A/HRC/48/76

Advance Unedited Version

Distr.: General
22 September 2021

Original: English

Human Rights Council
Forty-eighth session
13 September–1 October 2021
Agenda item 9
Racism, racial discrimination, xenophobia and related forms of intolerance, follow-up to and implementation of the Durban Declaration and Programme of Action

Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement

Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance[1]*

Summary

The present report complements the Special Rapporteur's prior report to the Human Rights Council, entitled "Racial discrimination and emerging digital technologies: a human rights analysis", and aims to highlight how digital technologies are being deployed to advance the xenophobic and racially discriminatory treatment and exclusion of migrants, refugees, and stateless persons. In some cases, discrimination and exclusion occur in the absence of explicit animus, but as a result of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards. The report also notes that vast economic profits associated with border securitization and digitization are a significant part of the problem.

[1] * The present report was submitted late to reflect the most recent information received in response to a call for submission issued by the mandate.

Contents

		Page
I.	Introduction	3
II.	The Rise of Digital Borders	4
III.	Mapping Racial and Xenophobic Discrimination in Digital Border and Immigration Enforcement	9
	A. Direct and indirect discrimination	9
	B. Discriminatory Structures	12
IV.	Recommendations	20

I. Introduction

1. The present report continues the analysis initiated by the Special Rapporteur in her prior report to the Human Rights Council, entitled "Racial discrimination and emerging digital technologies: a human rights analysis".[2] In that report, the Special Rapporteur introduced an equality-based approach to the human rights governance of emerging digital technologies, with a focus on the intersection of these technologies with racial equality and non-discrimination principles under international human rights law. She urged State and non-State actors to move beyond "colour-blind" or "race-neutral" strategies that ignore the racialized and ethnic impact of emerging digital technologies, and instead to confront directly the intersectional forms of discrimination that result from and are exacerbated by the widespread adoption of these technologies. This approach further entails moving beyond the tendencies of human rights and regulatory frameworks to focus only on explicit prejudice in the prohibition of racial discrimination. The prior report examined discrimination on the basis of race and ethnicity (including indigeneity), and drew attention to the effects of gender, religion, and disability status. The present report brings additional nuance by focusing on the xenophobic and racially discriminatory impacts of emerging digital technologies on migrants, stateless persons, refugees and other non-citizens, as well as on nomadic and other peoples with migratory traditions. In this analysis, the term "refugees" includes asylum seekers who meet the refugee definition but whose status as refugees has not been formally recognized by any State. Furthermore, this report addresses how the deployment of emerging digital technologies to contain the COVID-19 pandemic has accelerated these discriminatory trends.

2. Digital technologies now play a central role in mediating the enjoyment of fundamental rights, with States and private corporations relying upon these technologies to deliver essential goods and services.[3] Experts have usefully coined the term "digital borders"[4] to specify borders whose infrastructure increasingly relies upon machine learning, big data, automated algorithmic decision-making systems, predictive analytics and related digital technologies. These technologies form part of identification documents and systems, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases and even visa and asylum decision-making processes. Recently, border and immigration enforcement has experienced accelerated digitization in response to the COVID-19 pandemic.

3. Although emerging digital technologies are now prevalent in the governance of all aspects of society, unique concerns exist in the border and immigration context for at least two reasons. Under most, if not all, national governance frameworks:

(a) Non-citizens, stateless persons and related groups have fewer rights and legal protections from abuse of State power, and may be targeted by unique forms of xenophobic private violence;

(b) Executive and other branches of government retain expansive discretionary, unreviewable powers in the realm of border and immigration enforcement that are not subject to the substantive and procedural constraints typically guaranteed to citizens.

4. Refugees, migrants and stateless persons are subject to the violations enumerated in this report on account of their national origin, race, ethnicity, religion and other impermissible grounds. These violations cannot be dismissed as permissible distinctions between citizens and non-citizens. In this regard, the Special Rapporteur calls attention to her prior report on racial discrimination on the basis of citizenship, nationality and immigration status.[5]

5. Digital borders enhance the scope and precision of the racially discriminatory operation of borders. Governments and non-state actors are developing and deploying emerging

[2] A/HRC/44/57.

[3] See, e.g., A/74/493; A/73/348; A/HRC/44/57.

[4] See, e.g., Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" (2007).

[5] A/HRC/38/52.

digital technologies in ways that are uniquely experimental and dangerous in the border and immigration enforcement context. By so doing, they are subjecting refugees, migrants, stateless persons and others to human rights violations, and extracting large quantities of data from these groups on exploitative terms that strip them of fundamental human agency and dignity. Although this report focuses on recent technological innovations, many of these technologies have historical antecedents in colonial technologies of racialized governance.

6. The analysis in the Special Rapporteur's previous report on racial discrimination and emerging digital technologies is essential background for this report. That report is especially helpful for explaining the mechanisms that cause racial discrimination through emerging digital technologies, and for highlighting the economic, political and other societal forces driving the expansion in the discriminatory use of these technologies. Here, she reiterates that notwithstanding widespread perceptions of emerging digital technologies as neutral and objective in their operation, race, ethnicity, national origin and citizenship status shape access to and enjoyment of human rights in all fields in which these technologies are now pervasive. States have obligations to prevent, combat and remediate this racial discrimination, and private actors, such as corporations, have related responsibilities to do the same. In the context of border and immigration enforcement, preventing human rights violations may require outright bans or abolition of technologies due to a failure to control or mitigate their effects.

7. Not only is technology not neutral, but its design and use typically reinforce dominant social, political and economic trends. As highlighted in previous reports, the resurgence of ethnonationalist populism globally has had serious xenophobic and racially discriminatory consequences for refugees, migrants and stateless persons.[6] This report highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies which have proliferated in part due to widespread perceptions of refugees and migrants as *per se* threats to national security. In other cases, discrimination and exclusion occur not due to explicit animus, but because of the pursuit of bureaucratic and humanitarian efficiency without necessary human rights safeguards. The ongoing securitization of borders, and related massive economic profits, are a significant part of the problem.

8. This report reflects valuable input from: expert group meetings hosted by the Promise Institute for Human Rights at the University of California, Los Angeles, (UCLA) School of Law, the UCLA Center for Critical Internet Inquiry, the Institute on Statelessness and Inclusion, and the Migration and Technology Monitor; interviews with researchers, including stateless persons, migrants and refugees; and submissions received by a range of stakeholders in response to a public call for submissions. Non-confidential submissions are available on the webpage of the mandate.

II. The Rise of Digital Borders

9. Technology has always been a part of border and immigration enforcement, and instruments ranging from passports and even physical border walls are all properly understood as features of this technology. This report specifically focuses on the growing prevalence of *digital* technologies in immigration and border enforcement. The COVID-19 pandemic has accelerated this trend by encouraging the reliance on technological solutions to migration challenges. The "border industry" has begun advocating for "contactless biometrics" technology to combat the spread of the virus,[7] and public health and national security concerns are used to justify increased tracking and data collection of migrants.[8]

10. As a general matter, digital border technologies are reinforcing parallel border regimes that segregate the mobility and migration of different groups on the basis of national origin

6 See, e.g., A/73/312.

7 https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

8 https://www.opendemocracy.net/en/pandemic-border/covid-19-can-technology-become-tool-oppression-and-surveillance/.

and class, among other grounds. Automated border controls are one example of parallel border regimes in action. At Irish ports of entry, such as Dublin Airport, e-passport holders from EU/EEA and Switzerland can go through "eGates" on a "self-service" basis to clear immigration control.[9] "Only certain nationalities can adopt the 'self-service' approach, and the nationalities included are affluent and white nations (with the exception of Japan)"; non-nationals of EU/EEA or Switzerland traveling from outside Ireland by air or sea must present themselves to an Immigration Officer upon arrival.

11. One facet of the digital border is the expansive use of biometrics or the "automated recognition of individuals based on their biological and behavioural characteristics."[10] Biometrics can include fingerprint data, retinal scans, and facial recognition, as well as the recognition of a person's vein and blood vessel patterns, ear shape, and gait. Biometrics are used to establish, record and verify the identity of migrants and refugees. For example, the United Nations (UN) has collected the biometric data of over 8 million people, most of them fleeing conflict or needing humanitarian assistance.[11] Researchers have documented the racialized origins of biometric technologies,[12] as well as their contemporary discriminatory operation on the basis of race, ethnicity and gender.[13] A report on facial recognition technology (FRT) deployed in border crossing contexts such as airports, notes that even though the best algorithms misrecognize Black women twenty times more than White men, the use of these technologies is increasing globally.[14] Accordingly, "where facial recognition is applied as a gate-keeping technology, travellers are excluded from border control mechanisms on the basis of race, gender and other demographic characteristics (e.g. country of origin)." This differential treatment frequently perpetuates negative stereotypes, and may even entail prohibited discrimination that could lead to *refoulement*.

12. Governmental and humanitarian biometric data collection from refugees and migrants has been linked to severe human rights violations against these groups, notwithstanding the bureaucratic and humanitarian justifications behind the collection of this data. Furthermore, it is unclear what happens to this collected biometric data and whether affected groups have access to their own data. The UN's World Food Program (WFP), for example, has been criticised for partnering with data mining company Palantir Technologies for a $45 million (USD) contract and sharing 92 million aid recipients' data.[15] Private corporations such as Palantir have proved essential in providing the technology that supports the detention and deportation programs run by the United States (US) Immigration and Customs Enforcement (ICE) and the Department of Homeland Security (DHS),[16] raising justified concerns of corporate complicity in human rights violations associated with these programs. It is not yet clear what data sharing accountability mechanism will be in place during the WFP-Palantir partnership or whether data subjects will be able to opt out.[17] Data collection is not an apolitical exercise, especially when powerful Global North actors collect information on vulnerable populations with no regulated methods of oversight and accountability.[18] The

9 Immigrant Council of Ireland, Submission.

10 https://www.biometricsinstitute.org/what-is-biometrics/.

11 These enormous data sets are notoriously hard to track and can also include the retrofitting of old data with newly collected biometrics. See, e.g., http://humanitarian-congress-berlin.org/2018/.

12 See, e.g., Simone Browne, *Dark Matters: On the Surveillance of Blackness* (2015).

13 A/HRC/44/57.

14 Tamir Israel, Facial Recognition at a Crossroads: Transformation at our Borders & Beyond (2020).

15 https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

16 https://www.technologyreview.com/2018/10/22/139639/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/.

17 https://www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307.

18 Dragana Kaurin, Data Protection and Digital Agency for Refugees, (2019).

increasingly fervent collection of data on migrant populations has been criticized for its potential to cause significant privacy breaches and human rights concerns.[19]

13. History provides many examples of the discriminatory and even deadly use of data collection from marginalized groups. Nazi Germany strategically collected vast amounts of data on Jewish communities to facilitate the Holocaust, largely in partnership with a private corporation: IBM.[20] Other genocides also relied on systematic tracking of groups, such as the Tutsi registries based on ethnicity identity cards, which facilitated the magnitude of the Rwandan genocide.[21] Post 9-11, the US experimented with various modes of data collection on marginalized populations, which collected photographs, biometrics, and even first-person interview data from over 84,000 flagged individuals coming from mostly Arab States. [22] In all of these cases, different actors, including governments, exploited ideas about the neutrality or non-prejudicial necessity of data collection to target marginalized groups on a discriminatory basis.

14. Autonomous technologies are also increasingly used in monitoring and securing border spaces. For example, FRONTEX, the European Border and Coast Guard Agency, has been testing unpiloted military-grade drones in the Mediterranean and Aegean for the surveillance and interdiction of vessels containing migrants and refugees hoping to reach European shores.[23] An investigation by Bellingcat, Lighthouse Reports, Der Spiegel, TV Asahi and Report Mainz produced credible evidence in October 2020 that FRONTEX has been complicit in pushbacks,[24] or the forced returns of refugees and migrants over a border without consideration of individual circumstances and without possibility to apply for asylum or appeal. Such pushbacks likely violate non-refoulement obligations under international law, and are aided by surveillance technologies. Legal developments in Greece have permitted the police to use drone surveillance to monitor irregular migration in border regions, but allow doing so without ensuring the requisite legal protections for the human rights of those subject to this surveillance. [25]

15. The usage of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security, and the increasing criminalization of migration and use of risk-based taxonomies to demarcate and flag cases.[26] States, particularly those experiencing large numbers of refugee and migrant arrivals, have been using various methods to pre-empt and deter those seeking to legally apply for asylum. This normative shift towards criminalization of asylum and migration works to justify increasingly hard-line and intrusive technologies such as drones and various border enforcement mechanisms like remote sensors and integrated fixed-towers with infra-red cameras (so-called autonomous surveillance towers) to mitigate the 'threat environment' at the border.[27] These technologies can have drastic results. While so-called "smart-border" technologies have been called a more humane alternative to other border enforcement regimes, studies have documented that such technologies along the US-Mexico border have actually increased migrant deaths and pushed migration routes towards more dangerous

19 https://www.chathamhouse.org/2018/03/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants.

20 Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* (2012).

21 https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/.

22 http://www.aaiusa.org/nseers.

23 Petra Molnar, "Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up" (2020).

24 https://www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks; https://www.spiegel.de/international/europe/eu-border-agency-frontex-complicit-in-greek-refugee-pushback-campaign-a-4b6cba29-35a3-4d8c-a49f-a12daad450d7.

25 Homo Digitalis, Submission.

26 See Dimitri Van Den Meerssche, Submission.

27 Raluca Csernatoni, "Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management" (2018).

terrains.[28] Chambers et al. have found that migrant deaths have more than doubled since these new technologies have been introduced,[29] creating a "land of open graves."[30]

16. The use of these technologies by border enforcement is only likely to increase in the 'militarised technological regime'[31] of border spaces, without appropriate public consultation, accountability frameworks, and oversight mechanisms. In the Korean peninsula's Demilitarized Zone ("DMZ"), "South Korea (Republic of Korea) has deployed stationary, remote-operated semi-autonomous weapons[.]"[32] The South Korean government has stated that it has no intent to develop or acquire lethal autonomous weapons systems.[33] Due to a lack of transparency, often the status of autonomous weapons systems' deployment on borders is difficult to determine. In anticipation of such deployment, it is crucial that States account for and combat the disproportionate racial, ethnic and national origin impacts that fully autonomous weapons would have on vulnerable groups, especially refugees, migrants, asylum seekers, stateless persons, and related groups.

17. Member States and multiple organs of the UN are increasingly relying on Big Data analytics to inform their policies. For example, the International Organization for Migration's Displacement Tracking Matrix[34] monitors populations on the move to better predict the needs of displaced people, using mobile phone call records and geotagging, as well as analyses of social media activity. In the US, Big Data analytics are also being used to predict likely successful outcomes of resettled refugees based on pre-existing community links.[35] In an increasingly anti-immigrant global landscape, criticisms have surfaced that migration data has also been misinterpreted and misrepresented for political ends, for example to affect the distribution of aid. Inaccurate data can also be used to stoke fear and xenophobia, as seen in the characterization of the group of migrants attempting to claim asylum at the US-Mexico border[36] or the galvanization of anti-migrant sentiments in the Mediterranean, including the recently proposed floating barrier walls.[37] Societal fear is then used to justify increasingly hard-line responses that contravene international human rights law.[38] As one submission notes, in polarized, anti-immigrant and even xenophobic political contexts, "the data used to inform machine learning algorithms at borders or used in political campaigns or legislation can be flawed, and in an environment of structural bias against minorities such misrepresentation of data can fuel disinformation, hate speech and violence."[39]

18. Central to assessing the human rights landscape of digital borders is the role of private corporations whose pursuit of profit has played an important role in driving the expansion of digital technology in immigration and border enforcement, often in partnerships that allow governments to abdicate responsibility for violations that may result from the use of these technologies. The term "border industrial complex" has been used to describe "the nexus between border policing, militarisation and financial interest"[40] as governments increasingly turn to the private sector to manage migration through new technologies, predominately through a national security lens that neglects fundamental human rights.[41] The externalization, militarization and automation of borders fuel the border industrial-complex.[42] In the U.S., the budget for border and immigration enforcement has

28 Samuel Norton Chambers et al., "Mortality, Surveillance and the Tertiary 'Funnel Effect' on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence" (2019).
29 Ibid.
30 Jason De León, *The Land of Open Graves: Living and Dying on the Migrant Trail* (2015).
31 Csernatoni, "Constructing the EU's High-Tech Borders".
32 Campaign to Stop Killer Robots, Submission.
33 Ibid.
34 https://dtm.iom.int/about.
35 https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/.
36 See New York University School of Law Center on Race, Inequality, and the Law, Submission.
37 https://www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.
38 See also Ana Beduschi, "International Migration Management in the Age of Artificial Intelligence" (2020); Ana Beduschi, Submission.
39 Minority Rights Group International ("MRG"), Submission.
40 https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.
41 Dhakshayini Sooriyakumaran & Brami Jegan, Submission.
42 Ibid.

increased by more than 6,000 % since 1980.[43] The EU budget for the management of external borders, migration and asylum for 2021-2027 will increase by 2.6 times, amounting to more than 34.9 billion Euros, compared to 13 billion Euros for 2014-2020.[44] Recent market research projects the compound annual growth rate for this global border security market to be between 7.2 and 8.6 % (65 to 68 million US dollars) in 2025.[45]

19. Among the emerging digital technologies that drive the border industrial complex, drones that service border monitoring and biometrics that help build "smart borders"[46] play a key role. The big corporate players and beneficiaries in the border monitoring service sector are largely Global North military companies, some of which, like Lockheed Martin, are the largest arms sellers in the world.[47] Information technology companies such as IBM are also major players, including in data gathering and processing.[48] Many of these corporate actors exert great influence in domestic and international decision-making related to the governance of the digital border industry.[49] Corporations are also linked with governments through joint ventures. For example, in 2016, French public-private company Civipol set up fingerprint databases for Mali and Senegal.[50] Financed with 53 million Euros from the EU Emergency Trust Fund for Africa ("EUTF"), these projects aim to identify refugees arriving to Europe from both countries and deport them.[51] France owns 40% of Civipol, while arms producers Airbus, Safran and Thales each own more than 10% of its shares.[52] This further illustrates the manner in which Global North countries use international aid to advance their border agendas in the Global South.

20. One researcher has highlighted the pressing concern of the rise of "technocolonialism," which highlights "the constitutive role that data and digital innovation play in entrenching inequalities between refugees and humanitarian agencies and, ultimately, inequalities in the global context"[53] fueled in part by corporate profit and government abdication of human rights responsibility. These inequalities are entrenched through forms of technological experimentation, data and value extraction, and direct and indirect forms of discrimination described in Section III.

21. In short, many digital border technologies replace or aid human decision-making processes, sometimes in ways that raise serious human rights concerns. These technologies also expand the power and control that governments and private actors can exert over migrants, refugees, stateless persons and others while simultaneously shielding this power from legal and judicial constraints. In other words, they magnify the potential for grave human rights abuses, and do so in ways that circumvent substantive and procedural protections that have otherwise been essential in the border enforcement context. Section III highlights the range of discriminatory human rights violations enabled by digital border machinery and infrastructure.

43 Ibid.

44 Ibid.

45 Ibid., citing Global Reports Store, "Global Border Security System Industry is Estimated to Grow at a CAGR of 8.6 and Reach up to 67.81 Billion by 2025" (2019); Market Research Future, "Border Security Market Research Report—Global Forecast till 2025" (2019).

46 Sooriyakumaran & Jegan, Submission.

47 Ibid.

48 Ibid.

49 Ibid., citing https://www.escr-net.org/corporateaccountability/corporatecapture.

50 Sooriyakumaran & Jegan, Submission.

51 Ibid., citing https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/eutf_2016_annual_report_final_en.pdf.

52 Sooriyakumaran & Jegan, Submission.

53 Mirca Madianou "Technocolonialism: digital innovation and data practices in the humanitarian response to the refugee crisis" (2019).

III. Mapping Racial and Xenophobic Discrimination in Digital Border and Immigration Enforcement

A. Direct and indirect discrimination

1 Online Platforms

22. Migrants, refugees and stateless persons have reported that social media platforms such as Facebook, Twitter and Whatsapp are often used to spread racist and xenophobic hatred, and some reported being targeted directly through personal messages on these platforms. In Malaysia, for example, migrants reported increasing racist and xenophobic advocacy on social media platforms during the COVID-19 pandemic. In some cases, users posted photographs of migrants and refugees they perceived to be "illegal," raising serious concerns of subsequent, real world targeting of individuals, in addition to online abuse.

23. One submission called attention to an anonymously-run blacklisting website, Canary Mission that prejudicially identifies students, professors and activists who have publicly advocated for Palestinian rights, primarily targeting people of Arab descent. It reported that information published on Canary Mission has been used by Israeli immigration officials in the context of administration and enforcement of Israeli borders, and the borders of the occupied Palestinian territory, including to deny entry.[54] Such practices violate equality and non-discrimination rights, as well as freedom of expression protections and leave those whose rights are violated with limited avenues of redress.

2 Racial Profiling

24. Consultations with migrants, refugees and stateless persons also highlighted the role of digital technologies in racial and ethnic profiling in border enforcement. In November 2020, the Committee on the Elimination of Racial Discrimination adopted its General Recommendation No. 36 on preventing and combating racial profiling by law enforcement officials. It recognized that migrants, refugees and asylum seekers, people of African descent, indigenous peoples, and national and ethnic minorities, including Roma, are the groups most vulnerable to racial profiling.[55] The Committee also observed that the "the increasing use of new technological tools, including artificial intelligence, in areas such as security, border control and access to social services, has the potential to deepen racism, racial discrimination, xenophobia and other forms of exclusion."[56]

25. In consultations, participants raised concerns with ethnic profiling of Roma at the borders of Northern Macedonia. A 2017 case of racial profiling of Roma revealed that officials store biometric data of individuals prevented from crossing these borders on a STOP LIST.[57] Advocates raised valid concerns that these sorts of lists are disproportionately populated by Roma, who are subject to ethnic profiling and have limited means of redress.

3 Mandatory biometric data collection, digital identification systems, and exclusion from basic services

26. States are increasingly mandating extensive biometric data collection from non-citizens. The collection and use of this data raise concerns of direct and indirect forms of discrimination on the basis of race, ethnicity, national origin, descent and religion. In most cases, refugees, migrants and stateless persons have no control over how their data is shared. According to one submission, India requires mandatory biometric data collection

[54] Palestine Legal, Submission.
[55] CERD/C/GC/36.
[56] Ibid.
[57] See http://www.errc.org/uploads/upload_en/file/5209_file1_third-party-intervention-kham-delchevo-and-others-v-north-macedonia-5-february-2020.pdf.

from non-citizens with a primary use of this data being detention and deportation, including of refugees such as Rohingya.[58] Another concern raised in the context of India is the use of Aadhaar ID numbers to exclude migrants *de facto* from vital basic services which rely on automated systems.[59] Because refugees without residency permits are prohibited from holding Aadhaar cards, they are discriminated against and excluded from access to basic services and enjoyment of "rights that ensure a dignified refuge in India."[60] Even refugee children have reportedly been denied primary education based on not having Aadhaar.[61]

27. For stateless persons in particular, participants in consultations reported that the expansion of digital identification systems is destroying the informal means of survival that these groups have developed in the absence of proper documentation and recognition by the States in which they reside. Stateless persons, who are predominantly racial and ethnic minorities, are systematically excluded from digital identity databases and documentation. Centralized biometric ID systems challenge the internationally recognized framework of nationality and citizenship in multiple ways. Key problems include algorithmic decision-making, taking decisions on legal status out of the hands of government officials and placing them in the hands of machines or registrars administering biometric data kits. This can have the effect of de-facto denaturalization without due process or safeguards. The key considerations that must guide every nationality deprivation decision, including non-discrimination, avoidance of statelessness, prohibition of arbitrariness, proportionality, necessity and legality,[62] must also be considered when introducing centralized biometric ID systems. The introduction of digital governance structures risks deprivation of nationality by proxy measures, without due process – both intentionally and as a result of incomplete or flawed civil registration systems.[63] During consultations, participants from Kenyan Nubian and Somali communities, and Rohingya communities have reported systematic difficulties securing digital identification, which then threatened their ability to gain formal employment and satisfy other basic needs. In some cases, digital identification regimes seemed to exacerbate statelessness by resulting in exclusion and non-recognition of ethnic minority groups.

4 Language Recognition

28. Although automated registration systems may be adopted to enhance bureaucratic efficiency, their technology can produce discriminatory outcomes. According to one submission, the German Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge), "BAMF" uses TraLitA, an automatic transliteration program, to register Arabic names into the Latin alphabet[64]. However, the system is more error-prone for applicants whose names originate from the Maghreb region, at a success rate of 35% in contrast to 85 to 90% for names of Iraqi or Syrian applicants. Arabic-speaking applicants may also be subject to a dialect analysis upon registration. BAMF uses a software to analyse the applicant's spoken language sample to determine the plausibility of stated national origin. This software relies on the Arabic-Levantine dialect,[65] raising serious concerns that the software's "susceptibility to errors has never been checked by a specialist supervisory control and cannot be understood by external actors with no recourse to the algorithms used."[66] The obvious risk is that speakers of Arabic dialects not represented by the software may erroneously be deemed non-credible, and therefore excluded from legal and other protections on a discriminatory basis.

58 Anubhav Dutt Tiwari & Jessica Field, Submission.
59 Ibid.
60 Ibid.
61 Ibid.
62 Institute on Statelessness and Inclusion et al, "Principles on Deprivation of Nationality as a National Security Measure" (2020) available at: https://files.institutesi.org/PRINCIPLES.pdf.
63 Ibid., Principle 10.
64 Geselleschaft für Freiheitsrechte ("GFF"), Submission.
65 Ibid.
66 Ibid.

5 Mobile Data Extraction and Social Media Intelligence on Migrant and Refugee Populations

29. Governments are increasingly targeting the electronic devices of migrants and refugees to verify the information they provide to border and immigration authorities. Officials are able to do so using mobile extraction tools that download data from smartphones, including contacts, call data, text messages, stored files, location information, and more.[67] In some cases, officials go so far as to deprive migrants and refugees of their personal devices. One submission reported that "intercepted migrants are regularly stripped of their belongings by Croatian authorities[,] particularly passports and other forms of ID, cell phones and power banks[,] and are summarily expelled to Bosnia and Herzegovina."[68]

30. In Austria, Belgium, Denmark, Germany, Norway, and the United Kingdom (UK), laws allow for the seizure of mobile phones from asylum or migration applicants from which data are then extracted and used as part of asylum procedures.[69] These practices constitute a serious, disproportionate interference with migrants and refugees' right to privacy, on the basis of immigration status and, in effect, national origin. Furthermore, the presumption that data obtained from digital devices necessarily leads to reliable evidence is flawed.[70] Governments have also resorted to social media intelligence, the techniques and technologies that allow companies or governments to monitor social media networking sites.[71] Some of these activities are undertaken directly by government officials themselves but in some instances, governments call on companies to provide them with the tools and/or knowhow to undertake this surveillance.[72]

31. During the COVID-19 pandemic, the proliferation of contact-tracing apps has raised concerns that sharing information about areas with high concentrations of infections could reinforce the existing social stigmatization of disproportionately infected groups and communities, with a particular disparate impact on the basis of race, ethnicity, national origin and citizenship status. [73]

32. One submission detailed concerning practices regarding seizure of digital data in Germany.[74] Pursuant to the amended Asylum Act (Asylgesetz, "AsylG") § 15, asylum seekers unable to produce a valid passport or equivalent document must surrender all data carriers—not only mobile phones but also laptops, USB sticks, and even fitness wristbands—along with login information to be "read out" by BAMF to confirm identity or nationality.[75] The Law also empowers BAMF to share the data with other government agencies, such as security authorities and intelligence services.[76] If determined necessary, the readout takes place before the asylum hearing upon request by the Asylum Procedures Secretariat with the asylum applicant's signed consent,[77] although the submission notes that applicants are "under exceptional pressure to follow governmental requests" for fear of negative consequences that could result from their asylum procedure.[78] This routine practice affected more than half of all first-time asylum applicants in the past two years,[79] and certain nationalities more than others raising serious concerns of *de facto* national origin discrimination.

33. This invasive data extraction from personal devices is unprecedented, targets only asylum seekers, and the legalization of these measures was based on racist and xenophobic

67 Ibid.; Privacy International ("PI") et al., Submission.
68 Border Violence Monitoring Network ("BVMN"), Submission.
69 PI et al., Submission.
70 GFF, Submission.
71 PI et al., Submission.
72 Ibid.
73 https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/.
74 GFF, Submission.
75 Ibid.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid.

assumptions in political discourse.[80] The submission further highlights that data carrier evaluations have proven unsuitable to verify the identity or national origin of the asylum seeker with any degree of certainty, or to prevent abuse of asylum procedures.[81] Approximately a quarter of attempted readouts fail technically, and even if readouts are successful, most of the evaluation reports are unusable because the set of data reviewed is too small or otherwise inconclusive.[82] Among 21,505 mobile phones successfully read out in 2018 and 2019, only about 118 cases, or 0.55%, indicated a contradiction.[83] Furthermore, since neither the algorithms nor training data are known to the public, judges and other decision-makers cannot properly assess their reliability.[84]

34. Although regulations such as the European Union's General Data Protection Regulation ("GDPR") seek to protect data and privacy, some States create exemptions in the immigration enforcement context. Two submissions noted relevant GDPR exemptions in the UK Data Protection Act of 2018.[85] Under this "immigration exemption," an entity with the power to process data, known as a "data controller," may circumvent core rights of an individual around data access if to do otherwise would "prejudice effective immigration control."[86] These rights include the rights to object to and restrict the processing of one's data and the right to have one's personal data deleted.[87] The UK's amended Police Act empowers not only police but also immigration officers to interfere with mobile phones and other electronic devices belonging to asylum seekers.[88] Going far beyond even the data carrier evaluation permitted in Germany, the UK Crime and Courts Act of 2013 enables police and immigration officers to carry out secret surveillance measures, place bugging devices, and hack and search mobile phones and computers.[89] The individuals affected will disproportionately be targeted on national origin grounds when national origin should never be a basis for diminished privacy and other rights.

B. Discriminatory Structures

35. In her previous report, the Special Rapporteur showed how the design and use of different emerging digital technologies can produce racially discriminatory structures that undermine enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics. She urged that emerging digital technologies should be understood as capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms. In this sub-Section, the Special Rapporteur highlights ways in which migrants, refugees, stateless persons and related groups are being subjected to technological interventions that expose them to a broad range of actual and potential rights violations on the basis of actual or perceived national origin or immigration status.

1 Surveillance Humanitarianism and Surveillance Asylum

36. Commentators have cautioned of the rise of "surveillance humanitarianism"[90], whereby increased reliance on digital technologies in service provision and other bureaucratic processes perversely result in the exclusion of refugees and asylum seekers from essential basic necessities such as access to food.[91] Even a misspelled name can result in "bureaucratic chaos" and accusations of providing false information, slowing down what is

80 Ibid.
81 Ibid.
82 Ibid.
83 Ibid.
84 Ibid.
85 Ibid.; Platform for International Cooperation on Undocumented Migrants ("PICUM"), Submission.
86 PICUM, Submission.
87 Ibid.
88 GFF, Submission.
89 Ibid.
90 https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
91 Beduschi, Submission.

already a slow asylum process.[92] Potential harms around data privacy are often latent and violent in conflict zones, where data compromised or leaked to a warring faction could result in retribution for those perceived to be on the wrong side of the conflict.[93]

37. In this regard, one submission highlights the dangers associated with the growing use of digital technologies to manage aid distribution.[94] In refugee camps in Afghanistan, iris registration has reportedly been used as a pre-requisite for receiving assistance for returning Afghan refugees.[95] The impact of collecting, digitizing and storing the refugees' iris can be grave when systems are flawed or abused.[96] It has also been documented that such biometric surveillance tools have led to system aversion and loss of access to goods and services for survival.[97] This submission noted, for example, the failure of technology in Rohingya refugee camps in Bangladesh that resulted in the denial of food rations to refugees.[98] UNHCR reported to the Special Rapporteur that its policy is that safeguards should be in place to ensure that refugees can access assistance and protection services without the use of biometric technology, where necessary, and to address the risk of error or failure in its use.

38. Collection of vast amounts of data on migrants and refugees creates serious issues and possible human rights violations related to data sharing and access, particularly in settings such as refugee camps where there are stark power differentials between UN agencies, international NGOs and the affected communities. Although exchanging data on humanitarian crises or biometric identification is often presented as a way to increase efficiency and inter-agency and inter-state cooperation, benefits from the collection do not accrue equally. Data collection and the use of new technologies, particularly in contexts characterized by steep power differentials, raise issues of informed consent and the ability to opt out. In various forced migration and humanitarian aid settings, such as Mafraq, Jordan, biometric technologies are being used in the form of iris scanning in lieu of identity cards in exchange for food rations.[99] However, conditioning food access on data collection removes any semblance of choice or autonomy on the part of refugees—consent cannot freely be given where the alternative is starvation. Indeed, an investigation in the Azraq refugee camp[100] revealed that most refugees interviewed were uncomfortable with such technological experiments but felt that they could not refuse if they wanted to eat. The goal or promise of improved service delivery cannot justify the levels of implicit coercion underlying regimes such as these.[101]

39. Consultations highlighted concerns among Rohingya refugees in Bangladesh and India that their data may be shared in ways that increase their risk of *refoulement*, or shared with the government of Myanmar, increasing their vulnerability to human rights violations in the event of forcible and other forms of return of these groups to their country of origin. A serious concern in this context is that of "function creep" where data collected in one context (e.g. monitoring low level fraud) is shared and reused for different purposes (e.g. to populate registries of potential terror suspects),[102] with no procedural and substantive protections for the individuals whose data are being shared and repurposed. According to UNHCR, it did not collect information that could amount to consent voluntarily to

92 Mark Latonero et al., Digital Identity in the Migration & Refugee Context: Italy Case Study (April 2019).

93 https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

94 Amnesty International, Submission.

95 Ibid.

96 Ibid. citing A/HRC/39/29.

97 Amnesty International, Submission.

98 Ibid.

99 See Fleur Johns, "Data, Detection, and the Redistribution of the Sensible in International Law" (2017). See also https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b.

100 http://www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

101 See https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf; https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

102 Mirca Madianou, Submission.

repatriate, and it secured consent from refugees to share their data with the Government of Myanmar in order to verify their right of return.

40. In some cases, the very nature of data collection can produce profoundly discriminatory outcomes. Fleeing genocide in Myanmar, more than 742,000 stateless Rohingya refugees crossed over to Bangladesh since August 2017.[103] The UNHCR and Bangladeshi government registration system did not offer "Rohingya" as an ethnic identity option, instead using "Myanmar nationals," a term that Myanmar does not recognize, and which does not capture the reality that Rohingya are stateless due to having been arbitrarily deprived of their right to Myanmar nationality.[104] As one submission notes, categorization using this unrecognizable term on their digital identity cards amounts to a form of "symbolic annihilation of the Rohingya" required to carry and use these cards.[105] UNHCR reported that Rohingya refugees accepted this approach and were consulted in its adoption.

41. Exclusion of refugees and asylum seekers from essential basic services through digital technology systems also occurs outside of refugee camp settings. One submission provides an example from Germany. Under the German Asylum Seekers Benefit Act, undocumented persons have the same right to health care as asylum seekers.[106] However, the social welfare office that administers health care for the undocumented has a duty to report their personal data to immigration authorities under section 87 of the Residence Act, which governs the "transfer of data and information for foreign authorities" by all public authorities.[107] This means legally accessing healthcare may result in immigration enforcement, which likely has a chilling effect on migrant and refugees' use of even emergency healthcare.

2 Technological Experimentation

42. Submissions raise serious concerns with the widespread technological experimentation conducted by state and non-state actors on refugees, migrants, and stateless persons. This experimentation involves testing of various technological products under circumstances where targeted groups have limited or no means of providing informed consent, and where the human rights consequences of the testing and experimentation are negative or unknown. Typically, refugees, migrants and stateless persons have no or very limited recourse for challenging this technological experimentation and the human rights violations that may be associated with it. Furthermore, it is national origin and citizenship/immigration status that exposes refugees, migrants and stateless persons to this experimentation, raising serious concerns about discriminatory structures of vulnerability.

43. One submission called attention to the EU's Horizon 2020's iBorderCtrl, an "Intelligent Portable Control System" that "aims to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States"[108] iBorderCtrl uses hardware and software technologies that seek to automate border surveillance.[109] Among its features, the system undertakes automated deception detection.[110] The EU has piloted this lie detector at airports in Greece, Hungary and Latvia.[111] Reportedly, in 2019 iBorderCtrl was tested at the Serbian-Hungarian border and failed.[112] iBorderCtrl exemplifies the trend of experimenting surveillance and other technologies on asylum seekers based on scientifically dubious grounds.[113] Drawing upon the contested theory of "affect recognition science," iBorderCtrl replaces human border guards with a facial recognition system that scans for facial anomalies while travellers answer a series of questions.[114] Other countries

103 https://www.unhcr.org/en-us/rohingya-emergency.html.

104 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises" (2019).

105 Madianou, Submission.

106 PICUM, Submission.

107 Ibid.

108 PI et al., Submission.

109 See https://www.iborderctrl.eu/The-project.

110 PI et al., Submission.

111 Maat for Peace, Development & Human Rights ("Maat for Peace"), Submission. See also Petra Molnar, "Technology at the Margins: The Human Rights Impacts of AI in Migration Management" (2019); MRG, Submission.

112 PI et al., Submission.

113 Ibid.

114 MRG, Submission.

such as New Zealand are also experimenting with using automated facial recognition technology to identify so-called future "troublemakers," which has prompted civil society organizations to mount legal challenges on grounds of discrimination and racial profiling.[115] Canada and Romania have also experimented with similar "emotion-recognition" projects for border screening.[116]

44. States are currently experimenting with automating various facets of immigration and asylum decision making. For example, since at least 2014, Canada has used some form of automated decision-making in its immigration and refugee system.[117] A 2018 University of Toronto report examined the human rights risks of using AI to replace or augment immigration decisions, noting that these processes "create a laboratory for high-risk experiments within an already highly discretionary and opaque system."[118] The ramifications of using automated decision making in the immigration and refugee context are far-reaching. Although the Canadian government has confirmed that this type of technology is confined only to augmenting human decision-making and reserved for certain immigration applications only, there is no legal mechanism in place protecting non-citizen's procedural rights and preventing human rights abuses from occurring. Similar visa algorithms are currently in use in the UK and have been challenged in court for their discriminatory potential.[119] Canada, Switzerland and the UK also use automated or algorithmic decision-making "for selecting refugees and resettling them."[120] The introduction of new technologies impacts both the processes and outcomes associated with decisions that would otherwise be made by administrative tribunals, immigration officers, border agents, legal analysts, and other officials responsible for the administration of immigration and refugee systems, border enforcement, and refugee response management. There is a serious lack of clarity surrounding how courts will interpret administrative law principles like natural justice, procedural fairness, and standard of review where an automated decision system is concerned or where an opaque use of technology operates.

45. In some contexts, the nature of technological experimentation relates to the genetic data collection, whose purposes are justified on tenuous grounds. One submission described the Combined DNA Index System ("CODIS"), a forensic DNA database in the US through which individual states and the federal government collect, store and share genetic information.[121] Since January 2020, the federal government has been collecting DNA from any person in immigration custody.[122] This means that "for the first time, CODIS will warehouse the genetic data of people who have not been accused of any crime, for crime detection purposes," severing the longstanding prerequisite of prior alleged criminal conduct to compel DNA collection.[123] Non-citizens in immigration custody are not criminals as a rule.[124] In fact, the vast majority of immigration infractions for which an immigrant is detained are civil in nature.[125] In the case of asylum seekers, who form an increasingly large proportion of the detained non-citizen population, both international and domestic laws expressly allow them to enter the U.S. to claim the right to refuge.[126] The submission rightly highlights that the new immigration policy risks turning CODIS into a "genetic panopticon" that will "encompass anyone within [US] borders, including ordinary Americans neither convicted nor even suspected of criminal conduct," threatening democracy and human rights.[127]

115 https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.

116 https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

117 Petra Molnar & Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System" (2018).

118 Molnar & Gill.

119 Joint Council for the Welfare of Immigrants v. Secretary of State for the Home Department CO/2057/2020.

120 Maat for Peace, Submission; Beduschi, Submission citing Molnar & Gill.

121 Daniel I. Morales, Natalie Ram & Jessica L. Roberts, Submission.

122 Ibid.

123 Ibid.

124 Ibid.

125 Ibid.

126 Ibid.

127 Ibid.

46. As COVID-19 has further incentivized and legitimized surveillance and other technologies targeting refugees and migrants, these groups have been subjected to further experimentation.[128] One example is the experimental deployment of an immunity passport called "COVI-Pass" in Western Africa.[129] A partnership between Mastercard and GAVI Vaccine Alliance, this digital initiative combines biometrics, contact tracing, cashless payments, national identification and law enforcement.[130] Not only do such technologies operate outside human rights impact assessments and regulations, they also risk threatening human rights, including freedom of movement, the right to privacy, the right to bodily autonomy and the right to equality and non-discrimination, especially for refugees and migrants.[131]

47. In the UK, contact tracing apps and other data-collection technologies to combat COVID-19 have raised concerns that "mission-creep" could eventually lead to the systems being used for immigration enforcement. Fears that gathered data could be used for such purposes may undermine trust in contact-tracing technologies among immigrant communities, leading to their exclusion from effective health policies.[132] The US recently announced a new app named "CBP One" which uses facial recognition, GPS technology, and cloud storage to collect data on asylum seekers before they enter the US.[133] This technology raises serious privacy and non-discrimination concerns.[134]

48. States and international organizations,[135] have promoted the creation of "immunity" or "health" passports that would condition international travel and mobility on vaccination status. However, because of the unequal distribution of access to vaccines, such requirements will further exacerbate inequality in immigration and mobility opportunities. As vaccines become available, States and international organizations are turning to new technologies to facilitate the mobility of the vaccinated.[136] Organizations such as the WHO, International Air Travel Association, the WEF, and Gavi Vaccine Alliance are actively developing digital systems which can track vaccination data and facilitate travel. Private tech companies are also working to provide seamless digital access to vaccination records.[137] A report by the IOM and Migration Policy Institute has called for these efforts to be particularly sensitive to pre-existing inequalities which are worsened by digitization, including impacts on "those in vulnerable situations or unable to access the relevant technology."[138]

3 Border externalization

49. Border externalization—the extra-territorialization of national and regional borders to other geographic regions in order to prevent migrant and refugee arrivals—has become a standard border enforcement tool for many countries and regions. The human rights violations associated with border externalization are well documented.[139] Border externalization does not affect all nationality or national origin groups equally. It has a disproportionate impact on persons from Africa, Central and South America and South Asia, and in many regions is fuelled by racialized, xenophobic and ethnonationalist politics that seek to exclude certain national and ethnic groups from regions on discriminatory bases. States and regional blocs have increasingly relied on digital technologies to achieve

128 Amnesty International, Submission.
129 Ibid.
130 Ibid.
131 Ibid.
132 https://www.openrightsgroup.org/blog/contact-tracing-apps-vulnerable-migrants-key-concerns/.
133 https://www.latimes.com/politics/story/2021-06-04/asylum-bidens-got-an-app-for-that-with-privacy-risks-and-surveillance-beyond-border.
134 https://www.americanimmigrationcouncil.org/FOIA/investigating-cbp%E2%80%99s-use-mobile-application-cbp-one.
135 International Organization for Migration & Migration Policy Institute, "Covid-19 and the State of Global Mobility in 2020" (2021), p. 51.
136 Ibid., pp. 51-2.
137 Ibid.
138 Ibid., p. 52.
139 See, e.g., A/HRC/23/46, A/HRC/29/36 and A/72/335.

this border externalization, thereby consolidating and expanding discriminatory, exclusionary regimes.

50. One submission highlighted the European Border Surveillance system ("EUROSUR") as a program that uses big data technologies "to predict, control and monitor traffic across European Union borders."[140] It deploys surveillance drones in the Mediterranean Sea, in order to notify the Libyan coastguard to intercept refugee and migrant boats and return migrants to Libya.[141] Although the European Commission insists the drones are only for civil surveillance purposes,[142] the UN Office of the High Commissioner for Human Rights ("OHCHR") has spoken out against coordinated pushbacks and failures to assist migrants and refugees in the Mediterranean, one of the deadliest migration routes in the world.[143]

51. Another submission reported the participation of thirteen European nations in the ROBORDER project, a "fully functional, autonomous border surveillance system, consisting of unpiloted mobile robots capable of functioning on a standalone basis or in swarms, in a range of environments—aerial, water surface, underwater, and ground.[144] This proposed increased use of drones to police Europe's borders exacerbates the decentralization of the border zone into various vertical and horizontal layers of surveillance, turning people into security objects and data points to be analysed, stored, collected, and rendered intelligible.[145] The usage of military, or quasi-military, autonomous technology also bolsters the connection between immigration, national security, and the increasing criminalization of migration and use of risk-based taxonomies to flag cases.[146] Globally, States have been using various ways to pre-empt and deter those seeking to legally apply for asylum. This type of deterrence policy is very evident in Greece, Italy, and Spain,[147] countries which are on the geographic frontiers of Europe, and which increasingly rely on violent deterrence and 'push back' policies.

52. One submission highlighted Croatia's uses of EU-funded technologies to detect, apprehend and return refugees and migrants along the Balkan route, traveling from Bosnia and Herzegovina and Serbia through Croatia to reach the Schengen border.[148] This submission alleges hundreds of human rights abuses in the past three years, including "illegal push-backs" that reflect "inherently racist cleavages."[149] Surveillance technologies such as drones and helicopters with automated searchlights "have been weaponised against people on the move, making them easier to detect and thus compounding their vulnerability and the dangers they face."[150]

53. Discriminatory border externalization is also achieved through transnational biometric data-sharing programs. One submission reported a biometric data sharing program between the governments of Mexico and the U.S.[151] As of August 2018, Mexico had deployed the U.S.-funded program in all fifty-two migration processing stations.[152] This bilateral program uses biometric data to screen detained migrants in Mexico who allegedly had tried to cross the U.S. border or are members of a criminal gang.[153] However, Mexico's National

140 Maat for Peace, Submission citing Btihaj Ajana, "Augmented borders: Big Data and the ethics of immigration control" (2015).

141 Franciscans International, Submission citing https://www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/.

142 Franciscans International, Submission citing https://www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.

143 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25875&LangID=E.

144 Homo Digitalis, Submission. See also https://roborder.eu/..

145 Csernatoni.

146 See Van Den Meerssche, Submission.

147 https://www.statewatch.org/news/2017/november/eu-spain-new-report-provides-an-x-ray-of-the-public-funding-and-private-companies-in-spain-s-migration-control-industry/; https://www.efadrones.org/countries/italy/.

148 BVMN, Submission.

149 Ibid.

150 Ibid.

151 PI et al., Submission.

152 Ibid.

153 Ibid.

Institute of Migration has denied processing biometric data in answers to freedom of access to information requests.[154]

4 Immigration Surveillance[155]

54. One submission reported the ongoing construction at the US-Mexico border of "a network of fifty-five towers equipped with cameras, heat sensors, motion sensors, radar systems, and a GPS system."[156] This border enforcement system also surveils the Tohono O'odham Nation's reservation, located in Arizona approximately one mile from the border.[157] This "smart" border surveillance system has shifted the routes used by migrants, thereby "increasing [their] vulnerability to injury, isolation, dehydration, hyperthermia and exhaustion"—and deaths.[158] Another submission notes that researchers and civil society organizations have opposed these border technologies because "they would exacerbate racial and ethnic inequality in policing and immigration enforcement, as well as curbing freedom of expression and the right to privacy."[159] Other submissions also highlighted the operation of other autonomous surveillance AI infrastructure at the US-Mexico border, including drones designed to detect human presence and alert border enforcement officials.[160] As mentioned above, the current evidence is that so-called "smart" border technology forces ever more precarious journeys[161], with a disproportionate impact on certain national origin, ethnic and racial groups.

55. In the US, the communications of detained immigrants and their families and friends are surveilled.[162] Under business model of the corporate providers of the technology, detained immigrant and their families "get convenience in the form of calls, video chats, voice mail messages, photo sharing and text messaging, while [the company's] real clients," immigration officials, get user data.[163] The web-based surveillance software offers government officials free "call-pattern analysis, relationship analysis and tools for data visualization."[164]

56. Yet another facet of immigration surveillance involves social media screening. As of April 2019, the US State Department requires visa applicants to disclose their social media account information in the past five years from the time of application.[165] As the submission highlights, this expansive approach to social media screening is especially troubling because of the US immigration enforcement's demonstrated track record of utilizing social media information in a manner that disproportionately harms members of minority racial, ethnic, and religious groups.[166] DHS has already falsely accused Black and Latinx youth of gang membership by exploiting social media connections, resulting in their detention, deportation, and/or denial of immigration benefits.[167] Immigration and Customs Enforcement ("ICE"), a constituent agency of DHS, frequently combs social media to support gang membership allegations.[168] In one case, DHS evidenced its allegation with a Facebook photo of an immigrant youth wearing a Chicago Bulls hat. The immigration court denied him bond and rejected both his applications for asylum and permanent residence,

154 Ibid.

155 Anil Kalhan, "Immigration Surveillance," (2014) (defining immigration surveillance as the product of dramatically expanded identification, mobility tracking and control, and information sharing, and evasion of the traditional substantive and procedural legal protections that have typically been relied upon to protect non-citizens from a host of human rights abuses).

156 Campaign to Stop Killer Robots, Submission.

157 Ibid.

158 Samuel Norton Chambers et al.

159 MRG, Submission.

160 Mijente, Submission; Iván Chaar-López, Submission.

161 Franciscans International, Submission.

162 Mijente, Submission citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.htm.

163 Ibid.

164 Ibid.

165 Harvard Immigration & Refugee Clinical Program ("HIRC"), Submission.

166 HIRC, Submission.

167 Ibid., citing https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.

168 HIRC, Submission.

deporting him to a country where he feared for his life,[169] in violation of non-refoulement prohibitions under international law.

57. Moreover, social media screening has compounded the disproportionate risk of people belonging to or presumed to be of Muslim faith or Arab descent "by creating an infrastructure rife with mistaken inference and guilt-by-association."[170] For example, Customs and Border Protection, another constituent agency of DHS, denied a Palestinian college student entry to the country based on his friends' Facebook posts expressing political views against the U.S., even though he did not post such views of his own.[171] In addition to the direct burdens they place on non-citizens, the U.S. government's expanded social media disclosure requirements foreseeably affect freedoms of speech and association.

58. Homeland Security Investigations ("HSI"), ICE's investigative arm, had already been testing automated social media profiling as early as 2016,[172] strengthening its open source social media exploitation capabilities for the purposes of scrutinizing visa applicants and visa holders before and after they arrive in the U.S.[173] Submissions also raised concerns about the US government's consideration of technologies whose goal was "determinations via automation" regarding whether an individual applying for or holding a US visa was likely to become a "positively contributing member of society" or intended "to commit criminal or terrorist attacks."[174] One submission noted in particular the use in the US of risk assessments tools in immigration detention decisions, including one using an algorithm set to always recommend immigration detention, regardless of an individual's criminal history.[175]

59. All this points to a trend in immigration surveillance, where predictive models use artificial intelligence to forecast whether people with no ties to criminal activity will nonetheless commit crimes in the future. Yet these predictive models are prone to creating and reproducing racially discriminatory feedback loops.[176] Furthermore, racial bias is already present in the datasets on which these models rely.[177] When discriminatory datasets are treated as neutral inputs, they lead to inaccurate models of criminality which then "perpetuate racial inequality and contribute to the targeting and over-policing of non-citizens."[178]

60. The response to the COVID-19 pandemic has led to the rapid increase in "bio-surveillance"—the monitoring of an entire population's health and behaviour on an unprecedented scale, facilitated by emerging digital technologies.[179] As States increasingly move toward a bio-surveillance system to combat the pandemic, there has been an increase in the use of digital tracking, automated drones, and other technologies "purporting to help manage migration and stop the spread of the virus."[180] There is an outsize risk that these technologies will enable further discrimination on the basis of race, ethnicity and citizenship status.[181]

169 Ibid.
170 Ibid.
171 Ibid.
172 Mijente, Submission citing Sarah Lamdan, "When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing" (2019).
173 Mijente, Submission citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
174 Ibid.
175 MRG, Submission.
176 Mijente, Submission.
177 Ibid.
178 Ibid.
179 https://www.newstatesman.com/science-tech/2020/03/rise-bio-surveillance-state.
180 https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.
181 Ibid.

IV. Recommendations

61. **The Special Rapporteur recalls her previous report to the Human Rights Council and reminds Members States of the applicable international human rights obligations, in particular:**

(a) **The scope of legally prohibited racial discrimination in the design and use of emerging digital technologies;**

(b) Obligations to prevent and combat racial discrimination in the design and use of emerging digital technologies; and

(c) **(Obligations to provide effective remedies for racial discrimination in the design and use of emerging digital technologies.**

62. **The Special Rapporteur reiterates the analysis and recommendations in her previous report regarding the obligations of States and non-State actors and urges States to consider them alongside the recommendations included herein. In the specific context of border and immigration enforcement, she recommends that Member States:**

63. **Address the racist and xenophobic ideologies and structures that have increasingly shaped border and immigration enforcement and administration. The effects of technology are in significant part a product of the underlying social, political and economic forces driving the design and use of technology. Without a fundamental shift away from racist, xenophobic, anti-migrant, anti-stateless and anti-refugee political approaches to border governance, the discriminatory effects of digital borders highlighted in this report cannot be redressed. States must comply with international human rights obligation to prevent racial discrimination in border and immigration enforcement and implement the recommendations provided in report A/HRC/44/57. States should also follow the guidance provided by interventions such as the Principles on Deprivation of Nationality as a National Security Measure,[182] and the Principles of Protection for Migrants, Refugees, and Displaced People During COVID-19[183] which articulate existing State obligations, including with respect to equality and non-discrimination, to ensure the human rights of migrants, refugees, stateless persons and related groups.**

64. **Adopt and strengthen human rights-based racial equality and non-discrimination legal and policy approaches to the use of digital technologies in border and immigration enforcement and administration. There currently exists no integrated regulatory global governance framework for the use of automated and other digital technologies, which only raises the importance of existing international human rights legal obligations in the regulation of the design and use of these technologies.**

65. **Pursue the action steps prescribed by General Recommendation No. 36 of the Committee on the Elimination of Racial Discrimination on preventing and combatting racial profiling by law enforcement officials, particularly those recommendations for comporting the use of artificial intelligence with international human rights law.**

66. **Ensure, both at the domestic and international levels, that border and immigration enforcement and administration are subject to binding legal obligations to prevent, combat and remedy racial and xenophobic discrimination in the design and use of digital border technologies. These obligations include but are not limited to:**

(a) Swift and effective action to prevent and mitigate the risk of the racially discriminatory use and design of digital border technologies, including by making racial equality and non-discrimination human rights impact assessments a prerequisite for the public deployment of systems. These impact assessments must

[182] Institute on Statelessness and Inclusion et al.

[183] Zolberg Institute on Migration and Mobility et al., “Principles of Protection for Migrants, Refugees, and Displaced People During COVID-19,” (2020).

incorporate meaningful opportunity for co-design and co-implementation with representatives of racially or ethnically marginalized groups, including refugees, migrants, stateless persons and related groups. A purely or even mainly voluntary approach to equality impact assessments will not suffice; a mandatory approach is essential;

(b) An immediate moratorium on the procurement, sale, transfer and use of surveillance technology, until robust human rights safeguards are in place to regulate such practices. These safeguards include human rights due diligence that complies with international human rights law prohibitions on racial discrimination, independent oversight, strict privacy and data protection laws, and full transparency about the use of surveillance tools such as image recordings and facial recognition technology. In some cases, it will be necessary to impose outright bans on technology that cannot meet the standards enshrined in international human rights legal frameworks prohibiting racial discrimination;

(c) Ensuring transparency and accountability for private and public sector use of digital border technologies, and enabling independent analysis and oversight, including by only using systems that are auditable;

(d) Imposing legal obligations on private corporations to prevent, combat and remedy racial and xenophobic discrimination due to digital border technologies;

(e) Ensuring that public-private partnerships in the provision and use of digital border technologies are transparent and subject to independent human rights oversight, and do not result in abdication of government accountability for human rights.

67. **The Special Rapporteur had the opportunity to consult with representatives of UNHCR and IOM on their use of different digital border technologies. Based on those consultations, she recommends that both bodies adopt and implement mechanisms for sustained and meaningful participation and decision-making of migrants, refugees and stateless persons in the adoption, use and review of digital border technologies. She further recommends:**

<u>IOM:</u>

(a) Mainstream and strengthen international human rights obligations and principles, especially relating to equality and non-discrimination in its use and oversight of digital border technologies, including in all its partnerships with private and public entities. This requires moving beyond a narrow focus on privacy concerns relating to data sharing and data protection, and mandating rather than recommending equality and non-discrimination protections;

(b) Adopt mandatory policies and practices for systemic analysis of potential harmful and discriminatory impacts of digital border technologies prior to the adoption of these technologies, and prohibit adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. Provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies, and ensure the implementation of these guidelines;

(c) Adopt mandatory ongoing human rights assessment protocols for digital border technologies once deployed;

<u>UNHCR:</u>

68. **Relative to IOM, UNHCR has taken greater steps to engage with equality and non-discrimination norms in its guidance frameworks relating to digital border technologies, but it too has significant additional work to do to ensure that those norms are realized in its practice. In this regard, the Special Rapporteur recommends that UNHCR:**

(a) Ensure the effective implementation of its policies and practices for systemic analysis of potential harmful and discriminatory impacts of digital border

technologies prior to the adoption of these technologies, and prohibit adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. Provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies, and ensure the implementation of these guidelines;

(b) Ensure the use and implementation of mandatory ongoing human rights assessment protocols for digital border technologies once deployed;

69. **The Special Rapporteur recommends that IOM and UNHCR:**

(a) Create mechanisms for independent human rights oversight of their use of digital border technologies and implement reforms to ensure greater transparency in how decisions are made to adopt these technologies;

(b) Provide migrants, refugees, stateless persons and related groups with mechanisms for holding them directly accountable for violations of their human rights resulting from the use of digital border technologies.

<u>All UN Humanitarian and Related Bodies:</u>

Implement the recommendations above addressed to IOM and UNHCR.