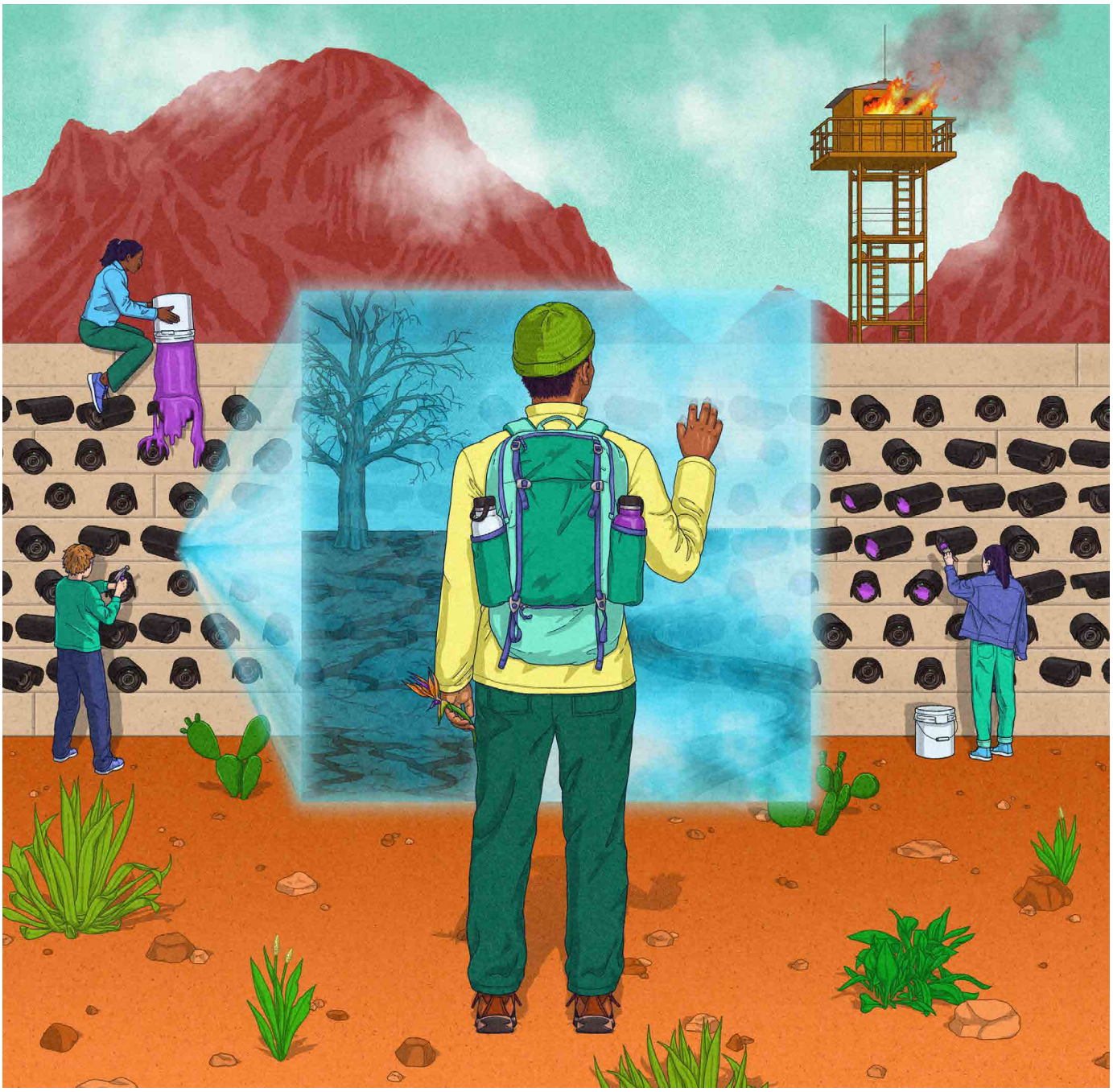

PRIMER: DEFENDING THE RIGHTS OF REFUGEES AND MIGRANTS IN THE DIGITAL AGE

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which 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.

First published in 2024
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street,
London WC1X 0DW, UK

Index: POL 40/7654/2024
Original language: English

amnesty.org

Cover Illustration by Eliana Rodgers:"A Dream Deterred". A migrant is confronted by mass surveillance at a border crossing and is reminded of his uncertain future. Activists work to resist these surveillance systems and walls.

AMNESTY INTERNATIONAL

CONTENTS

This primer is an introduction to the pervasive and rapid deployment of digital technologies in asylum and migration management systems that create and sustain systemic discrimination. It presents a high-level snapshot of some of the key digital technology developments in asylum and migration management systems, in particular systems that process large quantities of data, and highlights some of Amnesty International's key human rights concerns. This primer is not intended to be an exhaustive mapping of all digital developments to date in this field but rather a starting point for those considering how to defend the rights of refugees and migrants in the digital age.

With special thanks to Dr Keren Weitzberg and Roya Pakzad who undertook the scoping research and identified the human rights issues outlined in the report, and to the grassroots organisations and individuals who took part in the research and generously shared their knowledge and expertise, including, among others: Surveillance Resistance Lab, Derechos Digitales, Privacy International, ChinaMade project at the University of Colorado, Human Rights Watch, Access Now and The Migration Technology Monitor at the Refugee Law Lab, York University.

1. Dr Keren Weitzberg is a tech and migration researcher who works at the intersection of science and technology studies, migration studies, and critical race studies. She examines problematics related to mobility, digital identity, biometrics, and fintech in East Africa and beyond.
2. Roya Pakzad is the founder and director of Taraaz, a research and advocacy non-profit working at the intersection of technology and human rights. She is also an affiliated scholar at UC Berkeley's CITRIS Policy Lab.

1. DIGITAL TECHNOLOGY IN MIGRATION MANAGEMENT AND ASYLUM SYSTEMS: WHY IS IT A HUMAN RIGHTS CONCERN?

Digital technology interventions are increasingly shaping and delivering the migration management and asylum policies of states. While Amnesty International and other civil society organizations have long documented grave human rights violations by governments in deterring, preventing, pushing back and punishing people on the move, including refugees and asylum seekers,[3] more recently these policies and practices have become overlaid with rapidly expanding digital technology capabilities developed by private tech companies.[4] The proliferation of digital technologies and so called "smart border" technology has created new forms of private-public partnerships, and with them a gamut of human rights threats. From electronic monitoring, satellites, and drones to facial recognition, "lie detectors" and iris scanning, there is a growing and urgent need to investigate and understand these technologies and their impact.

Digital technologies are reinforcing border regimes that discriminate based on race, ethnicity, national origin, and citizenship status. Inherent racism is deeply ingrained within migration management and asylum systems. These technologies risk perpetuating and concealing racial biases and discrimination under the guise of neutrality and objectivity rooted in historical and colonial practices of racialised exclusion.[5] Their use disproportionately impacts racialised people and creates different forms of

3. For all relevant Amnesty International publications on refugees and asylum seekers, please see amnesty.org which can be found here: https://www.amnesty.org/en/search/refugees
4. Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement,* 17 December 2021, UN Doc. A/HRC/48/76, para. 47, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/379/61/pdf/G2137961.pdf?OpenElement; Amnesty International, "Mandatory Use of CBP One Application Violates the Right to Seek Asylum", (Index: AMR 51/6754/2023), 7 May 2023, https://www.amnesty.org/en/documents/amr51/6754/2023/en; Amnesty International, "Automated technologies and the future of Fortress Europe", 28 March 2019, https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe
5. Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited); Special Rapporteur, E. Tendayi Achiume, Report: *Contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, 10 November 2020, UN Doc. A/75/590, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/304/54/pdf/N2030454.pdf?OpenElement

discrimination. Much more robust safeguards against these technologies are needed, as the human rights risks to migrants, refugees and asylum seekers remain steadily on the rise and continue to perpetuate racial exclusion and discrimination.

Amnesty International recognises that digital technology could support the respect, protection and promotion of refugee and migrants' rights in certain situations, for example through connecting people on the move with vital services and reliable information.[6] Yet, it still entails risks including to the rights to privacy and non-discrimination. People on the move are increasingly perceived as "security threats", and "national security" measures are continuously implemented to exclude people based on their perceived race, ethnicity and religion, among other grounds. For example, disproportionate and unlawful surveillance and other measures increasingly used for racial profiling and policing create and sustain human rights violations, and are also increasingly adopted for use against asylum seekers, refugees and migrants, broadly. These measures and uses of digital technologies are a slippery slope towards the erosion of crucial protections for communities on the move. The combination of corporate interests, a general lack of respect for the rights of people on the move, and systemic racism and discrimination can allow technology to develop faster than the sufficient safeguards and oversight required to hold an ever-growing tech sector to account.

6. Mark Latonero and Paula Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control", 20 March 2018, https://journals.sagepub.com/doi/full/10.1177/2056305118764432

2. KEY TERMINOLOGY A-Z

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.

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 behaviour.

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.[7]

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.[8]

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

7. The Engine Room, *Primer: Biometrics in the Humanitarian Sector*, July 2023, https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Primer-2023.pdf
8. Todd Miller, "Why climate action needs to target the border industrial complex", 1 November 2019, Al Jazeera, https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex; Tanya Golash-Boza, "The immigration industrial complex: why we enforce immigration policies destined to fail", 18 March 2009, Sociology Compass, Volume 3, issue 2, p. 295–309.

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.

FACIAL RECOGNITION

A computer vision technique – that is, a method of visually identifying objects, people and terrain in computer systems – used to identify the faces of humans. This happens using a reference facial image (for example a picture gathered from CCTV footage), together with an algorithm previously trained to map, identify, and compare images served to it via other databases (for example, drivers' license registries, social media profiles, etc).

Facial recognition technology (FRT) for identification (also known as 1:n facial recognition) is a technology of mass surveillance by design, and as such is a violation of the right to privacy.

Facial recognition for authentication (commonly known as 1:1 facial recognition) uses a different process, in which two images are directly compared, and usually involves the person in question, for example when an image of a person is directly compared to their passport photo, or when one uses one's face to unlock a phone.

GPS TECHNOLOGIES

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

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 compounded 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 abuse.

RACIAL DISCRIMINATION

The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) defines racial discrimination as:

> **"any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life."[9]**

9. International Convention on the Elimination of All Forms of Racial Discrimination, Article 1, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

"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.

SYSTEMIC RACISM

The United Nations Human Rights Council Advisory Committee has pointed out that racism is a systemic problem that:

> **"operates through an interrelated or closely coordinated network of laws, policies, practices, attitudes, stereotypes and biases. It is upheld by a wide range of actors, involving State institutions, private sector and societal structures more broadly. It results not only in express, direct, de jure or intentional discrimination, but also in covert, indirect, de facto or unintentional discrimination, distinction, exclusion, restriction or preference on the basis of race, colour, descent or national or ethnic origin. It is frequently rooted in historical legacies of enslavement, the trade in enslaved Africans and colonialism. And it tends to govern opportunities and outcomes across generations."[10]**

TECHNO-SOLUTIONISM

The idea that complex social, economic and political problems can be overcome by technology.

10. Human Rights Council Advisory Committee, Advancing racial justice and equality by uprooting systemic racism, 8 August 2023, UN Doc. A/HRC/54/70, para. 7, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G23/140/55/pdf/G2314055.pdf?OpenElement

3. THE IMPACT OF DIGITAL TECHNOLOGY ON THE RIGHTS OF REFUGEES AND MIGRANTS

3.1 TECH-ENABLED "ALTERNATIVES TO DETENTION" (ATD)

Migration-related detention is often abusive and discriminatory, both because it is often arbitrary and targets racialised people and because human rights violations by states and abuses by private entities often happen during migration detention.[11] Migration-related detention carries the risk of having racially disparate impacts by targeting people on the basis of their perceived race, ethnicity, and religion.[12] Moreover, detention in itself constitutes a severe restriction of human rights and a serious intrusion on the right to liberty in particular, which can only be restricted in specific and most exceptional of circumstances. Under international law, the enjoyment of personal liberty 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 shall be clearly prescribed by law, strictly justified by a legitimate purpose, necessary, proportionate and non-discriminatory.

Several states have adopted ATD programmes, purportedly to reduce the use of immigration detention, including measures such as bail, designated residence, home curfews, community-based supervised release or case management.[13] Some governments have also adopted non-custodial programmes

11. Amnesty International, Forced Out or Locked Up: *Refugees and Migrants Abused and Abandoned*, (Index: EUR 53/5735/2022), 27 June 2022, https://www.amnesty.org/en/documents/eur53/5735/2022/en; Amnesty International, *Latvia: Return Home or Never Leave the Woods: Refugees and Migrants Arbitrarily Detained, Beaten and Coerced into "voluntary" Returns*, (Index: EUR 52/5913/2022), 12 October 2022, https://www.amnesty.org/en/documents/eur52/5913/2022/en; Amnesty International, *Libya: 'No One will Look for You': Forcibly Returned from the Sea to Abusive Detention in Libya*, (Index: MDE 19/4439/2021), 15 July 2021, *https://www.amnesty.org/en/documents/mde19/4439/2021/en*. Amnesty International, *Canada: "I didn't feel Like a Human in There": Immigration Detention in Canada and Its Impact on Mental Health*, (Index: AMR 20/4195/2021), 17 June 2021, https://www.amnesty.org/en/documents/amr20/4195/2021/en
12. Amnesty International, "States must end racist treatment of Haitian asylum seekers", 20 June 2023, www.amnesty.org/en/latest/news/2023/06/end-racist-treatment-haitian-asylum-seekers; Amnesty International, *Stop racism, not people: Racial profiling and immigration control in Spain*, (Index: EUR 41/011/2011), 14 December 2011, https://www.amnesty.org/en/documents/eur41/011/2011/en; Amnesty International, '*Between Life and Death': Refugees and Migrants Trapped in Libya's Cycle of Abuse*, (Index: MDE 19/3084/2020), 24 September 2020, www.amnesty.eu/wp-content/uploads/2020/09/Libya-report-Between-life-and-death.pdf
13. International human rights law restricts the use of both custodial and non-custodial measures, namely 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.

based on tech-enabled electronic ATD products (e-ATDs), such as electronic ankle monitors, voice recognition and facial recognition apps For example, in 2004 the United States (US) Department for Homeland Security (DHS) initiated two programmes, the Intensive Supervision Appearance Program (ISAP) and the Electronic Monitoring Device Program, to implement non-custodial measures for migrants and asylum seekers. According to US Immigration and Customs Enforcement (ICE), they were intended to "provide expanded options for release of adult aliens, by assisting officers in closely monitoring aliens released into the community".[14] The ISAP program reached over 350,000 enrolees but has been on the decline.[15]

While these products proliferate, academics and human rights defenders have linked these programmes to actual and potential human rights violations.[16] One significant concern is the lack of transparency or oversight when it comes to the privacy or security measures taken by companies in designing and developing e-ATD tools. This is not only a matter of weak cybersecurity measures or concerns over data breaches. 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, which can be unnecessary and/or disproportionate. In addition, opaque data-sharing practices between private companies, third-party partners, and government agencies (including law enforcement agencies and border control offices) are also cause for alarm. For example, corporate partnerships between ICE and tech companies such as Palantir have also been directly linked to the ability of the agency to use broad data surveillance practices to hone in on, detect and detain undocumented migrant workers. Nearly 700 workers were detained by ICE during a 2019 raid of a Mississippi chicken processing factory, with multiple media sources alleging the use of the Palantir-supplied Falcon – a relationship mapping and predictive tool in use by ICE Homeland Security Investigations (HSI) – to power the operation.[17]

Palantir has denied any wrongdoing to Amnesty International, stating that it "does not own or control data but enables its customers to analyze their own data".[18]

Additionally, e-ATDs – either as electronic ankle monitors or voice monitoring devices – are prone to false positives and technical glitches that might result in penalizing migrants arbitrarily, including for their manner of speaking or accent, which disproportionately affects racialized people.[19]

In 2016, the United Kingdom (UK) brought in mandatory electronic ankle "tagging" of all foreigners facing deportation.[20] In August 2021, this was extended to include those on immigration bail. By September 2022, nearly 15,000 people were enrolled in electronic monitoring in the UK, expanding a system that puts at risk human rights, including the rights to dignity and respect, privacy and bodily autonomy. In May 2022, plans to deploy more advanced forms of these already invasive surveillance

14. Wesley J. Lee, Acting Director of Detention and Removal Operations, US Immigration and Customs Enforcement, memorandum for Field Office Directors. "Eligibility Criteria for Enrollment into the Intensive Supervision Appearance Program (ISAP) and the Electronic Monitoring Device (EMD) Program." 11 May 2005, available at: https://www.scribd.com/document/24704584/ICE-Guidance-Memo-Eligibility-Criteria-for-Enrollment-Into-the-Intensive-Supervision-Appearance-Program-ISAP-and-the-Electronic-Monitoring-Device
15. TRAC, Syracuse University, "Detained Immigrant Population Grows to Nearly 40,000, the Highest Point in Nearly Four Years", 16 November 2023, https://trac.syr.edu/whatsnew/email.231116.html
16. Johana Bhuiyan, The Guardian, "Migrant advocates sue US government for data from surveillance program", 14 April 2022, https://www.theguardian.com/us-news/2022/apr/14/immigration-advocates-alternative-to-detention-lawsuit-ice
17. Amnesty International, *USA: Failing to do right: The urgent need for Palantir to respect human rights*, (Index: AMR 51/3124/2020), 28 September 2020, https://www.amnesty.org/en/documents/amr51/3124/2020/en; Mijente, "BREAKING: Palantir's technology used in Mississippi raids where 680 were arrested", 4 October 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Palantirs_technology_used_in_Mississippi_raids_where_680_were_arrested.pdf
18. The full Palantir letter can be found in the annex of this report: Amnesty International, *USA: Failing to do right: The urgent need for Palantir to respect human rights*, (Index: AMR 51/3124/2020), 28 September 2020, https://www.amnesty.org/en/documents/amr51/3124/2020/en
19. Jack Karsten and Darrell M. West. "Decades later, electronic monitoring of offenders is still prone to failure," Brookings Institute (Techtank blog), 21 September 2017, https://www.brookings.edu/articles/decades-later-electronic-monitoring-of-offenders-is-still-prone-to-failure; Bajorek, Joan Palmiter, Harvard Business Review, "Voice Recognition Still Has Significant Race and Gender Biases." 10 May 2019, https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases
20. Ministry of Justice, Electronic Monitoring Statistics Publication, England and Wales: September 2022, 20 October 2022, https://www.gov.uk/government/statistics/electronic-monitoring-statistics-publication-september-2022/electronic-monitoring-statistics-publication-england-and-wales-september-2022 (accessed 25 January 2024)

practices were rolled out; a data protection impact assessment (DPIA) shared by the UK's Home Office in a Freedom of Information request by Privacy International revealed plans to roll out a smartwatch tracking system for periodic daily monitoring of UK-based asylum seekers.[21]

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 having 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). Technology-driven alternatives to detention bring to the fore the question of whether these are proportionate, especially when they involve the usage of experimental technologies with wide-ranging privacy implications.

Another significant human rights concern is how the use of these technologies also exacerbate racial profiling and policing. Systemic racism also prompts human rights violations occurring in migration management and asylum systems, including in the use of e-ATD technologies. Inherent racism within law enforcement and immigration systems often lead to targeting of racialised people and communities, contributing to the criminalization of racialised people on the move.[22]

BOX 1: ON BUSINESS AND HUMAN RIGHTS

All companies have a responsibility to respect human rights wherever they operate in the world and throughout their operations – a concept clearly articulated in the globally acknowledged UN Guiding Principles on Business and Human Rights.[23] 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.[24]

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.[25] They should also refrain from lobbying governments to obtain concessions or advantages, such as beneficial changes in laws or policies which have a negative impact on the human rights of others.

21. Nicola Kelly, The Guardian, "Facial recognition smartwatches to be used to monitor foreign offenders in UK", 5 August 2022, https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk
22. Monish Bhatia, "Racial surveillance and the mental health impacts of electronic monitoring on migrants", 26 January 2021, Race & Class, Volume 62, Issue 3, pp. 18-36, https://doi.org/10.1177/0306396820963485
23. This responsibility was expressly recognized by the UN Human Rights Council on 16 June 2011, when it endorsed the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), and on 25 May 2011, when the 42 governments that had then adhered to the Declaration on International Investment and Multinational Enterprises of the OECD unanimously endorsed a revised version of the OECD Guidelines for Multinational Enterprises. See Human Rights and Transnational Corporations and other Business Enterprises, Human Rights Council, Resolution 17/4, UN Doc. A/HRC/RES/17/4, 6 July 2011; OECD Guidelines for Multinational Enterprises, OECD, 2011, https://www.oecd.org/daf/inv/mne/48004323.pdf
24. UN Guiding Principles on Business and Human Rights, Principle 11 including Commentary.
25. UN Office of the High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN Doc. HR/PUB/11/04, 2011, Principles 11 and 13 including Commentary, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

3.2 BORDER EXTERNALIZATION AND TECHNOLOGY

As part of efforts to prevent the irregular arrival of refugees and migrants, states in the Global North have enacted measures outside of their own borders through cooperation with other countries. Characterized as 'externalization', these measures bring immigration controls further along transit routes and can include formal agreements or informal arrangements providing funding and technical support for partner countries' border control agencies, including operational tools to facilitate containment and returns.[26]

Increasingly, border externalization policies are enacted through the deployment of sophisticated and invasive digital technologies. These technologies reinforce racialized forms of exclusion to deter the mobility of Black, Muslim, and other racialised migrants, asylum seekers and refugees.[27] For example, the European Union (EU) has expanded its borders virtually into the Mediterranean and across transit regions in Africa through a range of technologies, including radar, high-tech cameras, satellite data, electro-optical sensors (for example, motion detection), drones and biometric systems impacting Black African migrants, refugees and asylum seekers.[28]

These technologies bring additional human rights risks. The US and EU countries have entered into externalization arrangements involving data-sharing and technology exchanges with countries that have a track record of serious and widespread violations towards refugees and migrants. For example, through its provision of assets, training and coordination of assistance to Libyan authorities, the EU has enabled Libyan coastguards to intercept boats and take refugees and migrants back to Libya, where they are exposed to arbitrary detention, torture and other ill-treatment, including sexual violence, and other violations and abuse.[29] This support is bolstered by the EU's own aerial real-time surveillance: both Italy and Frontex, the European Border and Coast Guard Agency, operate drones and other aerial assets over the central Mediterranean to identify refugee and migrant boats at sea and report their position to the Libyan authorities, triggering their intervention. Frontex's Eurosur surveillance system also collects information via radar and satellites, which is shared with various countries through "Seahorse" networks.[30]

There are growing allegations that the use of technology to monitor, track and intercept refugees and migrants on their journeys may contribute to migrant deaths as migrants take more perilous routes to avoid surveillance. For example, a recent study using geospatial analysis showed a positive correlation between "hardship and suffering" – and by extension, migrant mortality, along the US-Mexico border between Arizona and Sonora state – and the expansion of "smart" surveillance infrastructure in the area. This includes sophisticated AI-driven watchtowers.[31] This case is also an example of how the use of technology has racially disparate impacts against Black, Latin American, and other racialised people and communities, increasing the risk of racial profiling along the border.[32]

---

26. Amnesty International, *Human rights risks of external migration policies*, (Index: POL 30/6200/2017), 13 June 2017, https://www.amnesty.org/en/documents/pol30/6200/2017/en/#:~:text=From%20the%20perspective%20of%20international,pose%20significant%20human%20rights%20risks
27. E. Tendayi Achiume, "Digital Racial Borders", 11 October 2021, AJIL Unbound, Volume 115, pp. 333-38, https://doi.org/10.1017/aju.2021.52
28. Ruben Andersson, *Illegality, Inc.: Clandestine Migration and the Business of Bordering Europe*, University of California Press, 2014, pp. 84-7; Frontex, *Artificial Intelligence-based capabilities for the European Border and Coast Guard*, 17 March 2021, https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_executive_summary.pdf
29. Amnesty International, "New evidence shows refugees and migrants trapped in horrific cycle of abuses", 24 September 2020, https://www.amnesty.org/en/latest/press-release/2020/09/libya-new-evidence-shows-refugees-and-migrants-trapped-in-horrific-cycle-of-abuses; Amnesty International, '*No one will look for you' Forcibly returned from sea to abusive detention in Libya,* (Index: MDE 19/4439/2021), 15 July 2021, https://www.amnesty.org/en/documents/mde19/4439/2021/en
30. Amnesty International, 'Contribution to European Ombudsman's Strategic Inquiry OI/3/2023/MHZ', 31 October 2023, amnesty.eu/news/contribution-to-european-ombudsmans-strategic-inquiry-oi-3-2023-mhz-the-role-of-the-european-border-and-coast-guard-agency-frontex-in-the-context-of-search-and-rescue-operations/
31. Samuel Norton Chambers, Geoffrey Alan Boyce, Sarah Launius, and Alicia Dinsmore. "Mortality, surveillance and the tertiary "funnel effect" on the US-Mexico border: a geospatial modeling of the geography of deterrence", 31 January 2019, Journal of Borderlands Studies, Volume 36, Issue 3, pp.443-468, https://www.tandfonline.com/doi/abs/10.1080/08865655.2019.1570861
32. Amnesty International, *In Hostile Terrain: Human Rights Violations in Immigration Enforcement in the US Southwest*, (Index: AMR 51/018/2012, 28 March 2012, https://www.amnesty.org/en/documents/amr51/018/2012/en

From the perspective of international law, external migration policies are not unlawful per se. However, policies focusing on the externalization of border control and/or asylum processing pose very significant human rights risks, and their implementation often results in refugees, asylum seekers and migrants being contained in or returned to countries where they are subjected to serious human rights violations. Among the rights at risk are the right to seek and enjoy asylum, the right not to be subjected to arbitrary arrest and detention; the right to be protected from refoulment – which prohibits States from removing or transferring anyone, in any manner whatsoever, to a place where an individual would be at real risk of torture or other serious human rights violations – [33] and the right to be free from discrimination.

In addition, externalization measures, which shift responsibility for providing international protection to third countries, exacerbate the unfair distribution of responsibility for protecting refugees between countries in the Global North and the Global South, where the vast majority of refugees are hosted. Externalization of refugee protection is also inconsistent with the principles of solidarity and international cooperation underpinning the international protection system.

3.3 DATA EXTRACTION SOFTWARE

There is a growing trend towards the use of data extraction software for immigration control. As the former Special Rapporteur on contemporary forms of racism has pointed out, it "targets only asylum seekers and is justified by racist and xenophobic political discourse".[34] In countries including Austria, Belgium, Denmark, Germany, Norway and the UK, the law allows for the phones of migrants and asylum seekers to be seized and data extracted from them for the purposes of corroborating (or not) their testimonies when processing asylum claims.[35] This may include reviewing searches, browsing and social media activity; tracking travel history through GPS records and metadata; and even accessing information on the cloud that a user may think they have deleted.[36]

The use of phone data extraction software has been the subject of a lawsuit brought by the German NGO Gesellschaft für Freiheitsrechte (GFF) on behalf of three asylum seekers.[37] The German Federal Office for Migration and Refugees (BAMF) initially introduced the policy in 2017, allowing the office to "extract and analyze data from data carriers such as phones in order to check their owner's stated origin and identity."[38] The system, which generates a report from every instance of extraction, is accessible only to lawyers but is kept out of reach from applicants. A report by the GFF summarizes that 64 per cent of cases contain no usable results, 34 per cent confirm the origin and identity claims of the individuals, while only 2 per cent contradict the applicants' claims. In the lawsuit, the plaintiffs argued that their rights to privacy were violated when German authorities routinely ordered them to unlock and hand over their mobile phones for "evaluation".[39] The court decided that, in this specific instance, the searches were routinely disproportionate since less intrusive measures would have been available. It left open the question of whether the practice could otherwise be lawful.

---

33. Amnesty International, *The Human Rights Risks of External Migration Policies*, (Index: POL 30/6200/2017), 13 June 2017, available at: https://www.amnesty.org/en/documents/pol30/6200/2017/en
34. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited), para. 33.
35. Petra Molnar, European Digital Rights (EDRi), and Refugee Law Lab, *Technological Testing Grounds: Border Tech Is Experimenting with People's Lives*. November 2020, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf, p.18.
36. Privacy International, *The UK's Privatised Migration Surveillance Regime: A rough guide for civil society,* February 2021, https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf
37. TRT World, "Refugees take Germany to court over mobile phone data checks", 6 May 2020, https://www.trtworld.com/europe/refugees-take-germany-to-court-over-mobile-phone-data-checks-36057
38. Anna Biselli, Lea Beckmann, *Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe*, February 2020, https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Gesellschaft_fur_Freiheitsrechte.pdf
39. Gesellschaft für Freiheitsrechte, 'Invading Refugees' Phones: Digital Forms of Migration Control', December 2019, https://legacy.freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf

In March 2022, the UK High Court ruled that the Home Office acted unlawfully in breach of human rights and data protection laws when it seized the phones of at least three asylum seekers arriving on small boats and pressured them into sharing their passwords.[40] Opaque policies of seizure and retention perpetuate and reinforce a hostile and unsafe environment for asylum seekers.

Involuntary data extraction for processing asylum claims poses a range of risks to human rights, including the right to privacy and the right to seek asylum, and puts individuals in danger of being forcibly returned to a country where there is a risk of persecution or other serious human rights violations. Data extraction may represent a disproportionate and unnecessary interference on refugees' and migrants' right to privacy on the basis of their status and it is often based on discrimination around race, ethnicity, national origin and citizenship status.[41] Even where such data extraction systems – due to the technical specifications of the tools in use or practice – take in all available data, they would constitute a disproportionate interference with the right to privacy per se. There are also concerns about the reliability of the data obtained by such intrusive methods, and, potentially, data extraction can be used to undermine the right to a fair asylum procedure where it enables authorities to make dubious and sweeping conclusions about an asylum seeker's application.[42] Furthermore, it also reinforces existing stigmatization and discrimination against racialised people and communities.

BOX 2: ON INTERSECTIONALITY

Whilst this primer provides a general overview of the adverse human rights impacts of digital technologies on the lives of migrants, refugees, and asylum seekers, the severity of the impacts can significantly increase depending on age, gender, sexuality, race, ethnicity, class or caste, disability, socio-economic factors, and more. In other words, age, gender, sexuality, race, ethnicity, class or caste, disability and socio-economic factors all play a role in shaping, and in some ways exacerbating the risks posed by technology for migrants, refugees, and asylum seekers. As structural discrimination does not operate in isolation, individuals may suffer additional or unique forms of discrimination due to a combination of different forms of discrimination they are subjected to.

For instance, migrant and refugee children may be more vulnerable to invasive data collection and surveillance due to their age, more limited autonomy, power imbalances between them and the adults collecting the data and even more limited understanding of the short and long-term implications of their data being collected. Governments, companies, and humanitarian actors need to take these factors into account when collecting children's biometrics.

Viewing technologies through a racial justice lens similarly highlights serious discriminatory impacts. Professor Tendayi Achiume, former Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, has written and spoken extensively on this. She has previously argued:

40. Full court ruling available here: Royal Courts of Justice, Case No: CO/4793/2020, CO/577/2021, 25 March 2022, https://dpglaw.co.uk/wp-content/uploads/2022/03/MA-KH-judgment.pdf
41. Usually, this process involves an assumption of deception, and uses reductive variables (such as language of phone device, where it was purchased, and the language in which communication is done on it) as a metric for country of provenance. Gesellschaft für Freiheitsrechte, "Germany: Invading refugees' phones – security or population control?", 11 March 2020, https://edri.org/our-work/germany-invading-refugees-phones-security-or-population-control; Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited).
42. Amnesty International, "Open Letter to the Rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure Protection of Rights of Migrants, Asylum Seekers and Refugees", 26 April 2023, https://www.amnesty.eu/wp-content/uploads/2023/04/TIGO_IOR_10_2023_3987_Open-letter-to-the-Rapporteurs-on-the-EU-AI-Act-1.pdf

Examples from different parts of the world show that the design and use of different emerging digital technologies can be combined intentionally and unintentionally to produce racially discriminatory structures that holistically or systematically undermine enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics. In other words, rather than only viewing emerging digital technologies as capable of undercutting access to and enjoyment of discrete human rights, they should also be understood as capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms."[43]

3.4 BIOMETRICS

Biometrics are among the most ubiquitous technologies deployed for identification, verification, and authentication purposes along borders. The collection and use of biometric data raise concerns of direct and indirect forms of discrimination based on race, ethnicity, national origin, descent and religion, such as the misrecognition of Black people by facial recognition technologies or the de facto exclusions based on national origin. A range of national and international agencies are building biometric databases to cross-check people against watchlists, identify origin and transit countries and verify refugees' and migrants' identities.[44] Humanitarian organizations such as the UN Refugee Agency (UNHCR),[45] and the UN World Food Programme (WFP), have developed vast global fingerprint/iris databases in an apparent effort to prevent multiple registrations and duplications of refugee data. EU member states rely heavily on databases containing biometric data, such as Eurodac,[46] which among other functions helps to determine the state responsible for processing an asylum claim made in the EU.[47]

In October 2018 the EU announced it was funding a new automated border control system to be piloted in Hungary, Greece and Latvia. Called iBorderCtrl, the project uses an artificial intelligence (AI) "lie-detecting" system fronted by a virtual border guard to quiz travellers seeking to cross borders, while assessing the minute details of their facial expressions (known as "micro expressions") using facial and emotion recognition technologies. Travellers deemed to answer questions honestly by the system are provided with a code allowing them to cross, while those not so lucky are transferred to human border guards for further questioning.[48]

iBorderCtrl is only one of many projects seeking to automate EU borders with the objective of countering irregular migration. This new tendency within Europe raises a series of serious human rights concerns, not least as such lie-detection on the basis of micro expressions has been debunked as

43. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial Discrimination and emerging digital technologies: a human rights analysis,* 18 June 2020, UN Doc. A/HRC/44/57, para. 38, https://documents.un.org/doc/undoc/gen/g20/151/06/pdf/g2015106.pdf?token=SEBp9t4TsuGpIteR0l&fe=true.
44. Claire Walkey, Caitlin Procter, and Nora Bardelli, "Biometric refugee registration: between benefits, risks and ethics", LSE Blog, 18 July 2019, https://blogs.lse.ac.uk/internationaldevelopment/2019/07/18/biometric-refugee-registration-between-benefits-risks-and-ethics/
45. UNHCR, "Biometric Identity Management System: Enhancing registration and data management", https://www.unhcr.org/media/biometric-identity-management-system
46. Irma Van der Ploeg, "The illegal body: Eurodac and the politics of biometric identification", December 1999, Ethics and Information Technology, Volume 1, https://doi.org/10.1023/A:1010064613240, pp. 295-302; Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), http://data.europa.eu/eli/reg/2013/603/oj
47. Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), http://data.europa.eu/eli/reg/2013/604/oj
48. Amnesty International, "Automated technologies and the future of Fortress Europe", 28 March 2019, https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe

rooted in phrenology, which has strong ties and parallels with eugenicist thought.[49] First named in Paul Ekman's work, "micro expressions" are misleadingly claimed to be able to establish truthfulness as a function of the frequency of eye-blinking, direction of sight, movement of facial muscles, and changes in tone of voice. The iBorderCTRL tool categorizes this data into levels of deceptiveness, on the basis of a universal baseline of the intersection between facial expressions and morality.

Such presumptions are sure to shore up undignified treatment of migrants, whose intentions are measured against pseudoscientific dissections of their facial expressions, as opposed to their stated intent. This is not only inaccurate and unnecessary, but has severe implications for the right to privacy, equality and non-discrimination, the right to asylum, and the freedom of movement.

Border monitoring systems around the EU are just one manifestation of the trend of techno-solutionism, a trend that has seen governments and tech companies alike, resort to high-tech solutions to everything from climate change to famine and migration, often distracting from the non-technical, structural policy solutions required. In light of the amount of investments in projects using automated technologies for border control purposes funded by Horizon 2020,[50] the biggest EU research and innovation programme ever, the EU's interest in this area is very clear

For instance, between 2014 and 2020, Frontex invested €434 million on surveillance and IT infrastructure; for 2021-2027, the European Commission earmarked some €34.9 billion for border control more broadly.[51] This includes, for example, the forthcoming European Travel Information and Authorisation System (ETIAS). The ETIAS system cross-references with open-source data online, including social media, medical information and more, to assess digital identity and determine the threat a traveller might pose to the security of Europe. These types of systems facilitate and reinforce racialised exclusion.[52]

In 2016 and 2020, the European Commission proposed successive revisions to the Eurodac Regulation, which sought to expand the Eurodac biometric migration database. On 20 December 2023, the Council and the European Parliament reached a political agreement on this Regulation, as part of a broader package of reforms. The reforms, which will be formally adopted in 2024, will expand the categories of personal data being stored in Eurodac, such as facial images; make the collection of biometric data mandatory for anyone over six years of age (compared to 14 years under current rules); expand the personal scope of Eurodac; and facilitate access to data for law enforcement authorities.[53]

Biometric data is considered especially sensitive as it allows the identification of an individual through a record of immutable personal characteristics. The creation of permanent biometric records of refugees and migrants poses particular human rights concerns. In the case of refugees and asylum seekers, there is a risk that their information might be shared – either intentionally (for example, as a form of state policy) or inadvertently (for example, through data breaches/insecure systems) – with authorities in the country from which they have fled, increasing the chances of further abuse and persecution

49. Amnesty International, "Amnesty International and more than 170 organisations call for a ban on biometric surveillance", 7 June 2021, https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/; Catherine Stinson, "The Dark Past of Algorithms That Associate Appearance and Criminality", January-February 2021, American Scientist, Volume 109, Number 1, p. 26, https://www.americanscientist.org/article/the-dark-past-of-algorithms-that-associate-appearance-and-criminality; Javier Sánchez-Monedero and Lina Dencik, "The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl", Information, Communication & Society, Volume 25, Issue 3, https://doi.org/10.1080/1369118X.2020.1792530, pp. 413-430.
50. European Commission, Horizon 2020, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en (accessed 25 January 2024)
51. Frontex, *Artificial Intelligence-based capabilities for the European Border and Coast Guard*, 17 March 2021, https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_executive_summary.pdf
52. E. Tendayi Achiume, "Racial Borders", 2022, Georgetown Law Journal, Volume 110, Issue 3, https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-110/volume-110-issue-3-may-2022/racial-borders
53. Council of the European Union, "The Council and the European Parliament reach breakthrough in reform of EU asylum and migration system", 20 December 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/12/20/the-council-and-the-european-parliament-reach-breakthrough-in-reform-of-eu-asylum-and-migration-system

for them and their family members.[54] Further concerns relate to the potential for surveillance, data breaches, restrictions to freedom of movement, discriminatory profiling and the further criminalization of marginalized ethnic, religious, and other racialised groups.

Outside the migration context, Amnesty International's research in the occupied Palestinian territories, for instance, uncovered how the facial recognition system, Red Wolf, deployed at Israeli military checkpoints in Hebron, was being used to restrict the movement of Palestinians in the area. Here, Amnesty International discovered that the facial recognition-enabled restriction on movement at checkpoints was not temporary or limited, but systematic and discriminatory, with the system using databases consisting only of Palestinian data, at checkpoints intended for only Palestinian people, with Jewish Israeli settlers unaffected.[55]

BOX 3: ON FACIAL RECOGNITION, MASS SURVEILLANCE AND RACISM

Facial recognition technology for identification violates the right to privacy because it cannot satisfy the requirements of necessity and proportionality under international human rights law. It entails widespread bulk monitoring, collection, storage, analysis or other use of material and collection of sensitive personal data (biometric data). Moreover, facial recognition systems are trained with image recognition algorithms that rely on vast amounts of individuals' faces as input data to improve the system's "success rate", without the individuals' knowledge or consent. Even where input data or training data is deleted, the algorithm underpinning the system has already benefitted from, and is in effect acting on the bases of, faces previously fed to the system, without the individual's knowledge or control.

Additionally, the human rights harms of facial recognition technology are not experienced equally and raise well-known discrimination risks. For instance, certain groups may be disproportionately represented in facial image datasets due to discriminatory policing or other practices. Moreover, it is well-established that facial recognition technology systems perform unequally depending on key characteristics including skin colour, ethnicity and gender. These discrimination risks have been highlighted by various UN experts.[56]

In January 2021, Amnesty launched "Ban the Scan", a global campaign to ban the use of facial recognition systems, a form of mass surveillance that amplifies racist policing and threatens the right to protest. The Ban the Scan campaign has exposed how facial recognition has violated human rights from New York City, to Hyderabad, and Hebron and East Jerusalem in the occupied Palestinian territories. In particular, Amnesty International continues to expose the ways in which the technology is deployed in discriminatory manners against historically marginalised communities.

There is also the broader danger of function creep, that is, the widening use of a technology or of data beyond its initial purpose, for example, data collection by humanitarian agencies for the purpose of registration and access to services being used for migration control. The former Special Rapporteur on contemporary forms of racism has warned and raised concerns about how data is collected and the

54. Ben Hayes and Massimo Marelli. "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases", in AI NOW Institute, Amba Kak (editors), *Regulating Biometrics: Global Approaches and Urgent Questions,* 2020, https:// www.ainowinstitute.org/regulatingbiometrics-hayes-marelli.html
55. 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/mde15/6701/2023/en; Article 49 of the Fourth Geneva Convention states: "The Occupying Power shall not deport or transfer parts of its own civilian population into the territory it occupies." It also prohibits the "individual or mass forcible transfers, as well as deportations of protected persons from occupied territory".
56. Committee on the Elimination of Racial Discrimination (CERD), Draft General Recommendation No. 36 on preventing and combating racial profiling, 14 May 2019, https://www.ohchr.org/sites/default/files/Documents/HRBodies/CERD/GC36/DraftGC36.docx, para. 23.

potential for significant discriminatory outcomes.[57] In particular, using centralized systems for storing biometric information can facilitate surveillance and misuse of information, and make data breaches more damaging. In 2018, reports emerged about the Bangladesh government sharing the biometric data of Rohingya refugees collected by UNHCR with Myanmar – the country from which they had fled ethnic cleansing and violence.These reports were later confirmed by Human Rights Watch, who accused UNHCR of providing personal information from refugees to the government of Bangladesh.[58] Biometric data, initially collected for the purposes of registration and access to services, was shared for repatriation purposes in the absence of free and informed consent by refugees, putting them at risk.

An enabling factor of these dangerous linkages is the growth of interoperability which supports data-sharing between humanitarian organizations, national governments, and security agencies. While useful in certain contexts, interoperability poses significant risks in the migration context.[59] Despite bureaucratic, national, corporate and proprietary hurdles to interoperability, there is a growth of international data-sharing arrangements between humanitarian organizations as well as border/immigration enforcement agencies. In 2019, two EU Regulations on interoperability entered into force, which merged "six existing EU databases created for security and border management purposes...into one single, overarching EU information system".[60]

Biometric and data-sharing can also be used to determine and deny access to services. Even when governments or humanitarian organisations obtain consent to data processing from refugees and migrants, this consent cannot be understood as necessarily freely given, as people cannot generally opt-out of biometric data collection without losing access to registration and essential services.[61]

In his 2013 report to the United Nations General Assembly, the UN Special Rapporteur on the human rights of migrants, François Crépeau, called on states to allow migrants to access the public services needed for the enjoyment of their rights without fear of being arrested, detained and deported. In order to do so, states should implement "firewalls" between public services and migration control, whereby public services (healthcare, education, housing, labour inspection, local police) would be instructed not to request migration status information unless essential; and migration control would not have access to the information collected by public services relating to migration status.[62]

3.5 ALGORITHMIC DECISION MAKING IN ASYLUM AND MIGRATION MANAGEMENT SYSTEMS

In a report entitled *Bots at the Gate*, researchers at the Citizen Lab at the University of Toronto surveyed various algorithmic decision-making tools developed for Canada's immigration and asylum system, both at the border and in cities. Particularly alarming was the use of algorithmic risk assessment

57. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited), para. 40.
58. Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent", 15 June 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
59. As an example, see "Weak anti-discrimination safeguards" in Statewatch and PICUM, D*ata Protection, Immigration Enforcement and Fundamental Rights: What the EU's regulations on interoperability mean for people with irregular status*, November 2019, https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf, pp. 33-34.
60. Cristina Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU", June 2021, Human Rights Law Review, Volume 21, Issue 2, https://doi.org/10.1093/hrlr/ngaa057, pp. 433–457.
61. Amnesty International interview with Marwa Fatafta of Access Now, 16 March 2021; Ben Hayes and Massimo Marelli. "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases", in AI NOW Institute, Amba Kak (editors), *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020, https:// www.ainowinstitute.org/regulatingbiometrics-hayes-marelli.html
62. UN Special Rapporteur on the Human Rights of Migrants, Report, 7 August 2013, UN Doc. A/68/283, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/421/15/PDF/N1342115.pdf?OpenElement, para 82.

tools by Canadian migration officers for the approval or rejection of visa and asylum applications.[63] Academics Petra Molnar and Lex Gil have called these initiatives a "laboratory for high-risk experiments", raising concerns about their human rights implications.[64]

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, often on the false assumption that individuals of certain nationalities or with certain characteristics pose a "migration risk" for the compliance with immigration policies or "security threats" for national security concerns.[65] These assumptions are based and justified in racist and xenophobic ideologies, discourses and structures.

Similar automated and risk-prediction methods have been deployed by the UK's Home Office.[66] In 2020, Foxglove, a non-profit organisation that fights to make tech fair for everyone, and the Joint Council for the Welfare of Immigrants (JCWI) successfully pressured the Home Office to drop its visa-streaming algorithms, which they claimed "entrenched racism and bias into the visa system",[67] through assigning certain nationalities risk scores that reinforce discrimination, combined with feedback loop problems, that use past biases and discrimination as baselines for the assessment of future cases.

BOX 4: ON SYSTEMIC RACISM AND THE PROHIBITION ON RACIAL DISCRIMINATION

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. Increasingly, digital technologies are being used to push racist and xenophobic agendas, discourses, and structures contrary to international human rights standards.

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."

63. Petra Molnar and Lex Gil. *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System,* 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf
64. Petra Molnar and Lex Gil. *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System,* 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf
65. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited).
66. Foxglove, "Home Office says it will abandon its racist visa algorithm—after we sued them", 4 August 2020, https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them; Joe Tomlinson, "EU Settlement Scheme ushers in a new era of automated decision-making at the Home Office." 16 July 2019, Free Movement, https://www.freemovement.org.uk/eu-settlement-scheme-automated-decision-making
67. Foxglove, "Home Office says it will abandon its racist visa algorithm—after we sued them", 4 August 2020, https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them

Automated risk assessment systems further pose risks to data protection rights and principles. Even when profiling is not based directly on special categories of personal data that are protected by enhanced safeguards under applicable legislation, such as the EU General Data Protection Regulation (GDPR), it may use information that indirectly reveals such data. For example, a traveller's religious beliefs or health data can be inferred from their dietary preferences, violating their right to data protection and resulting in racial profiling. Given the imbalance of power between refugees, migrants, and asylum and migration management authorities, information used for profiling systems can also be coercively and illegally extracted, without the freely given, specific, and informed consent of individuals as prescribed by the GDPR.[68]

Risk assessment tools pose further risks to individuals' right to liberty and security under international human rights law. In an opinion regarding a proposed agreement between the EU and Canada on the transfer and processing of Passenger Name Records ("PNR"), the Court of Justice of the European Union has warned that automated processing of PNR could result in binding decisions affecting a person's rights without proof that the person concerned is a public security risk.[69] A risk assessment tool which was modified to always recommend immigration detention in the United States,[70] for example, illustrates how such tools can facilitate arbitrary arrest and detention forbidden by international human rights law. In this instance, the software used to assess an individual's case was altered to remove the possibility of release, leading to an increase in undue detentions.[71]

Given stated risks to the rights to non-discrimination, privacy and data protection, as well as right to liberty and security, Amnesty International holds that automated risk assessment and profiling systems in the context of migration management, asylum, and border control must be prohibited.[72]

BOX 5: ON PRIVACY

AI technologies rely on mass data collection and processing. Their growing adoption incentivizes an expansion in data harvesting infrastructures, which in turn requires expanding surveillance capabilities.

Under international law, States must demonstrate that an interference with the right to privacy is a legal, necessary and proportionate means of addressing a legitimate aim, which means balancing the nature and the extent of the interference against the reason for interfering with the right to privacy and ensuring that the technology used is the least intrusive means available.

Widespread bulk monitoring, collection, storage, analysis or other use of material and collection of sensitive personal and biometric data without individualised reasonable suspicion of criminal wrongdoing, amounts to indiscriminate mass surveillance. Amnesty International believes that indiscriminate mass surveillance is never a proportionate interference with the rights to privacy, freedom of expression, freedom of association and of peaceful assembly. Moreover, facial recognition systems are trained with image recognition algorithms that rely on vast amounts of input

68. Amnesty International, "Open letter to the rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure protection of rights of migrants, asylum seekers and refugees", 26 April 2023, https://www.amnesty.eu/wp-content/uploads/2023/04/TIGO_IOR_10_2023_3987_Open-letter-to-the-Rapporteurs-on-the-EU-AI-Act-1.pdf
69. Court of Justice of the European Union, Case C-817/19, 21 June 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105en.pdf
70. Daniel Oberhaus, Vice, "ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention", 26 June 2018, https://www.vice.com/en/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention
71. Mica Rosenberg and Reade Levinson, Reuters, "Trump's catch-and-detain policy snares many who have long called U.S. home", 20 June 2018, https://www.reuters.com/investigates/special-report/usa-immigration-court
72. Amnesty International, "Open letter to the rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure protection of rights of migrants, asylum seekers and refugees", 26 April 2023, https://www.amnesty.eu/wp-content/uploads/2023/04/TIGO_IOR_10_2023_3987_Open-letter-to-the-Rapporteurs-on-the-EU-AI-Act-1.pdf

data from individuals' faces to improve their "success rate", without their knowledge or consent. Because such systems cannot operate without this biometric reference database, they are – as discussed earlier in this document – incompatible with the right to privacy by design.

3.6 CASE STUDY: THE CBP ONE MOBILE APPLICATION

In May 2023, new migration regulations adopted by the United States (USA) government came into force requiring asylum seekers and their families, arriving at the southern border of the United States without prior authorization, to use a mobile application – the CBP One mobile Application (CBP One) – to seek an appointment to present themselves at a port for entry into the USA.[73] While CBP One had been used prior to May 2023, the new regulations made it mandatory. The application requires asylum seekers to be physically located in specific areas inside Mexico and to request and schedule an appointment to present themselves at a port of entry, whilst also submitting personal data, including a facial photograph for facial recognition purposes.

Even prior to wider roll-out in May 2023, Amnesty International and other organizations received information regarding numerous deeply concerning problems with CBP One, such as frequent crashing of the application and flaws with the facial recognition technology disproportionately affecting racialized individuals such as Haitians, Cubans, Nicaraguans and Venezuelans.[74] Asylum seekers are forced to install the application on their mobile devices, which enables US Customs and Border Protection to collect data about their location by "pinging" their phones.

Issues that continue to be salient include problems with accessibility due to language availability or literacy barriers, lack of access to a cell phones or internet, and unavailability of appointments. Most significantly, the shortage of appointments means that many asylum seekers are left stranded and waiting for months in areas of Mexico where they are at risk of serious human rights violations, including rape and kidnappings, as reported by organizations.[75] Those who choose to cross into the USA due to threats to their security in Mexico without an appointment may be considered presumptively ineligible for asylum and at higher risk of immigration detention.[76]

The mandatory and exclusive use of CBP One undermines the right of persons arriving at the USA southern border to seek asylum and risks violating the principle of non-refoulment, a norm of customary international law. The use of facial recognition in CBP One, which appears to be referenced across a number of "derogatory databases", indicates that there's a risk of mass surveillance against groups of precarious communities on the move, compounded by GPS technologies and the digital collection of data on asylum seekers prior to entering the US. This raises serious privacy and non-discrimination concerns.[77]

73. U.S. Citizenship and Immigration Services, Proposed Rule, Circumvention of Lawful Pathways, USCIS-2022-0016-0001, 23 February 2023, https://www.regulations.gov/document/USCIS-2022-0016-0001
74. The Guardian, "Facial recognition bias frustrates Black asylum applicants to US, advocates say", 8 February 2023, https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias; Amnesty International, *Mandatory use of CBP One Application Violates the Right to Seek Asylum*, (Index: AMR 51/6754/2023), 7 May 2023, www.amnesty.org/en/wp-content/uploads/2023/05/AMR5167542023ENGLISH.pdf
75. Christina Asencio, "Asylum ban strands asylum seekers and migrants in Mexico and returns them to danger", 28 November 2023, https://humanrightsfirst.org/library/asylum-ban-strands-asylum-seekers-and-migrants-in-mexico-and-returns-them-to-danger
76. Stephanie Leutert and Caitlyn Yates, *Asylum Processing at the U.S.-Mexico Border: February 2023*, 28 February 2023, https://www.strausscenter.org/publications/asylum-processing-at-the-u-s-mexico-border-february-2023, p. 3; Amnesty International, "Amnesty International statement for hearing on "Examining the Human Rights and Legal Implications of DHS's 'Remain in Mexico' Policy", 18 November 2019, https://www.amnestyusa.org/updates/amnesty-international-statement-for-hearing-on-examining-the-human-rights-and-legal-implications-of-dhss-remain-in-mexico-policy
77. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited), para. 47.

3.7 CASE STUDY: THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

AI systems are already widely used in Europe, including drones, lie detectors, biometrics, facial recognition and other often experimental technologies, creating a vast net of mass surveillance at, within and sometimes beyond Europe's borders.[78] These have "the potential to deepen racism, racial discrimination, xenophobia and other forms of exclusion".[79] In December 2023, the European Parliament, Member States, and the European Commission reached a deal on legislation governing the use of artificial intelligence in a Regulation on Artificial Intelligence (AI Act).[80] Though the final text of the law is yet to be adopted, this is a significant step in so far as it has the potential to improve protections for people impacted by artificial intelligence. However civil society and other actors have voiced concerns about aspects of the draft Act pertaining to the use of AI systems in migration contexts,[81] as the draft does not sufficiently protect people on the move and other marginalised groups from racism, discrimination, and a range of other human rights abuses.[82] In some cases, the AI Act risks not only failing to address human rights harms in the migration context, but also facilitating them, for example by providing a legal basis for mass and discriminatory surveillance systems such as facial recognition and emotion recognition technologies used to disproportionately target people on the move, among other marginalised communities.[83]

The AI Act does not sufficiently prevent the potential harms and risks these technologies pose, nor does it currently ban outright the most dangerous among them, for example predictive analytics systems used for preventing, curtailing, or interdicting migration, and pseudo-scientific lie detectors, such as AI polygraphs.[84] In addition, EU member states are pushing to incorporate blanket exceptions in the AI Act for authorities using AI for "national security" purposes. This poses a risk of AI misuse against people on the move, and allows national security exemptions from public transparency and accountability measures on how law enforcement, migration and national security authorities are using AI systems.

The AI Act also fails to address the export of AI systems from Europe, which means surveillance and other unlawful technologies banned in the EU could be exported to countries neighbouring the EU to stop people's movement before they reach EU borders.[85] #Protectnotsurveil,[86] a cross-disciplinary coalition of partners, including Amnesty International has been calling for the AI Act to regulate all high-risk AI systems deployed in migration contexts, ban AI systems that pose an unacceptable risk and ensure that the Act applies to the EU's huge migration databases.[87]

---

78. Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch, *Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act,* 2022, https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf
79. Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Report: *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement* (previously cited), para. 24.
80. European Commission, *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*, 21 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206; Amnesty International, "AI Act must ban dangerous, AI-powered technologies in historic law", 28 September 2023, https://www.amnesty.org/en/latest/news/2023/09/eu-ai-act-must-ban-dangerous-ai-powered-technologies-in-historic-law/#:~:text=Amnesty%2C%20within%20a%20coalition%20of,without%20exceptions%20in%20the%20EU; Thierry Breton, Twitter post: "Historic! The EU becomes the very first continent to set clear rules for the use of AI. The #AIAct is much more than a rulebook – it's a launch pad for EU startups and researchers to lead the global AI race. The best is yet to come!", 8 December 2023, https://twitter.com/ThierryBreton/status/1733256557448630344
81. For example, see #Protect not Surveil website: https://protectnotsurveil.eu
82. Amnesty International, "The EU must respect human rights of migrants in the AI Act", 26 April 2023, https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act
83. Amnesty International, "AI Act must protect all people, regardless of migration status", 6th December 2022, https://www.amnesty.eu/news/eu-ai-act-must-protect-all-people-regardless-of-migration-status; Amnesty International, "Bloc's decision to not ban public mass surveillance in AI Act sets a devastating global precedent", 9 December 2023, https://www.amnesty.org/en/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-global-precedent; Amnesty International, "Council risks failing human rights in the AI Act", 29th November 2023, HTTPS://WWW.AMNESTY.EU/NEWS/COUNCIL-RISKS-FAILING-HUMAN-RIGHTS-IN-THE-AI-ACT
84. EDRi, *The EU's Artificial Intelligence Act: Civil society amendments*, 3 May 2022, https://edri.org/our-work/the-eus-artificial-intelligence-act-civil-society-amendments
85. Amnesty International, "EU policymakers : regulate police technology", 21st September 2023, https://www.amnesty.eu/news/eu-policymakers-regulate-police-technology
86. See, https://protectnotsurveil.eu
87. See, https://protectnotsurveil.eu/#calls

4. CONCLUSIONS AND RECOMMENDATIONS

Technology has become a ubiquitous and risky tool in shaping and delivering the migration management and asylum policies of states. It has the potential to create and sustain systemic racism, discrimination, and oppression, and it is continuously used to push racist and xenophobic agendas, discourses, and structures. Where states are pushing an agenda which is at odds with their human rights obligations towards refugees and migrants, these technologies risk contributing to or even exacerbating human rights violations. The technologies used in asylum and migration management may also be problematic in their own right, as their systems are vulnerable to bias and errors or lead to the collection, storage and use of information that threaten the right to privacy, non-discrimination, and other human rights.

Amnesty International is making the following recommendations when it comes to the use of data-intensive digital technologies in asylum and migration management systems:

STATES SHOULD:

- Address systemic racism, xenophobia, and discrimination that historically and increasingly shape migration management, asylum systems, border 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.
- Address the risk that these tools will facilitate discrimination and other human rights violations against racial minorities, people living in poverty, and other marginalized populations.
- Incorporate human rights safeguards against abuse into any use of technologies.
- 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 been subjected to 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 asylum.
- Prohibit AI-based emotion recognition tools, especially in the context of migration, asylum, and border control management.

ORGANIZATIONS AND SERVICE PROVIDERS DEPLOYING DIGITAL TECHNOLOGIES MUST:

- Conduct mandatory 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 racialised people and communities, people living in poverty, and other marginalized populations.
- Explore any alternative non-invasive avenues that could meet the needs identified by service-providers, without unduly compromising the right to privacy, equality and non-discrimination, and freedom from surveillance.
- 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.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@amnesty

PRIMER: DEFENDING THE RIGHTS OF REFUGEES AND MIGRANTS IN THE DIGITAL AGE

This is an introduction to the pervasive and rapid deployment of digital technologies in asylum and migration management systems across the globe including the United States, United Kingdom and the European Union.

Defending the Rights of refugees and Migrants in the Digital Age, highlights some of the key digital technology developments in asylum and migration management systems, in particular systems that process large quantities of data, and the human rights issues arising from their use. This introductory briefing aims to build our to collective understanding of these emerging technologies and hopes to add to wider advocacy efforts to stem their harmful effects.

INDEX: POL 40/7654/2024
JANUARY 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL