly speaking, inequality occurs along multiple vectors, including gender, socio-economic, disability and race. As such, it must be understood as pertaining to violations of both civil and political rights (right to freedom of expression, right to privacy, etc.) but also economic and social rights (right to social security, right to housing, right to an adequate standard of living, right to decent working conditions, etc.).

When considering the impact of new technologies on migrants and refugees, these intersecting inequalities are crucial to understanding how technology-enabled rights violations are tested upon certain populations, before often becoming widespread.

---


Biometrics\textsuperscript{187} are some of the most common forms of technology used for identification, verification, and authentication purposes for people on the move.\textsuperscript{188} A range of national and international agencies are building biometric databases to process and store the information of people at and around borders, including to identify origin and transit countries and verify refugees’ and migrants’ identities.\textsuperscript{189} Biometric data can make use of fingerprints, retinal scans, facial and voice recognition, as well as blood vessel and vein patterns, ear shapes, gait, and more, for the purpose of verifying a person’s identity.\textsuperscript{190} The utility and accuracy of such identification tools, many of which in multiple studies display significantly higher rates of false positives for racialized groups including Black and Indigenous populations,\textsuperscript{191} remains an open question.

\textbf{THE UTILITY AND ACCURACY OF SUCH IDENTIFICATION TOOLS, MANY OF WHICH IN MULTIPLE STUDIES DISPLAY SIGNIFICANTLY HIGHER RATES OF FALSE POSITIVES FOR RACIALIZED GROUPS INCLUDING BLACK AND INDIGENOUS POPULATIONS, REMAINS AN OPEN QUESTION.}

Despite calls from human rights organizations to ban their use,\textsuperscript{192} States are increasingly using biometric data as the basis for identity verification, both for citizens\textsuperscript{193} and non-citizens. Mounting evidence suggests that this technology poses direct threats to the rights to privacy, non-discrimination and equality, and the right to remedy, among others.\textsuperscript{194}

States and international organizations frequently partner with private sector actors to build tools for capturing, storing, and sharing biometric data,\textsuperscript{195} raising questions about the transparency and safety of sensitive information sharing, particularly when this function is outsourced to for-profit actors.\textsuperscript{196} Some of these partnerships are now the basis of some of the world’s largest databases of biometric data. EURODAC, a massive biometric data collection system, is the basis of enforcement for the EU’s Dublin Regulation and requires refugees to immediately surrender fingerprints and often other biometric information. As of 2023, EURODAC was fast approaching its maximum capacity of 7 million datasets,\textsuperscript{197} and poised for expansion.\textsuperscript{198} A range of human rights organizations have called for a halt to the expansion of EURODAC, citing its frequent inaccuracy and use in justifying deportations and detention of people seeking asylum.\textsuperscript{199}
The U.S., for its part, is currently developing the Homeland Advanced Recognition Technology System (HART), which will enable the Department of Homeland Security (DHS) and other users to access the biographic information of more than 260 million people, including DNA. This tool, which will reportedly also include data such as officer comments, relationship patterns, and more, will reportedly enable widespread dissemination of private information about citizens and noncitizens alike, both domestically and internationally. International agencies such as the UNHCR and the UN World Food Programme have also partnered with state agencies and private actors to build and use biometric identity management tools. This use case may pose a direct threat to the rights of people in need of humanitarian protection. The collection of biometric data at and around borders, including DNA analysis, seems poised to expand alongside accompanying human rights violations.

Surveillance made possible by biometric data is a form of technology that can multiply the impacts of structural inequality. Marginalized, oppressed, or groups otherwise facing structural barriers are often among the first on whom new forms of biometric-enabled surveillance technology are tested, and for whom there are the fewest safeguards when these tools cause undeniable and serious harm. Other highly marginalized groups, including people who rely upon humanitarian aid, people experiencing homelessness, as well as populations with highly restricted movement, such as Palestinians living in the Occupied Territories, are much more likely to be subject to biometric data collection, and are much less likely to have the right to opt out. Refugees and migrants, who often experience multiple forms of marginalization and inequality, including racial, social, and economic inequalities, are often among the groups for whom new uses of biometric data capture are tested. Widespread use of biometric data capture for people on the move also opens the door to its use in racially-biased interior policing and in other settings. Biometric technology therefore acts as a multiplier of inequality for multiple groups, threatening the rights to privacy, non-discrimination, and equality.

ALGORITHMIC BIAS

An algorithmic system is a set of instructions that is used in support of various steps of decision-making processes. Algorithms have repeatedly been shown to perpetuate, amplify and entrench historic discrimination or other biases. Biases generally stem from data imbued with historical biases or through the (deliberately or unconsciously) biased choices of the individuals who design, develop, and deploy algorithmic decision-making systems. One of the most frequently reported impacts of algorithms on human rights is the impact on the right to equality and non-discrimination. Although algorithmic decision-making (ADM) systems are often cited as a method by which States can streamline social services and prevent fraud, a more consistent outcome is the penalization of society’s most marginalized groups for attempting to access their rights and/or essential services. These systems have been shown to disproportionately associate people who already experience one or multiple forms of marginalization with higher criminal, financial, or social risk.

Algorithmic decision-making in asylum and migration management systems can result in arbitrary decisions which may be impossible to challenge in the absence of procedural safeguards.

VULNERABLE TO BIAS, SYSTEM FAILURE AND OTHER ERRORS, THE USE OF THESE TOOLS COULD HAVE A DEVASTATING IMPACT ON REFUGEES AND MIGRANTS INCLUDING FAMILY SEPARATION, DEPORTATION AND DENIAL OF ASYLUM.

It can also lead to racial and ethnic profiling and discriminatory denial of visas to people, based on their real or perceived ethnicity, race, national origin, descent, religion, and other characteristics.

---

ALGORITHMIC DECISION-MAKING

The use of algorithmic decision-making (ADM) by government entities that manage movement of persons across borders is increasingly common, as part of a larger expansion of ADM into governance more broadly.\(^{219}\) Although ADM in the public sector is often presented as objective and unbiased, it is virtually impossible to create a value-neutral technology or database that is free from bias.\(^{220}\) Algorithmic systems have been repeatedly shown to replicate or exacerbate underlying racial, economic, and social inequalities,\(^{221}\) including for migrants and asylum seekers, who are often subject to experimental uses of new forms of ADM without sufficient safeguards or protections.\(^{222}\)

Some States, including Canada, and various countries in the European Union, have begun rolling out or experimenting with the use of algorithmic risk assessment tools for the approval or rejection of asylum applications,\(^{224}\) or for the screening of visas for employment sponsorship,\(^{225}\) and even systems that purport to screen a person’s risk in an application for marriage.\(^{226}\) Other States, including the UK, Sweden, and Norway,\(^{227}\) have experimented with the use of ADM in the process of undertaking and issuing decisions on a person’s asylum petition.\(^{228}\) Uses of algorithmic risk assessment have also been reported in the processing of citizenship and visa applications, as in the example of a now defunct “triaging” system used by the UK Home Office between 2015 and 2020,\(^{229}\) which was revealed to use a color coding system that flagged certain applicants from “suspect nationalities” with higher risk.\(^{230}\) Some uses of risk assessment algorithmics in the migration process provide the pretext on which countries make decisions about detention and release. The Risk Classification Assessment (RCA) employed by U.S. Immigration and Customs Enforcement (ICE) in coordination with the Department of Homeland Security (DHS),\(^{231}\) is one such automated risk tool. Researchers have shown that this system, in particular, leads to a drastic increase in the number of migrants detained without bond by ICE,\(^{232}\) particularly among those designated as low risk.\(^{233}\) Such risk assessment tools, which are also used in the criminal justice sector,\(^{234}\) are often open to manipulation\(^{235}\) and highly prone to perpetuate racial discrimination and other forms of bias.\(^{236}\)

---


222 Amnesty International, Digitally Divided (previously cited), 16-17.

223 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Report, 10 November 2020, UN Doc. A/75/950, para. 57.


228 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Report, 10 November 2020, UN Doc. A/75/950, para. 44.


Other new and experimental forms of ADM at the border include systems that merge algorithmic risk assessment with identity verification, including speech, voice, and dialect recognition software, automated transliteration tools, data extraction tools, and so-called emotion recognition software.237 Although these tools are often cited as a way of providing another layer of security in the process of issuing asylum and immigration claims, many scholars and activists have pointed out that the accuracy and neutrality of these tools remains uncertain, particularly in the absence of any standards for transparency,238 and particularly when populations detained or processed at borders have very little ability to opt out of engaging with such systems. Dialect recognition and transliteration software piloted by Germany, for example, has never been subject to expert outside review, and has been shown to display huge gaps in accuracy for certain dialects of Arabic and Persian dialects, potentially discriminating against migrants and refugees who speak these dialects.239 Other forms of extractive and potentially privacy violating technologies at the border include mobile phone data analysis and extraction for the purpose of establishing identity and screening migrants,240 particularly when migrants or refugees are unable to present identification documents.241 Such practices also include the automated analysis of mobile phone data, often in the context of illegal seizure of mobile phones from migrants.242

237 Vidushi Marda and Ella Jakubowska, “Emotion (Mis)Recognition: is the EU missing the point?” 2 February 2023, Article 19, https://www.article19.org/resources/eu-emotion-misrecognition/

238 UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement (previously cited), para. 25.

239 Automating Immigration and Asylum (previously cited), p. 46.


241 Automating Immigration and Asylum (previously cited) p. 50.

As States enact more measures to push back on the right to seek asylum and the right to freedom of movement, technology-enabled security interventions increasingly extend into the lives of people who have already crossed borders.\textsuperscript{243} Such technology-enabled tools, such as the widespread use of facial recognition systems, amplify racist policing, normalize the use of surveillance technology in more areas of public life, threaten the right to protest,\textsuperscript{244} and multiply the forms of inequality that are experienced by people who, regardless of citizenship status, experience forms of racial, economic, or social marginalization.\textsuperscript{245} As new technological tools are increasingly the method by which states justify or enact racist and xenophobic ideologies under the banner of national security,\textsuperscript{246} these tools, in the absence of human rights oversight, inevitably impact more and more groups of people. In other words, technology-enabled rights violations that take place external to or at physical borders are often the testing ground on which they are refined before their use is expanded and normalized,\textsuperscript{247} subjecting more and more groups of people to the rights violations experienced by refugees and migrants.

\textsuperscript{243} Cecilia Menjívar, “Immigration Law Beyond Borders: Externalizing and Internalizing Border Controls in an Era of Securitization,” (previously cited).


\textsuperscript{245} Amnesty International, Digitally Divided (previously cited), p. 10.

\textsuperscript{246} UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Report, 10 November 2020, UN Doc. A/75/590, para. 3.

\textsuperscript{247} Technological Testing Grounds (previously cited), p. 16.
An increasingly common outcome for migrants and asylum seekers who have crossed international borders is some form of forcible confinement, or detention, often as a strategy of deterrence. The adverse and inhumane conditions in immigration detention facilities around the world have been well documented, including in for-profit facilities that are increasingly common in the United States. Migration-related detention often amplifies inequalities and patterns of discrimination, both because it targets racialized people and economically marginalized people and because human rights violations often occur in detention facilities. Immigration detention facilities have also been linked to increasingly unsafe and unsanitary conditions for people residing in them.

Any form of detention must respect all peoples’ right to the presumption of liberty, and any imposed restrictions on this right must be clearly prescribed by law, strictly justified by a limited purpose, necessary, proportionate, and non-discriminatory.

Technology-enabled alternatives to detention (ATD) are one of the most common and pervasive ways that digital tools undermine human rights for migrants and refugees. Several forms of ATD have been linked to human rights violations, particularly where such systems are built with technology that is experimental, faulty or implemented with little oversight or transparency. GPS ankle tagging of asylum seekers and immigrants for the purpose of electronic monitoring, for example, has been referred to as a form of “digital shackles,” with reports of physical and mental harm and privacy violations which may be unnecessary and/or disproportionate. Other such ATD technologies include smartwatches which require wearers to take photos of themselves up to five times a day, as in the case of the technology contracted by a private British company for the security purposes of the UK Home Office, and a smartphone application used by ICE in the United States, which requires immigrants to check in daily by submitting a selfie for facial recognition matching, and share their phone’s GPS

IT TARGETS RACIALIZED PEOPLE AND ECONOMICALLY MARGINALIZED PEOPLE AND BECAUSE HUMAN RIGHTS VIOLATIONS OFTEN OCCUR IN DETENTION FACILITIES


The privacy of migrants and asylum seekers – and in some cases their family members – is at risk of being violated through the constant surveillance of their movements, in ways which may be neither proportionate nor necessary.

While the interference with an individual’s right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful, people on the move – with precarious immigration status; migrants, refugees, and asylum seekers alike – are increasingly required to sacrifice more of their personal data and privacy in order to reunite with family, avoid the degrading conditions of brick-and-mortar detention, or gain access to asylum. Technology-driven alternatives to detention bring to the fore the question of whether these are proportionate or necessary, particularly when they disproportionately impact Black and racialized people, impact peoples’ health and ability to obtain work, and have wide-ranging privacy implications.

---

264 Immigration Cyber Prisons: Ending the Use of Electronic Ankle Shackles (previously cited), pp. 12-17.
ECONOMIC, SOCIAL AND CULTURAL RIGHTS

Other technology-enabled harms impact refugees and migrants after they have crossed borders, and while they are attempting to access their rights to social protection, decent working conditions, and other basic elements of survival. A complex reality of migration around the world is that many States rely on the movement of migrants and refugees as a way of accessing cheap and highly exploitable labor, often allowing borders to function as a filter for migrants who are considered “safe” or “legitimate” while criminalizing those who are deemed unworthy. Many countries host refugees and migrants, including undocumented people, who remain in a state of constant surveillance and fear, and are often criminalized or punished for seeking to access their economic, social, and cultural needs, even as their labor and taxable income is freely accessible to the communities in which they reside. Such surveillance often takes the form of ATDs such as GPS ankle tagging, which collects vast amounts of personal and sensitive data and can create additional obstacles to migrants attempting to access work, basic goods, and public services as well as significantly limiting mobility. Such devices are faulty or require constant maintenance. Other uses of technology include technology-enabled case management and data aggregation tools, some of which have been shown to be used in workplace raids against undocumented people. This surveillance and deprivation, which is often made possible by means of technology-enabled tools, exacerbates the inequalities experienced by racialized groups and other marginalized people, and reflects underlying historical patterns of colonial extraction.

Many municipalities and governments have adopted some form of automated or machine enabled decision-making in tools for managing or making decisions around whether an individual qualifies for government assistance. These systems have been shown to disproportionately connect people who already experience one or multiple forms of marginalization with higher criminal, financial, or social risk. These biases disproportionately impact racialized people and groups from ethnic minority backgrounds, groups including refugees and asylum seekers. One such system implemented in the Netherlands, for example, used an algorithmic decision-making system designed to predict the likelihood of a person to commit tax or benefits fraud, and was exclusively deployed in “problem neighborhoods,” a proxy designation that disproportionately impacted people living in poverty and people with immigrant backgrounds. An automated system used to distribute welfare benefits to asylum seekers in Norway reportedly requires consistent human input to guarantee its accuracy and guard against errors, raising questions about the untested nature of many automated systems in welfare allocation. This is of particular concern where States implement such systems without sufficient oversight and as a cost-cutting measure, and with substantial evidence to show that high-tech tools are often used to justify the surveillance and punishment of marginalized people. The double bind of undocumented people means that people living in extreme poverty, including women and children, may also be less likely to seek life-saving food, healthcare, or housing assistance because of their understanding that accessing these necessities may put them at risk of surveillance and criminalization.

270 Coda Story, “For migrants under 24/7 surveillance, the UK feels like ‘an outside prison’” (previously cited).
272 Amnesty International, Trapped by automation: Poverty and discrimination in Serbia’s welfare state, (previously cited), pp. 16-17
274 Amnesty International, Trapped by Automation (previously cited), pp. 16-17
276 Automating Immigration and Asylum (previously cited), p. 57
278 Asad L. Asad, “The everyday surveillance of undocumented immigrants,” (previously cited).
Migrant workers with particular types of visas and migrants with irregular migration status, who seek work after crossing international borders, may experience rights violations at work that are increasingly exacerbated by new forms of technology.²⁷⁹ Migrant populations, including refugees and undocumented people, may struggle to find work outside of sectors with little formal protection for workers’ rights.²⁸⁰ These sectors include work in the gig economy, such as delivery driving and ride sharing,²⁸¹ as well as care work,²⁸² agricultural work,²⁸³ and warehouse work.²⁸⁴ Migrants, in particular those in an irregular situation, are therefore disproportionately more likely to experience rights violations in the workplace, and lack the ability to seek redress or other work because of precarious visas or lack of status.²⁸⁵

A growing number of workplace rights violations are made possible by new forms of technology. Migrant workers in these sectors are disproportionately likely to be subject to workplace surveillance²⁸⁶ and algorithmic management.²⁸⁷ All of these systems are technology-enabled systems that allow employers to make use of unregulated data capture to push workers to produce more in shorter windows of time, and for lower wages. Workplace surveillance²⁸⁸ and management technologies also enable the widespread and unregulated capture of workers’ biometric data.²⁸⁹ Technologies such as wearable employee trackers and surveillance cameras have also been shown to discourage workers from taking breaks and to push the speed of work in ways that may contribute to more workplace injuries.²⁹⁰ Migrant workers are also overrepresented in the growing ‘click work’ sector,²⁹¹ including in image labeling and content moderation supply chains that make social media platforms and AI tools²⁹² suitable for public consumption.²⁹³ These industries, which often operate among third-party contractors in companies with little oversight or protection for workers’ rights, have been shown to cause undue mental stress to workers,²⁹⁴ and generally offer extremely low wages.²⁹⁵

²⁸⁶ Amnesty International, ‘Don’t worry, it’s a Branch of Amazon,’ (previously cited), p. 16.
²⁹³ “Refugees help power machine learning advances at Microsoft, Facebook, and Amazon.” (previously cited).
orders and the movement of persons across them have historically functioned as ordering mechanisms, facilitating the extraction of resources from colonized and subjugated people, and exacerbating unequal hierarchies of power that are at the root of today’s crisis of inequality. The digital technologies that facilitate rights violations at and around borders today are extensions of pre-existing systems of racial, economic, and social inequality, and are increasingly deployed to criminalize the lives and curtail the rights of some of the world’s most marginalized people. As E. Tendayi Achiume, UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, has written: “Technology is the new border enforcer, and it discriminates.”

Governments around the world should work to rein in the unregulated development and deployment of technologies that impact the lives of people on the move around the world. States must fulfill their obligations under international human rights law to protect the rights of refugees and migrants and not use new and untested technologies to circumvent their obligations. Companies that develop and own these technologies must fulfill their responsibilities to respect human rights including by being transparent. They must publicly disclose what due diligence they have done on their technologies that are used in border and migration management, including what risks and abuses they have identified and what measures they have taken to prevent actual harm and mitigate risk, so that governments and civil society can hold them accountable for rights abuses linked to these technologies.

---

296 Harsha Walia, “The border is surveillance: abolish the border,” in Mizue Aizeki and others (editors), Resisting Borders and Technologies of Violence, p. 11.


AMNESTY INTERNATIONAL IS MAKING THE FOLLOWING RECOMMENDATIONS WHEN IT COMES TO THE USE OF DATA-INTENSIVE DIGITAL TECHNOLOGIES THAT ACCELERATE INEQUALITY FOR REFUGEES AND MIGRANTS:

**STATES SHOULD:**

Address systemic racism and inequality that historically and increasingly shape migration management, asylum systems, border, labor management, and immigration enforcement.

Conduct human rights impact assessments and data protection impact assessments in advance of the deployment of digital technologies and throughout their lifecycle.

Before any system is deployed, assess and establish the necessity and proportionality of the measure, as any technologies or surveillance measures adopted must be lawful, necessary and proportionate, and serve a legitimate aim under international human rights law.

Incorporate human rights safeguards against abuse into any use of technologies, including those that are used in managing laborers in sectors that disproportionately impact refugees and migrants.

Give individuals the opportunity to know about, provide or withdraw consent for, and challenge any measures to collect, aggregate, retain, and use their personal data.

Require businesses involved in developing and providing technologies in the context of refugee registration and border enforcement, including big data, artificial intelligence and biometric systems, to undertake human rights due diligence, in line with international standards such as the UN Guiding Principles on Business and Human Rights and the OECD’s Guidance on due diligence.

Hold technology companies liable for human rights harms they have caused or contributed to, or for their failure to carry out human rights due diligence.

Protect people’s data, including ensuring principles of data minimization, security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage.

Ensure that individuals who have experienced human rights violations resulting from being subject to the misuse of technologies have access to effective remedies.

Enact legislation to ban the use, development, production, sale and export of remote biometric recognition technology for mass surveillance as well as remote biometric or facial recognition technology used for identification purposes used within their own jurisdictions.

Prohibit automated risk assessment and profiling systems in the context of migration management, asylum, and border control.

Prohibit any use of predictive technologies that wrongfully threaten the right to seek asylum.

Prohibit AI-based emotion recognition tools, especially in the context of migration, asylum, and border control management.

Carefully monitor and assess the working conditions in sectors that disproportionately impact migrants, including new industries such as content moderation and image labeling, to ensure standards of non-discrimination and rights for workers.
ORGANIZATIONS AND SERVICE PROVIDERS DEPLOYING DIGITAL TECHNOLOGIES

Conduct human rights due diligence and data protection impact assessments in advance of the deployment of digital technologies and throughout their lifecycle.

Before any system is deployed, assess and establish the necessity and proportionality of the measure, as any technologies or surveillance measures adopted must be lawful, necessary and proportionate, and serve a legitimate aim under international human rights law.

Address the risk that these tools will facilitate discrimination and other rights abuses against racialized people and communities, people living in poverty, and other marginalized populations.

Explore alternative, non-invasive avenues that could meet the needs identified by service-providers, without unduly compromising the right to privacy, equality and non-discrimination.

Incorporate safeguards against abuse into any use of technologies.

Give individuals the opportunity to know about, give or withdraw consent for and challenge any measures to collect, aggregate, retain, and use their personal data.