AMNESTY INTERNATIONAL
INTERNATIONAL SECRETARIAT

www.amnesty.org

RACE, BORDERS, AND DIGITAL TECHNOLOGIES

SUBMISSION TO THE UN SPECIAL RAPPORTEUR ON CONTEMPORARY FORMS OF RACISM, XENOPHOBIA AND RELATED INTOLERANCE

SEPTEMBER 2020

Amnesty International welcomes your call for contributions ahead of your forthcoming report on race, borders, and digital technologies, which will examine how digital technologies deployed in the context of border enforcement and administration reproduce, reinforce, and compound racial discrimination.

We are encouraged by this report for paying particular attention to the potential human rights violations experienced by refugees and migrant populations at large who are subject to these technologies, especially in light of their reinforcement amidst the COVID-19 pandemic.

- While the usage of biometric technologies in the context of refugee registration and border enforcement traces back to 2001[i] (specifically when the Dutch government and the company HSB Netherlands integrated existing registration databases with digital fingerprinting, as part of "Project Profile"), the system has seen leaps in technological sophistication since. By 2013, "one million fingerprints and 500,000 iris records" had been gathered, globally.[ii] The current tools used to this end— the Biometric Identity Management System (BIMS) and Global Distribution Tools— were developed and deployed in partnership with Accenture in 2014[iii], and first tested in Chad, Malawi, and Thailand[iv], before eventually being integrated by the Kenyan government.
- In a number of camp contexts, such as those experienced by returning Afghan refugees, UNHCR mandated iris registration was made a compulsory pre-requisite for receiving assistance. This was justified under the auspices of fraud-detection. Afghan refugees' iris images were collected, digitized, and stored in the UNHCR database. To receive assistance, a refugee's iris would have to match their pre-existing biometric file to prove they were entitled to humanitarian aid, as part of BIMS. While resource management is important, the use of biometric surveillance tools such as iris registration systems can present certain risks as biometric data is being processed. This type of data is especially sensitive and the impact of the processing of such data can be particularly grave when it is misused.[v] In addition, these systems have been documented to lead to system aversion and the loss of access to crucial goods and services for survival[vi] [vii] [viii].
- While free connectivity for displaced populations is undoubtedly providing an essential service[ix], several initiatives provided by predominantly MercyCorps, Cisco, and Google[x], have reportedly offered limited browsing capabilities[xi], seen great variation in maintenance and upkeep, and provided little transparency over data protection practices. In particular, these initiatives have insisted on providing limited connectivity in refugee camps only, despite pushback from affected communities, who are often in-between places and in need of connectivity beyond the confines of the camp.

- Access to the internet has long been recognised as a critical enabler of human rights in the digital age. In 2011, the UN Special Rapporteur on Freedom of Expression acknowledged the "unique and transformative nature of the internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the progress of society as a whole."[xii] In 2016, the UN Human Rights Council stressed the importance of "applying a comprehensive human rights-based approach when providing and expanding access to the internet and for the internet to be open, accessible and nurtured."[xiii] Combined, the limitation of browsing capabilities, variable connectivity, and disregard for spatial requirements of refugees, not only point to a failure to take into account the needs of marginalized groups but can have serious consequences on their ability to access the internet.
- Technological interventions in migration contexts are also used in more directly invasive and experimental ways, such as the deployment of IrisGuard's iris scanner technology by the UNHCR and the WFP in Jordan's Za'atari and Azraq refugee camps [xiv]. The iris scanner was celebrated as a prime example of how information communications technologies for development (ICT4D) could provide access to credit. However, surveillance-related fears from affected communities, aid workers, and academics about the invasive and obscure data practices of the technology have allegedly disincentivized individuals from registering upon arrival to camps, potentially barring them from access to critical services[xv].
- Similarly, the World Food Programme and the UNHCR's partnerships with several technology companies for food distribution in Jordan, Kenya, and Rwanda, including M-PESA, IrisGuard, and Palantir, risk similar consequences, by presenting a Hobson's choice to refugees: compromise your identity, or risk starvation or death.[xvi] [xvii]
- The COVID-19 pandemic, in particular, has given rise to a race to the bottom for technology corporations in the development of not only contact tracing systems but also surveillance, biometric and digital identification systems more broadly.[xviii]
- In combination with heightened fears of further infections, the emboldened demand for tighter border restrictions against the inflow of refugees and migrants at large, technologies deployed to register, surveil and ultimately police refugee and migrant populations have similarly been given further impetus.
- Examples of this include Mastercard and GAVI's recent COVI-pass:[xix] a combination of biometric ID, contact-tracing, cashless payments, national ID and law enforcement, centralised under a single digital initiative deployed experimentally in the context of Western Africa. Not only do these technologies work outside the purview of rigorous human rights impact assessments and regulations, but they risk significantly stifling several rights, enjoyed marginally by refugees and migrants, including freedom of movement, the right to privacy, the right to bodily autonomy, and the right to equality and non-discrimination, among others.

Recommendations

Technology giants have become more intimately involved with migration governance and border enforcement broadly, and while extending digital infrastructure that could ensure connectivity and a digital lifeline to refugees and vulnerable migrant populations is important, data collection, storage and use takes place in environments shaped by anti-migration policies, imposing so-called "national security" measures, corporate interests and a general lack of respect for refugees' rights. The absence of sufficient safeguards and oversight within an ever-growing tech sector can allow technology to develop faster than interventions which protect against its misuse or mitigate potential harms. Stringent safeguards are required to ensure that they are in line with human rights:

1. Any technologies or surveillance measures adopted must be lawful, necessary and proportionate. Before any system is deployed, the necessity and proportionality of the measure must be fully explored. Is the minimum amount of data being collected and processed for a legitimate objective? Can the type and scale of data needed to be collected by other less privacy-invasive means? Does the system under consideration potentially transcend the remit of the organisation or service provider? Can the organisation or service-provider justify the need for the additional data?
2. These technologies often require an extraordinary amount of data collection from populations who are often stateless and therefore face significant obstacles and challenging these practices. As such, it is crucial that the relevant state authorities conduct mandatory human rights due diligence and data protection impact assessments in advance of their deployment and throughout their lifecycle

3. Any use of technologies, including big data, artificial intelligence and biometric systems, must address the risk that these tools will facilitate discrimination and other rights abuses against racial minorities, people living in poverty, and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets.
4. Data contestability must also be incorporated into any data collection system. The lack of alternative methods of providing data in particularly sensitive contexts has led to reported incidents of self-harm e.g. through damaged fingertips[xx] [xxi] [xxii]. Similarly, individuals who are not easily registered due to physical particularities that appear obscure to the technology, may also invariably face the risk of being perceived as suspicious. In Rohingya refugee camps in Bangladesh, the technology was reported to have failed to recognise finger prints for a person, leaving them without food rations. While the UNHCR and IOM disputed this, there must be consideration for the fact that some of this technology will be employed in remote areas vulnerable to technological disruptions. Furthermore, with the use of force or detention as a very real consequence, the ability to contest biometric data collection, and indeed output of any migration technology system, must be a part of the data governance architecture of the intervention in question;
5. States should require businesses involved in developing and providing technologies in the context of refugee registration and border enforcement, including big data, artificial intelligence and biometric systems, to undertake human rights due diligence, in line with international standards such as the UN Guiding Principles on business and human rights and the OECD's Guidance on due diligence. Technology companies must be held liable for human rights harms they have caused or contributed to, or if they fail to carry out human rights due diligence.
6. Affected communities must be meaningfully consulted in developing a comprehensive consent and equitable data-ownership model. In the context of refugees and asylum seekers, having some degree of control over identifiable data can make the difference between resisting or being subject to a deportation order – the difference between life and death[xxiii];
7. It is also crucial that those institutions weigh up any potentially unaccounted or unquantifiable costs associated with their proposed systems; what are the costs in terms of the agency and dignity of refugees and migrants? What are the costs associated with risks of function creep, hacking, and the unlawful access and misuse of data?
8. Governments must take every effort to protect people's data, including ensuring sufficient security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage.
9. Where there are alternative non-invasive avenues that could meet the gap experienced by service-providers, without compromising the right to privacy, equality and non-discrimination, and freedom from surveillance, these must be explored. Technological determinism, if left unaddressed, may lead to dire consequences for human rights;
10. Any use of technologies must incorporate accountability protections and safeguards against abuse. Further, individuals must be given the opportunity to know about and challenge any measures to collect, aggregate, and retain, and use their personal data. Individuals who have been subjected to technologies, including big data, artificial intelligence and biometric systems, must have access to effective remedies.

[i] Maitland, C., 2018. Digital Lifeline?: ICTs for Refugees and Displaced Persons. MIT Press.

[ii] Ibid.

[iii] United Nations High Commissioner for Refugees and Accenture Deliver Global Biometric Identity Management System to Aid Displaced Persons [WWW Document], n.d. URL /news/united-nations-high-commissioner-for-refugees-and-accenture-deliver-global-biometric-identity-management-system-to-aid-displaced-persons.htm

[iv] UNHCR, Accenture provide global biometric identity management system to help refugees | Biometric Update [WWW Document], n.d. URL https://www.biometricupdate.com/201505/unhcr-accenture-provide-global-biometric-identity-management-system-to-help-refugees

[v] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 14; see also: Privacy International, Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism, June 2019, www.privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf

[vi] Race in the Digital Periphery: The New (Old) Politics of Refugee Representation, 2019. . The Sociological Review. URL https://www.thesociologicalreview.com/race-in-the-digital-periphery-the-new-old-politics-of-refugee-representation/

[vii] Madianou, M., 2019. Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. Social Media + Society 5, 205630511986314. https://doi.org/10.1177/2056305119863146

[viii] Thomas, E., 2018. Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database. Wired UK.

[ix] Latonero, M., Kift, P., 2018. On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control. Social Media + Society 4, 205630511876443. https://doi.org/10.1177/2056305118764432

[x] Standing with refugees and nonprofits that serve them on World Refugee Day [WWW Document], 2017. . Google. URL https://blog.google/outreach-initiatives/google-org/standing-refugees-and-nonprofits-serve-them-world-refugee-day/

[xi] How technology is affecting the refugee crisis [WWW Document], 2016. Mercy Corps. URL https://www.mercycorps.org/blog/technology-refugee-crisis

[xii] Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the Human Rights Council, 16 May 2011, UN Doc A/HRC/17/27

[xiii] UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, June 2016, UN Doc A/HRC/32/L.20

[xiv] WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari | World Food Programme [WWW Document], n.d. URL https://www.wfp.org/news/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu

[xv] The New Humanitarian | UN gives ultimatum to Yemen rebels over reports of aid theft [WWW Document], n.d. URL https://www.thenewhumanitarian.org/news/2019/06/17/un-yemen-rebels-aid-theft-biometrics

[xvi] Palantir and WFP partner to help transform global humanitarian delivery | World Food Programme [WWW Document], n.d. URL https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery

[xvii] One of the UN's largest aid programmes just signed a deal with the CIA-backed data monolith Palantir [WWW Document], n.d. . Privacy International. URL http://privacyinternational.org/news-analysis/2712/one-uns-largest-aid-programmes-just-signed-deal-cia-backed-data-monolith

[xviii] Madianou, M., 2019. Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. Social Media + Society 5, 205630511986314. https://doi.org/10.1177/2056305119863146

[xix] Public-private partnership launches biometrics identity and vaccination record system in West Africa [WWW Document], n.d. . Privacy International. URL http://privacyinternational.org/examples/4083/public-private-partnership-launches-biometrics-identity-and-vaccination-record-system

[xx] Sweden refugees mutilate fingers, 2004.

[xxi] UK immigration staff safety fears amid migrant fingerprinting [WWW Document], 2020. . Workpermit.com. URL https://workpermit.com/news/uk-immigration-staff-safety-fears-amid-migrant-fingerprinting-20200612

[xxii] EU's migrant fingerprinting system Eurodac under review | Europel News and current affairs from around the continent | DW | 09.11.2017 [WWW Document], n.d. URL https://www.dw.com/en/eus-migrant-fingerprinting-system-eurodac-under-review/a-41311572

[xxiii] Stenum, H., 2017. The Body-Border – Governing Irregular Migration Through Biometric Technology. Spheres. URL http://spheres-journal.org/the-body-border-governing-irregular-migration-through-biometric-technology/