Advance Unedited Version

Distr.: General
10 November 2020

Original: English

Seventy-fifth session
Item 70 (b) of the provisional agenda*
Elimination of racism, racial discrimination, xenophobia and related intolerance: comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action

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

Note by the Secretary-General

The Secretariat has the honour to transmit to the General Assembly the report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, prepared pursuant to General Assembly resolution 74/137.

Summary

Governments and UN agencies are developing and using emerging digital technologies in ways that are uniquely experimental, dangerous, and discriminatory 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 them on exploitative terms that strip these groups of fundamental human agency and dignity. This report highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have become so prevalent, in part due to widespread perceptions of refugees and migrants as *per se* threats to national security. In other 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.

* A/75/150.

** The present report is submitted late owing to circumstances beyond the Special Rapporteur's control.

Contents

I. Introduction

1. This report continues the analysis initiated by the Special Rapporteur in her most recent report to the Human Rights Council: *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*.[1] In that report, the Special Rapporteur introduced an equality-based approach to human rights governance of emerging digital technologies, with a focus on racial discrimination resulting from the design and use of these technologies. 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. That report focused on those subject to discrimination primarily on the basis of race and ethnicity (including Indigeneity), and drew attention to the effects of gender, religion, and disability status. This report to the General Assembly 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 nomadic and other peoples for whom migratory traditions are central. The term "refugees" includes asylum seekers who meet the refugee definition but whose status as refugees has not yet been formally recognized by any state.

2. 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 the targets of 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 typical substantive and procedural constraints, constitutionally and otherwise guaranteed to citizens.

3. As this report highlights, governments and non-state actors are developing and deploying emerging digital technologies in ways that are uniquely experimental, dangerous, and discriminatory 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 them on exploitative terms that strip these groups of fundamental human agency and dignity. Although the focus of this report is relatively recent technological innovations, many of these technologies have historical antecedents in colonial technologies of racialized governance, including through migration controls. 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.[2] This report highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have become so prevalent, in part due to widespread perceptions of refugees and migrants as *per se* threats to national security. In other 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 highlights how ongoing securitization of borders, and related massive economic profits are a significant part of the problem.

4. Refugees, migrants and stateless persons are subject to the violations enumerated in this report on account of their national origin, race, ethnicity, and 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

[1] A/HRC/44/57.
[2] See, e.g., A/73/312.

status, in which she highlights discriminatory trends and the application of international human rights law where such violations are concerned.[3]

5. Many of the same factors highlighted in the Special Rapporteur's Human Rights Council report are essential background for this report, and she recommends that the present report be read in conjunction with that prior report. Her prior report is especially helpful, among other reasons, 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 of the 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 (as in other contexts), preventing human rights violations may require outright bans or abolition of technologies due to a failure to control or mitigate their effects.

6. In the preparation of the report, the Special Rapporteur benefited from 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 will be available on the webpage of the mandate.

II. The Rise of Digital Borders

7. 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. The specific focus of this report is the growing prevalence of *digital* technologies in immigration and border enforcement, such that some commentators appropriately refer to the rise of "digital borders"[4]—which in this report refers to borders whose infrastructure and processes increasingly rely on machine learning, automated algorithmic decision-making systems, predictive analytics and related digital technologies. These technologies are integrated into identification documents, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases, asylum decision-making processes and many other facets of border and immigration enforcement.

8. 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 and class, among others. Automated border controls are one example of these parallel border regimes in action. One submission offered the example of the introduction of "eGates" at Irish ports of entry, such as Dublin Airport, where e-passport holders from EU/EEA and Switzerland can go through eGates on a "self-service" basis to clear immigration control.[5] The submission notes that "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.

9. 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[.]"[6] Biometrics can include fingerprint data, retinal scans, and facial recognition, as well as less

[3] A/HRC/38/52.
[4] See, e.g., Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" (2007).
[5] Immigrant Council of Ireland, Submission.
[6] https://www.biometricsinstitute.org/what-is-biometrics/.

well-known methods such as the recognition of a person's vein and blood vessel patterns, ear shape, and gait, among others. Biometrics are used to establish, record and verify the identity of migrants and refugees. The UN, for example, has collected the biometric data of over 8 million people, most of them fleeing conflict or needing humanitarian assistance.[7] Researchers have documented the racialized origins of biometric technologies,[8] as well as their contemporary discriminatory operation on the basis of race, ethnicity and gender.[9] A recent report on facial recognition technology (FRT) deployed in border crossing contexts such as airports, notes that despite the fact that even the best algorithms misrecognizes Black women twenty more times than White men, the use of these technologies is increasing globally.[10] As that report notes, "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)." The frequent results of this differential treatment include perpetuation of negative stereotypes, and even prohibited discrimination that for asylum seekers might lead to *refoulement*.

10. Examples below show that 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.[11] Private corporations such as Palantir have proved essential in providing the technology that supports the detention and deportation programs run by the US Immigration and Customs Enforcement (ICE) and the Department of Homeland Security (DHS),[12] 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.[13] Data collection is not an apolitical exercise, especially when powerful Global North actors collect information on vulnerable populations with no regulated methods of oversights and accountability.[14] The increasingly fervent collection of data on migrant populations has been criticized for its potential to cause significant privacy breaches and human rights concerns.[15]

11. 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.[16] Other genocides also relied on systematic tracking of groups, such as the Tutsi registries based on ethnicity identity cards, which facilitated the magnitude of the Rwandan genocide in 1994.[17] Post 9-11, the US experimented with various modes of data collection on marginalized populations through the Department of Homeland Security's National Security-Entry Exit Registration System (NSEERS), which collected photographs, biometrics, and even first-person interview data from over 84,000 flagged individuals coming

[7] 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/.

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

[9] A/HRC/44/57.

[10] Tamir Israel, FACIAL RECOGNITION AT A CROSSROADS: TRANSFORMATION AT OUR BORDERS & BEYOND (2020).

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

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

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

[14] Dragana Kaurin, DATA PROTECTION AND DIGITAL AGENCY FOR REFUGEES, (2019).

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

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

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

from mostly Arab states. [18] In all of these cases, different actors, including governments, exploited ideas about the neutrality or non-prejudicial necessity of data collection from marginalized groups to then target these groups on a discriminatory basis.

12. Autonomous technologies are also increasingly used in monitoring and securing border spaces. For example, FRONTEX, the European Border and Coast Guard Agency, has been testing various unpiloted military-grade drones in the Mediterranean and Aegean for the surveillance and interdiction of vessels of migrants and refugees hoping to reach European shores.[19] A joint 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,[20] 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. One submission highlighted legal developments in Greece that permit the police to use drone surveillance to monitor irregular migration in border regions, but that do so without ensuring the requisite legal protections for the human rights of those subject to this surveillance. [21]

13. The usage of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security, and the increasing push towards the criminalization of migration and using risk-based taxonomies to demarcate and flag cases.[22] States, particularly those on the frontiers of large numbers of refugee and migrant arrivals, have been using various ways 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.[23] 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, for example, have actually increased migrant deaths and pushed migration routes towards more dangerous terrains through the Arizona desert.[24] Chambers et al have found that migrant deaths have more than doubled since these new technologies have been introduced,[25] creating a "land of open graves."[26]

14. The use of these technologies by border enforcement is only likely to increase in the 'militarised technological regime'[27] of border spaces, without appropriate public consultation, accountability frameworks, and oversights mechanisms. One submission provided an example of the Korean peninsula's Demilitarized Zone ("DMZ") where "South Korea (Republic of Korea) has deployed stationary, remote-operated semi-autonomous weapons[.]"[28] The South Korean government stated that it has no intent to develop or acquire lethal autonomous weapons systems.[29] Due to a lack of transparency, often the status of autonomous weapons systems' deployment on borders is difficult to determine. In anticipation of such systems underway it is crucial that States account for and combat the

[18] http://www.aaiusa.org/nseers.

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

[20] 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.

[21] Homo Digitalis, Submission.

[22] See Dimitri Van Den Meerssche, Submission.

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

[24] 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).

[25] Ibid.

[26] Jason De León, *The Land of Open Graves: Living and Dying on the Migrant Trail* (2015).

[27] Csernatoni.

[28] Campaign to Stop Killer Robots, Submission.

[29] Ibid.

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.

15. UN 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[30] 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 United States, Big Data analytics are also being used to predict likely successful outcomes of resettled refugees based on pre-existing community links.[31] 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[32] or the galvanization of anti-migrant sentiments in the Mediterranean, including the recently proposed floating barrier walls.[33] Societal fear is then used to justify increasingly hard-line responses that contravene international human rights law.[34] 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."[35]

16. 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"[36] 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.[37] Trends that fuel the border industrial complex include the externalization, militarization and automation of borders.[38] In the U.S., the budget for border and immigration enforcement has increased by more than 6,000 % since 1980.[39] 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.[40] Recent market research reports project the compound annual growth rate for this global border security market between to be between 7.2 and 8.6 % (65 to 68 million US dollars) in 2025.[41]

17. Among the emerging digital technologies that drive the border industrial complex, drones that service border monitoring and biometrics that help build "smart borders"[42] 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

[30] https://dtm.iom.int/about.
[31] https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/.
[32] See New York University School of Law Center on Race, Inequality, and the Law, Submission.
[33] https://www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.
[34] See also Ana Beduschi, "International Migration Management in the Age of Artificial Intelligence" (2020); Ana Beduschi, Submission.
[35] Minority Rights Group International ("MRG"), Submission.
[36] https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.
[37] Dhakshayini Sooriyakumaran & Brami Jegan, Submission.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] 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).
[42] Sooriyakumaran & Jegan, Submission.

largest arms sellers in the world.[43] Information technology companies such as IBM are also major players, including in data gathering and processing roles.[44] Many of these corporate actors exert great influence in domestic and international decision-making related to the governance of the digital border industry.[45] The "revolving door" between public office and private companies further tightens and blurs the line between government (border control, military) and industry (security and consulting companies).[46] Corporations are also linked with governments through joint ventures. According to one submission, for example, in 2016, French public-private company Civipol set up fingerprint databases for Mali and Senegal.[47] 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.[48] France owns 40% of Civipol, while arms producers Airbus, Safran and Thales each own more than 10% of the shares.[49] This further illustrates the manner in which Global North countries use international aid to advance their border agendas in the Global South.

18. One researcher has highlighted the pressing concern of the rise of "technolonialism," 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"[50] 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.

19. In short, many digital border technologies substitute 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 below highlights the range of discriminatory human rights violations enabled by digital border machinery and infrastructure, calling attention to these expansions of power and contraction of constraints.

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

A. Direct and indirect discrimination

i. Online Platforms

20. Consultations with migrants, refugees and stateless persons highlighted the use of social media platforms such as Facebook, Twitter and Whatsapp to spread racist and xenophobic hatred, and some reported being targeted directly through personal messages on these platforms. Participants in Malaysia, for example, reported the rise of racist and xenophobic advocacy on social media platforms in the wake of 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.

[43] Ibid.
[44] Ibid.
[45] Ibid., citing https://www.escr-net.org/corporateaccountability/corporatecapture.
[46] Sooriyakumaran & Jegan, Submission.
[47] Ibid.
[48] Ibid., citing https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/eutf_2016_annual_report_final_en.pdf.
[49] Sooriyakumaran & Jegan, Submission.
[50] Mirca Madianou "Technocolonialism: digital innovation and data practices in the humanitarian response to the refugee crisis" (2019).

21. One submission called attention to an anonymously-run blacklisting website, Canary Mission, that prejudicially targets students, professors and activists who have publicly advocated for Palestinian rights and disproportionately targeting people of Arab descent. According to the submission, 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.[51] 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.

ii. Racial Profiling

22. Consultations with migrants, refugees and stateless persons also highlighted the role of digital technologies in racial and ethnic profiling in border enforcement. 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.[52] 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 challenging their presence on these lists.

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

23. States are increasingly mandating extensive biometric data collection from non-citizens, where 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 even religion. As mentioned above, in most cases, refugees, migrants and stateless persons have no control over how the data collected from them are shared. According to one submission, India requires mandatory biometric data collection from non-citizens with a primary use of this data being detention and deportation even for refugees such as Rohingya.[53] Another concern raised in the context of India, is the use of Aadhaar as de facto exclusion from vital basic services which rely on automated systems from which non-citizens are excluded entirely.[54] 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."[55] According to this submission, even refugee children have been denied primary education based on not having Aadhaar.[56]

24. 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 same key considerations that must flow into every nationality deprivation decision, including non-discrimination, avoidance of statelessness, prohibition of arbitrariness, proportionality, necessity and legality,[57] must also be present when considering the introduction of centralized biometric ID systems. The introduction of digital governance structures risks deprivation of nationality by proxy measures, without due process – both intentionally and

[51] Palestine Legal, Submission.

[52] 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.

[53] Anubhav Dutt Tiwari & Jessica Field, Submission.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] 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.

as a result of incomplete or flawed civil registration systems.[58] During consultations participants from Kenyan Nubian and Somali communities, and Rohingya communities, for example, reported systematic difficulties securing digital identification, which then threatened their ability to formal employment and other basic needs. In some cases, digital identification regimes seemed to exacerbate statelessness by resulting in complete exclusion and non-recognition of ethnic minority groups.

iv. Language Recognition

25. Although automated registration systems may be adopted for the purpose of enhancing 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"[59] uses TraLitA, an automatic transliteration program, to register Arabic names into the Latin alphabet. 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,[60] and the submission raises the serious concern 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."[61] 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.

v. Mobile Data Extraction and Social Media Intelligence on Migrant and Refugee Populations

26. Governments are increasingly targeting the electronic devices of migrants and refugees as means 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.[62] 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."[63]

27. In Austria, Belgium, Denmark, Germany, Norway, and the United Kingdom, 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.[64] 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.[65] Governments have also resorted to social media intelligence, the techniques and technologies that allow companies or governments to monitor social media networking sites, such as Facebook or Twitter.[66] 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.[67]

---

58 Ibid., Principle 10.
59 Geselleschaft für Freiheitsrechte ("GFF"), Submission.
60 Ibid.
61 Ibid.
62 Ibid.; Privacy International ("PI") et al., Submission.
63 Border Violence Monitoring Network ("BVMN"), Submission.
64 PI et al., Submission.
65 GFF, Submission.
66 PI et al., Submission.
67 Ibid.

28. One submission detailed concerning practices in Germany.[68] 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.[69] The Law also empowers BAMF to share the data with other government agencies, such as security authorities and intelligence services.[70] 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,[71] 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.[72] This routine practice affected more than half of all first-time asylum applicants in the past two years,[73] and certain nationalities more than others raising serious concerns of *de facto* national origin discrimination.

29. This invasive data extraction from personal devices in Germany is unprecedented, targets only asylum seekers, and the legalization of these measures was based on racist and xenophobic assumptions in political discourse.[74] 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.[75] 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.[76] Among 21,505 mobile phones successfully read out in 2018 and 2019, only about 118 cases, or 0.55%, indicated a contradiction.[77] Furthermore, since neither the algorithms nor training data are known to the public, judges and other decision-makers cannot properly assess their reliability.[78]

30. Although regulations such as the European Union's General Data Protection Regulation ("GDPR") seeks 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.[79] 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."[80] 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.[81] The exemption also frees data controllers from their responsibility to provide information to the individuals concerned when their data are collected, including from other sources, like a school, employer or local authority.[82] 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.[83] 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.[84] 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.

---

68 GFF, Submission.
69 Ibid.
70 Ibid.
71 Ibid.
72 Ibid.
73 Ibid.
74 Ibid.
75 Ibid.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid.; Platform for International Cooperation on Undocumented Migrants ("PICUM"), Submission.
80 PICUM, Submission.
81 Ibid.
82 Ibid.
83 GFF, Submission.
84 Ibid.

B. Discriminatory Structures

31. In her Human Rights Council report, the Special Rapporteur provided examples of how 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, she urged that they should also be understood as capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms. In this sub-Section, the Special Rapporteurs 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.

i. Surveillance Humanitarianism and Surveillance Asylum

32. Commentators have cautioned of the rise of "surveillance humanitarianism"[85], 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.[86] Surveillance humanitarianism refers to "enormous data collection systems deployed by aid organizations that inadvertently increase the vulnerability of people in urgent need."[87] Even a misspelled name can result in "bureaucratic chaos" and accusations of providing false information, slowing down what is already a slow asylum process.[88] 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.[89]

33. In this regard, one submission highlights the dangers associated with UNHCR's growing use of digital technologies to manage aid distribution.[90] In refugee camps in Afghanistan, UNHCR mandated iris registration for returning Afghan refugees as a pre-requisite for receiving assistance.[91] Though UNHCR justifies collecting, digitizing and storing the refugees' iris images in the Biometric Identity Management System ("BIMS") as a means of detecting and preventing fraud,[92] the impact of processing such sensitive data can be grave when systems are flawed or abused.[93] 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.[94] 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.[95]

34. 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 power differentials between UN agencies, international NGOs and the affected communities are already stark. 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

85 https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
86 Beduschi, Submission.
87 https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
88 Mark Latonero et al., Digital Identity in the Migration & Refugee Context: Italy Case Study (April 2019).
89 https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
90 Amnesty International, Submission.
91 Ibid.
92 Ibid.
93 Ibid. citing A/HRC/39/29.
94 Amnesty International, Submission.
95 Ibid.

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.[96] 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[97] 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.[98]

35. 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),[99] with no procedural and substantive protections for the individuals whose data are being shared and repurposed.

36. 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.[100] 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.[101] 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.[102]

37. 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. In Germany, under the Asylum Seekers Benefit Act, undocumented persons have the same right to health care as asylum seekers.[103] However, the social welfare office that administers health care for the undocumented has a duty to report their personal data with immigration authorities under section 87 of the Residence Act, which governs the "transfer of data and information for foreign authorities" by all public authorities.[104] 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.

ii. Technological Experimentation

38. Submissions received for this report 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

96 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.

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

98 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.

99 Mirca Madianou, Submission.

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

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

102 Madianou, Submission.

103 PICUM, Submission.

104 Ibid.

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.

39. 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."[105] iBorderCtrl uses hardware and software technologies that seek to automate border surveillance.[106] Among its features, the system undertakes automated deception detection.[107] The EU has piloted this lie detector at airports in Greece, Hungary and Latvia.[108] Reportedly, in 2019 iBorderCtrl was tested at the Serbian-Hungarian border and failed.[109] iBorderCtrl exemplifies the trend of experimenting surveillance and other technologies on asylum seekers based on scientifically dubious grounds.[110] 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.[111] Other countries 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.[112]

40. 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.[113] 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."[114] 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.[115] Canada, Switzerland and the UK also use automated or algorithmic decision-making "for selecting refugees and resettling them."[116] 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.

41. In some contexts, the nature of technological experimentation relates to the genetic data collection, whose purposes are justified on tenuous grounds, but raise serious and

105 PI et al., Submission.
106 See https://www.iborderctrl.eu/The-project.
107 PI et al., Submission.
108 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.
109 PI et al., Submission.
110 Ibid.
111 MRG, Submission.
112 https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.
113 Petra Molnar & Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System" (2018).
114 Molnar & Gill.
115 Joint Council for the Welfare of Immigrants v. Secretary of State for the Home Department CO/2057/2020.
116 Maat for Peace, Submission; Beduschi, Submission citing Molnar & Gill.

concrete human rights concerns. One submission described the Combined DNA Index System ("CODIS"), a forensic DNA database in the United States through which individual states and the federal government collect, store and share genetic information.[117] Since January 2020, the federal government has been collecting DNA from any person in immigration custody.[118] What this means is 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.[119] Non-citizens in immigration custody are not criminals as a rule.[120] In fact, the vast majority of immigration infractions for which an immigrant is detained is civil in nature.[121] 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.[122] The submission rightly highlights that the new immigration policy expanding CODIS moves the U.S. toward constructing a "genetic panopticon," whose purposes and effects may well be discriminatory. CODIS risks turning into a dystopian tool of genetic surveillance that will "encompass anyone within United States borders, including ordinary Americans neither convicted nor even suspected of criminal conduct," threatening democracy and human rights,[123] including on the basis of national origin.

42. As the COVID-19 has further incentivized and legitimized surveillance and other technologies targeting refugees and migrants, these groups have been subjected to further experimentation.[124] One example is the experimental deployment of an immunity passport called "COVI-Pass" in Western Africa.[125] A product of partnership between Mastercard and GAVI, a private-public alliance for vaccination, this digital initiative combines biometrics, contact tracing, cashless payments, national identification and law enforcement.[126] 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.[127]

iii. Border externalization

43. 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.[128] 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, 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 this border externalization, thereby consolidating and expanding discriminatory, exclusionary regimes.

44. 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."[129] It deploys surveillance drones in the

[117] Daniel I. Morales, Natalie Ram & Jessica L. Roberts, Submission.
[118] Ibid.
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Amnesty International, Submission.
[125] Ibid.
[126] Ibid.
[127] Ibid.
[128] See, e.g., A/HRC/23/46, A/HRC/29/36 and A/72/335.
[129] Maat for Peace, Submission citing Btihaj Ajana, "Augmented borders: Big Data and the ethics of immigration control" (2015).

Mediterranean Sea, in order to notify the Libyan coastguard to intercept refugee and migrant boats and return migrants to Libya.[130] Although the European Commission insists the drones are only for civil surveillance purposes,[131] 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, making it one of the deadliest migration routes in the world.[132] Surveillance technologies are essential for coordination in this context.

45. Another submission reported the participation of thirteen European nations in the ROBORDER project, a "fully functional, autonomous border surveillance system."[133] ROBORDER consists 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.[134] 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, suspending state power from the skies, and extend the border visually and virtually, turning people into security objects and data points to be analysed, stored, collected, and rendered intelligible. [135] The usage of military, or quasi-military, autonomous technology also bolsters the connection between immigration, national security, and the increasing push towards the criminalization of migration and using risk-based taxonomies to demarcate and flag cases.[136] Globally, States, particularly those on the frontiers of large numbers of migrant arrivals, have been using various ways to pre-empt and deter those seeking to legally apply for asylum. This type of deterrence policy is very evident in Greece, Italy, and Spain,[137] countries which are on the geographic frontiers of Europe, which increasingly rely on violent deterrence and 'push back' policies.

46. One submission highlighted Croatia's use 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.[138] This submission alleges hundreds of human rights abuses in the past three years, including "illegal push-backs" that reflect "inherently racist cleavages."[139] 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."[140]

47. Discriminatory border externalization is also achieved through transnational biometric data-sharing programs across multiple countries. One submission reported a biometric data sharing program between the governments of Mexico and the U.S.[141] As of August 2018, Mexico had deployed the U.S.-funded program in all fifty-two migration processing stations.[142] 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

[130] Franciscans International, Submission citing https://www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/.
[131] Franciscans International, Submission citing https://www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.
[132] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25875&LangID=E.
[133] Homo Digitalis, Submission. See also https://roborder.eu/. The participating States are: Belgium, Bulgaria, Estonia, Finland, Germany, Greece, Hungary, Italy, Portugal, Romania, Spain, Switzerland, and the United Kingdom.
[134] Ibid.
[135] Csernatoni.
[136] See Van Den Meerssche, Submission.
[137] 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/.
[138] BVMN, Submission.
[139] Ibid.
[140] Ibid.
[141] PI et al., Submission.
[142] Ibid.

gang.[143] However, Mexico's National Institute of Migration has denied processing biometric data in answers to freedom of access to information requests.[144]

iv. Immigration Surveillance[145]

48. 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."[146] This border enforcement system also surveils the Tohono O'odham Nation's reservation, located in Arizona approximately one mile from the border.[147] This "smart" border surveillance system replaces a prior one, which research showed had failed to prevent undocumented border crossings, but instead shifted migrants' routes, thereby "increasing [their] vulnerability to injury, isolation, dehydration, hyperthermia and exhaustion"—and deaths.[148] 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."[149] 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.[150] The UN Committee on the Elimination of Racial Discrimination has expressed its concern to the General Assembly over the "ever more precarious journeys being taken by asylum seekers, refugees and migrants in search of safety and dignity resulting in unnecessary deaths and suffering."[151] As mentioned above, the current evidence is that so-called "smart" border technology forces these ever more precarious journeys, with a disproportionate impact on certain national origin, ethnic and racial groups.

49. In the United States, the communications of detained immigrants and their families and friends are surveilled.[152] The business model of the corporate providers of the technology is one whereby detained immigrant and their families "get convenience in the form of calls, video chats, voice mail messages, photo sharing and text messaging, while its real clients," immigration officials, get user data.[153] The web-based surveillance software, promoted as free government officials with every installation "includes call-pattern analysis, relationship analysis and tools for data visualization."[154]

50. Yet another facet of immigration surveillance involves social media screening. As of April 2019, the U.S. State Department requires visa applicants to disclose their social media account information in the past five years from the time of application.[155] In September 2019, the U.S. Department of Homeland Security ("DHS") proposed to compel such disclosures from non-citizens already present and even residing in the country who apply for immigration benefits, including naturalization, permanent residence and asylum.[156] As the submission highlights, this expansive approach to social media screening is especially troubling because of the U.S. immigration enforcement's demonstrated track record of utilizing social media information in a manner that disproportionately harms members of minority racial, ethnic,

143 Ibid.
144 Ibid.
145 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).
146 Campaign to Stop Killer Robots, Submission.
147 Ibid.
148 Samuel Norton Chambers et al.
149 MRG, Submission.
150 Mijente, Submission; Iván Chaar-López, Submission.
151 Franciscans International, Submission.
152 Mijente, Submission citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.htm.
153 Ibid.
154 Ibid.
155 Harvard Immigration & Refugee Clinical Program ("HIRC"), Submission.
156 Ibid., citing https://www.govinfo.gov/content/pkg/FR-2019-09-04/pdf/2019-19021.pdf.

and religious groups.[157] 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.[158] Immigration and Customs Enforcement ("ICE"), a constituent agency of DHS, frequently combs social media to support gang membership allegations.[159] In one case, DHS evidenced its allegation with a Facebook photo of the immigrant youth wearing a Chicago Bulls hat. The immigration court denied him bond and rejected both his applications for asylum and permanent residence, deporting him to a country where he feared for his life,[160] in violation of non-refoulement prohibitions under international law.

51. 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."[161] For example, last fall, 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.[162] In addition to the direct burdens they place on non-citizens, the U.S. government's expanded social media disclosure requirements foreseeably affected freedoms of speech and association.

52. Homeland Security Investigations ("HSI"), ICE's investigative arm, had already been testing automated social media profiling as early as 2016, [163] 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.[164] Submissions also raised concerns about the US governments consideration of technologies whose goal was "determinations via automation" regarding whether an individual applying for or holding a U.S. visa was likely to become a "positively contributing member of society" or intended "to commit criminal or terrorist attacks."[165] One submission noted in particular the use in the United States 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.[166] This example is one in which technology has been tailored to pursue punitive immigration enforcement measures rooted in the racist, xenophobic and ethnonationalist vision of immigration that has been advanced by the Trump administration.

53. 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.[167] Furthermore, racial bias is already present in the datasets on which these models rely.[168] 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."[169]

[157] HIRC, Submission.
[158] Ibid., citing https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.
[159] HIRC, Submission.
[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Mijente, Submission citing Sarah Lamdan, "When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing" (2019).
[164] Mijente, Submission citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[165] Ibid.
[166] MRG, Submission.
[167] Mijente, Submission.
[168] Ibid.
[169] Ibid.

IV. Recommendations

54. **In her report to the Human Rights Council, the Special Rapporteur provided states with a structural and intersectional human rights law approach to racial discrimination in the design and use of emerging digital technologies. It explained the applicable international human rights obligations highlighting:**

(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.**

55. **The Special Rapporteur explained the concepts and doctrines of direct, indirect and structural racial discrimination under international human rights law and outlined the obligations they impose on States where emerging digital technologies are concerned. She highlighted that these obligations also have implications for non-State actors, including corporations, which in many respects exert more control over these technologies than States do. She reiterates her analysis and recommendations in that report and urges states to consider them alongside the recommendations included herein. The focus of this section is recommendations for implementing the human rights equality and non-discrimination obligations highlighted in the Human Rights Council Report, in the specific context of border and immigration enforcement.**

56. **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 of the Special Rapporteur. States should also follow the guidance provided by interventions such as the Principles on Deprivation of Nationality as a National Security Measure,[170] and the Principles of Protection for Migrants, Refugees, and Displaces People During COVID-19[171] which articulate the existing obligations States have, including with respect to equality and non-discrimination, to ensure the human rights of migrants, refugees, stateless persons and related groups.**

57. **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.**

58. **<u>UN Member States</u>: at both the domestic and international levels, Member States must ensure 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**

[170] Institute on Statelessness and Inclusion et al.

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

the adoption of systems before they can be publicly deployed. These impact assessments must 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.**

59. **<u>UN bodies such as UNHCR and IOM</u>: 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;**

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

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

UNHCR:

60. **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) **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;**

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

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

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

All UN Humanitarian and Related Bodies:

- **Implement the recommendations above addressed to IOM and UNHCR.**