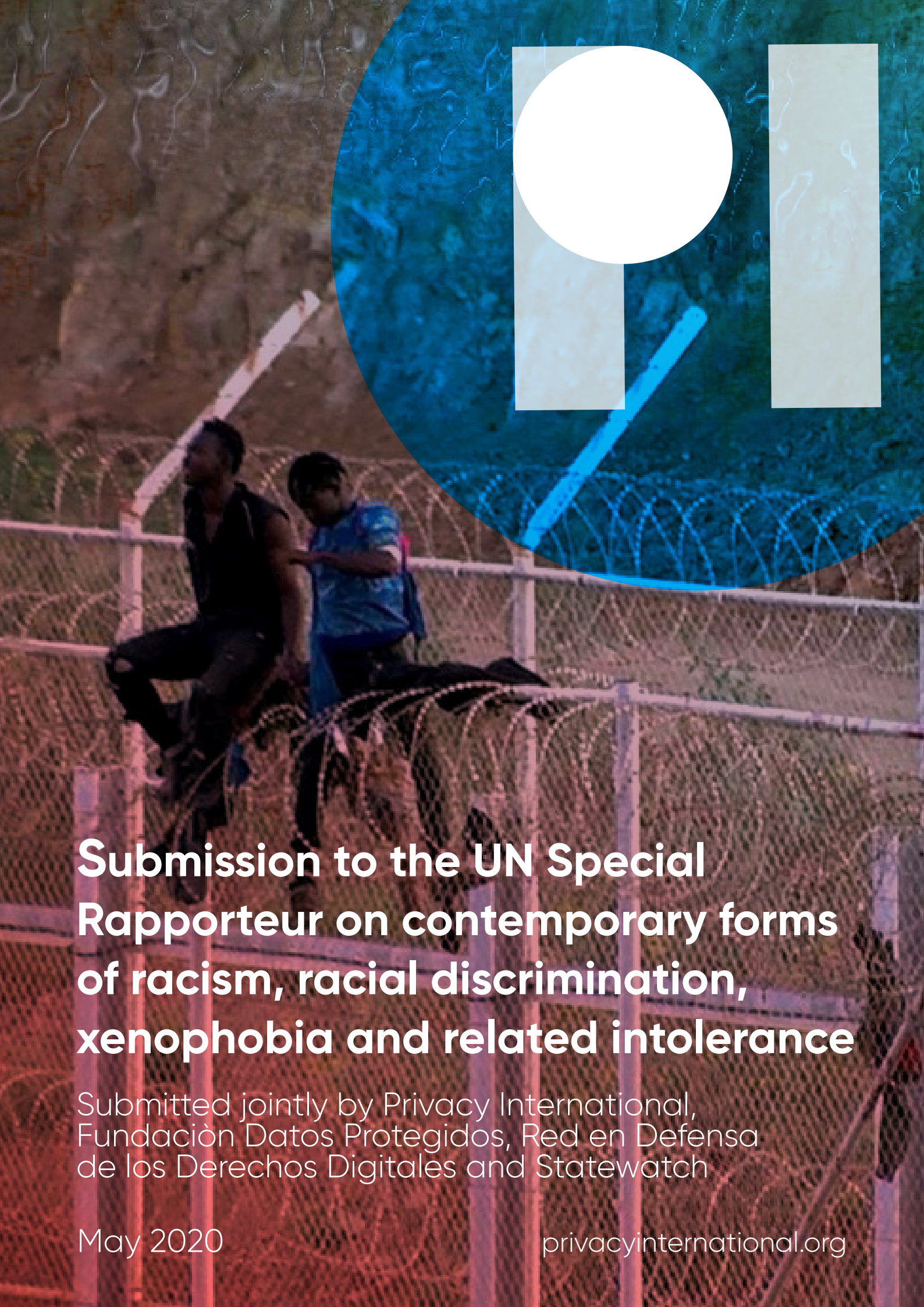

Submission to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance

Submitted jointly by Privacy International, Fundaciòn Datos Protegidos, Red en Defensa de los Derechos Digitales and Statewatch

May 2020

privacyinternational.org

Privacy International, Fundaciòn Datos Protegidos, Red en Defensa de los Derechos Digitales, and Statewatch's submission on Race, Borders, and Digital Technologies

May 2020

Privacy International (PI), Fundaciòn Datos Protegidos, Red en Defensa de los Derechos Digitales (R3D) and Statewatch welcome the decision of the UN Special Rapporteur on contemporary forms of racism, xenophobia and related intolerance to focus her 2020 annual report on how digital technologies deployed in the context of border enforcement and administration reproduce, reinforce, and compound racial discrimination.

Recommendations

We recommend the UN Special Rapporteur in her upcoming report to:

- analyse and assess the regulation and governance of digital technologies deployed in the context of border enforcement and administration;
- demand that such technologies should be used only in accordance with human rights standards, ensuring a legal framework, appropriate safeguards, effective oversight and remedial mechanisms are in place;
- call states to take into account before implementing such measures the need to ensure that the deployment of new technologies is not discriminatory.
- examine how the deployment of these technologies are contributing to the marginalisation and further discrimination of people in vulnerable situations;
- underline the impact of these digital technologies on people at the border;
- consider adopting a wide approach to the understanding of border, to take into account border externalisation and border digitalisation considerations;
- consider the role of private companies in immigration enforcement and in particular in building digital borders;
- underline states' accountability for financing border externalisation and using such financing to extend their border to other countries.

This submission provides information on specific digital technologies in service of border enforcement and administration policies, as well as an overview of how such practices amount to serious violations of the right to privacy of migrants and as a result facilitate violations of other human rights of migrants, refugees, stateless people, non-citizens, and individuals or groups who are or who are perceived to be foreign.

1. Digital Technologies in Border Enforcement and Administration – Forms, Context, and Relevant Actors

1.1. Examples of digital technologies deployed in border enforcement and administration

Governments around the world are using migrants as the testing ground for many of technology innovations biometric schemes, invasive mobile phone extraction procedures, automated systems and more. Compulsory identification of travellers now includes the collection of fingerprints and facial images, and secret watchlists, dossiers and profiles are being developed. Below we outline some of those initiatives.

Biometric data collection and processing

As with many other sectors, we have seen the deployment of biometric systems in immigration and border management mechanisms. Biometric technology is provided by companies to serve a variety of purposes including in screening and/or determination of asylum as part of age and origin verification, as well registration, authentication and verification of identity.

In 2003, the Identification of applicants (EURODAC) was adopted and set-up an EU asylum central fingerprint database.[1] It is to this central database that the fingerprints of any person seeking asylum over the age of 14[2] anywhere in the European get transmitted. It is used for fingerprint comparison evidence to assist with determining the Member State responsible for examining an asylum application made in the EU to ensure compliance with the Regulation (EU) No. 604/2013 ('the Dublin Regulation')[3] which requires those seeking asylum to submit their claim in the first country of the EU they enter. Legislative negotiations are ongoing to expand this database, with the aim of gathering more personal data from more people and lowering the age of data collection from to six years of age.[4]

As of August 2018, according to the United States Department of State International Narcotics Control Strategy Report for the year 2019[5], the biometric data sharing program between the governments of Mexico and the United States was active in all 52 migration processing stations in Mexico. The program uses biometric information to screen detained migrants in

---

1 PI, "The EURODAC Debate: Do Asylum-Seekers Deserve Human Rights?", 12 December 2012, https://privacyinternational.org/blog/1424/eurodac-debate-do-asylum-seekers-deserve-human-rights (accessed 19 March 2020).

2 A new proposal aims to lower the age limit to 6 years old. European Commission, Identification of applicants (EURODAC), https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en (accessed 19 March 2020).

3 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ L 180, 29.6.2013, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex%3A32013R0604 (accessed 19 March 2020), pp 31–59.

4 Statewatch, PICUM, "Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status", page. 24, November 2019, https://www.statewatch.org/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf

5 US State Dept. International Narcotics Control Strategy Report. March 2019. Available at: https://www.state.gov/wp-content/uploads/2019/04/INCSR-Vol-INCSR-Vol.-I-1.pdf, p. 215.

Mexico that have allegedly tried to previously cross the U.S. border or are "members of a criminal gang"[6].

Inconsistencies and errors in databases also result in large numbers of wrong identity identification. A report of the Department of Home Security found errors in 825,000 registries in a border crossing database[7]. Failure rates in identification affects disproportionately people from some races, class and age groups[8].

There is also a lack of transparency in this process: for example, despite contradicting evidence, Mexico's National Institute of Migration has denied processing biometric data in answers to freedom of access to information requests made by R3D.[9]

Another example is provided by the high rate of return of Honduran people, who tried to enter the United States and Mexico, showing an evident crossing of data in the databases of the National Biometric Control System of the National Institute of Migration (INM) from Honduras. This system collects a series of specific data on the identity of people, keeping a biographical control of people –even children-, which includes and concentrates data such as sex, date of birth, and destination of migrants.[10]

Lie detectors testing as a verification tool

The use of extraction tools presented above is part of a broader trend of aiming surveillance and other security technology at asylum seekers and migrants, often on scientifically dubious grounds. In Europe, this includes the use of technology which supposedly identifies if a person is lying based on their 'micro-gestures', a person's origin based on their voice, and their age based on their bones.[11]

The European Union's Horizon 2020 research and innovation programme has been funding a project called iBorderCtrl, defined as "an innovative project that aims to enable faster and thorough border control for third country nationals crossing the land borders of EU Member

---

6 Washington Post. U.S. gathers data deep in Mexico, a sensitive program Trump's rhetoric could put at risk. April, 2018. Available at: https://www.washingtonpost.com/world/national-security/us-gathers-data-on-migrants-deep-in-mexico-a-sensitive-program-trumps-rhetoric-could-put-at-risk/2018/04/06/31a8605a-38f3-11e8-b57c-9445cc4dfa5e_story.html?utm_term=.bd1317c13a5f

7 Department of Homeland Security. Office of the Inspector General. US-VISIT Faces Challenges Identifying and Reporting Multiple Biographic Identities. August 2012. p. 3,6. Available at: https://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-111_Aug12.pdf

8 Wevers, R., 2018. Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection. Journal for Media History, 21(2), pp.89–105. DOI: http://doi.org/10.18146/2213-7653.2018.368

9 R3D, "La frontera en el cuerpo: registro biometrico en el context migratorio", 28 January 2020 (accessed on 15 May 2020)

10 See: https://reconocimientofacial.info/controles-biometricos-para-migrantes-en-honduras/

11 Melanie Ehrenkranz, "An AI Lie Detector Is Going to Start Questioning Travelers in the EU", *Gizmodo*, 31 October 2018, https://gizmodo.com/an-ai-lie-detector-is-going-to-start-questioning-travel-1830126881 (accessed 19 March 2020); "Automatic Speech Analysis Software Used to Verify Refugees", Dialects, DW, 17 March 2017, https://www.dw.com/en/automatic-speech-analysis-software-used-to-verify-refugees-dialects/a-37980819 (accessed 19 March 2020); Miranda Aldersley, "Young Migrants Will Have to Undergo X-Ray Tests to Establish Age", *Mail Online*, 22 March 2019, https://www.dailymail.co.uk/news/article-6839551/Young-migrants-undergo-X-ray-tests-BONES-establish-age-France.html (accessed 19 March 2020).

States".[12] In addition to other features, the system undertakes automated deception detection. [13]

The system was tested at the border in Hungary, Latvia and Greece[14]. In July 2019, The Intercept used the system at the Serbian-Hungarian border: reportedly, the system failed, and the results were not disclosed.[15]

This is highly experimental technology whose results cannot be trusted. There are few places in the world where an individual is as vulnerable as at the border of a foreign country.[16] New technologies should not be used in situations where people are in most vulnerable positions and where they are unable to cross-check or challenge their results.

Mobile phone extraction as a verification tool

Governments are increasingly using migrants' electronic devices as verification tools often to corroborate the information they provide to the authorities. This practice is enabled with the use of mobile extraction tools, which allow an individual to download key data from a smartphone, including contacts, call data, text messages, stored files, location information, and more.[17]

In Austria, Germany, Denmark, Norway, the United Kingdom, and Belgium, we have seen laws allowing for the seizure of mobile phones from asylum or migration applicants from which data is then extracted and used as part of asylum procedures.[18]

Not only such kind of practices constitute a serious interference with their right to privacy that is neither serious nor proportionate but also the assumption that data obtained from digital devices leads to reliable evidence is flawed. If a person claims certain information is true, and there exists information on their smartphone suggesting otherwise, it is not evidence that they are being disingenuous. They are a variety of legitimate reasons why the data extracted would differ from the information provided by an applicant.

Social media intelligence (SOCMINT) as a verification tool

Over the last decade, we have seen governments across sectors including for immigration enforcement purposes resorting to social media intelligence (SOCMINT), the techniques and

---

12 iborderCtrl website, https://www.iborderctrl.eu/The-project (accessed 19 March 2020).
13 iborderCtrl Participants, https://www.iborderctrl.eu/#Project-Participants (accessed 19 March 2020).
14 iborderCtrl Pilot Results, https://www.iborderctrl.eu/Pilot-Results (accessed 19 March 2020).
15 Ryan Gallagher and Ludovica Jona, "We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive", *The Intercept*, 26 July 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector (accessed 07 May 2020).
16 PI, Tech at the Border, https://privacyinternational.org/taxonomy/term/703 (accessed 19 March 2020). PI, Protecting Migrants at Borders and beyond, https://privacyinternational.org/protecting-migrants-borders-and-beyond (accessed 19 March 2020).
17 I. Kaplan, UNHCR, How Smartphones and Social Media have Revolutionized Refugee Migration", https://www.unhcr.org/blogs/smartphones-revolutionized-refugee-migration/, 26 October 2018 (accessed 07 May 2020).
18 Morgan Meaker, "Europe Is Using Smartphone Data as a Weapon to Deport Refugees", *Wired UK*, 2 July 2018, https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations (accessed 19 March 2020).

technologies that allow companies or governments to monitor social media networking sites (SNSs), such as Facebook or Twitter.[19]

Some of these activities are undertaken directly by government themselves but in some instances, governments are calling on companies to provide them with the tools and/or knowhow to undertake this sort of activities. One example is the Giant Oak Search Technology (GOST)[20], which uses "sophisticated analytics scoring" to prioritise how results are shown, allowing customers like ICE (the U.S. Immigration and Custom Enforcement) to search by keywords, and provides a "dossier creation user interface".[21]

In September 2010, Frontex, the European Border and Coast Guard Agency, published a call for tender to pay €400,000 to a surveillance company to track people on social media."[22] Eventually, they decided to cancel the tender process.[23]

Reportedly, the European Asylum Support Office (EASO) also monitored refugee networks to detect new routes and find smugglers[24], a practice that stopped in 2019 after the European Data Protection Supervisor (EDPS) imposed a temporary ban, saying EASO had no legal basis for monitoring refugee routes on social media.[25]

Similar concerns to the ones raised in relation to mobile phone extraction apply here as well.

1.2. Border Externalisation as a structural and economic factor that has led to the prevalence of digital technologies in border enforcement

Countries with the largest defence and security sectors are transferring technology and practices to governments and agencies around the world, including to some of the most authoritarian countries in the world. China, European countries, Israel, the US, and Russia, are all major providers of such surveillance worldwide, as are multilateral organisations such as the European Union.

"Border Externalisation", the transfer of border controls to foreign countries, has in the last few years become the main instrument through which the United States[26] and the European Union (EU) seeks to stop migratory flows to Europe. It relies on utilising modern technology,

---

19 PI, "Social Media Intelligence", 23 October 2017, https://privacyinternational.org/explainer/55/social-media-intelligence (accessed 07 May 2020).

20 OAK Website, GOST® (Giant Oak Search Technology), https://www.giantoak.com/product (accessed 19 March 2020).

21 PI, "Who Supplies the Data, Analysis, and Tech Infrastructure to US Immigration Authorities?", 9 August 2018, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities (accessed 19 March 2020).

22 'ETendering - Data', 25 September 2019, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=5471 (accessed 19 March 2020).

23 PI, "#PrivacyWins: EU Border Guards Cancel Plans to Spy on Social Media (for Now)", 19 November 2019, https://privacyinternational.org/node/3289 (accessed 12 May 2020).

24 Alexander Fanta, "[Investigation] Data Watchdog Raps EU Asylum Body for Snooping", *EUobserver*, 9 December 2019, https://euobserver.com/investigations/146856 (accessed 7 May 2020).

25 Formal consultation on EASO'social media monitoring reports (case 2018-1083), European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf (accessed 19 March 2020).

26 PI, "Here's the Surveillance the US Exports to Central America as Aid - And it's Surviving Trump's Cuts", https://privacyinternational.org/news-analysis/3011/heres-surveillance-us-exports-central-america-aid-and-its-surviving-trumps-cuts, 29 July 2019, (accessed 07 May 2020).

training, and equipping authorities in third countries to export the border far beyond its shores.[27] The surveillance industry is playing an essential role in the process.

Their involvement is enabled by the adoption of *ad hoc* funds, like the controversial "EU-Turkey deal", an agreement which saw €6 billion given to Turkey in exchange for its commitment to seal its border with Greece and Syria,[28] and the EU Trust Fund for Africa (EUTF).[29]

Surveillance technologies and practices developed and used by the most advanced surveillance agencies in the world are being spread globally, including to countries which lack safeguards for their use. Without such safeguards, surveillance is being used to entrench political control, and used to spy on activists, journalists, dissidents and any opposition. These transfers of surveillance are driven by governments and institutions aiming to outsource the ongoing wars on migration, terror and drugs to other countries.

Borders are not only those we can see: we are witnessing an increasing externalisation of migration controls with the transfer of border management to third countries and digital borders, i.e. digital portals and databases.[30] Technological developments, such as the ones mentioned above, turn borders invisible. They are putting barriers that cannot be overcome or challenged particularly when tested against people in extremely vulnerable positions.

1.3. Role of private companies

Within the immigration ecosystem there are an array of actors from governments and governmental bodies and oversight mechanisms, inter and intra-governmental institutions, non-governmental organisations as well as increasingly companies[31] who are governing, developing and participating in the deployment of digital technologies deployed in the context of border enforcement and administration.

Public-private collaborations to build digital borders

One of these actors is the private companies that eagerly provide technology, equipment, expertise and implementation of the digitalisation of borders, always for a fee.

---

[27] PI, "New Report Underlines the EU's Strategy in the War on Migration: Border Externalisation", https://privacyinternational.org/news-analysis/3224/new-report-underlines-eus-strategy-war-migration-border-externalisation", 18 September 2019, (accessed 07 May 2020).

[28] Daniele Biella, "L'accordo Ue-Turchia viola i diritti umani, ci sono le prove", *Vita*, 28 June 2016, http://www.vita.it/it/article/2016/06/28/laccordo-ue-turchia-viola-i-diritti-umani-ci-sono-le-prove/139960/ (accessed 19 March 2020).

[29] PI, "Policy Briefing - The Future of the EU Trust Fund for Africa", 18 September 2019, https://privacyinternational.org/advocacy/3220/policy-briefing-future-eu-trust-fund-africa (accessed 19 March 2020).

[30] PI, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance (accessed 13 May 2020).

[31] See: PI's submission to the 'UN Working Group on the use of mercenaries' on the role of private companies in immigration and border management and the impact on the rights of migrants, https://privacyinternational.org/advocacy/3756/pis-submission-un-working-group-use-mercenaries-role-private-companies-immigration, 07 May 2020

As calls for a 'secure southern border' have been amplifying in the US by politicians, experts, and Silicon Valley techies are coming out in force to proffer swanky digital solutions in the place of 30-foot steel slats or concrete blocks.[32]

In early 2019, the Washington Post reported that Anduril Industries had landed a contract with US Customs and Border Protection (CBP) to expand its digital border security system in California.[33]

In a study published in January 2020, researchers found that as a result of the building of the towers along the border, many migrants were forced to explore new ways to cross pushing them to more dangerous routes leading to deaths from dehydration, exhaustion, and exposure.[34]

Recently the US announced a new rule[35] which could soon begin collecting DNA samples from hundreds of thousands of migrants apprehended along the U.S.-Mexico border. This will dramatically expand a federal database of individual genetic information used by law enforcement.[36]

Lack of transparency and oversight of funding

One key area which PI has been exploring in relations to the role of industry in immigration and border management has been the transparency and oversight of funding enabling these public-private partnerships.

It is often public funds that drive the expansion of an industry to a specific sector and nowhere is this clearer at the moment than in the migration sector. The aforementioned EU Trust Fund for Africa uses currently funds numerous projects[37] including national biometric databases, surveillance equipment, such as IMSI catchers[38] and wiretapping equipment for border agencies in Niger, training on using surveillance technologies for authorities across Africa.[39] Besides supporting operations by border security forces, European countries also fund data

---

32 PI, "The Questions the New Company Vying for Border Dominance in the US Needs to Answer", 15 February 2019, https://privacyinternational.org/long-read/2731/questions-new-company-vying-border-dominance-us-needs-answer (accessed 19 March 2020).

33 Cat Zakrzewski, "The Technology 202: Trump Wants a Border Wall. One of His Biggest Supporters in Tech Is Expanding a Virtual One", *The Washington Post*, 5 February 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/02/05/the-technology-202-trump-wants-a-border-wall-one-of-his-biggest-supporters-in-tech-is-expanding-a-virtual-one/5c5884b71b326b66eb098610/ (accessed 19 March 2020).

34 Samuel Norton Chambers, Geoffrey Alan Boyce, Sarah Launius and Alicia Dinsmore, "Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence", *Journal of Borderlands Studies* (2019), https://doi.org/10.1080/08865655.2019.1570861 (accessed 19 March 2020), pp 1–26.

35 https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-04256.pdf

36 U.S. immigration authorities will collect DNA from detained migrants

37 Resources currently allocated to the EU Trust Fund for Africa as of July 2019 amount to EUR 4.6 billion including more than EUR 4.0 billion from the European Development Fund(EDF),the EU's main instrument for development aid, the Development Cooperation Instrument(DCI), and the European Neighbourhood Instrument(ENI),funding from the Directorate General (DG) for Migration and Home Affairs and DG European Civil Protection and Humanitarian Aid Operations(ECHO). EU Member States and Norway and Switzerland have so far contributed EUR 526 million.

38 PI, "Explainer – IMSI Catcher", https://privacyinternational.org/explainer/2222/imsi-catchers (accessed 19 March 2020).

39 PI, "The EU Funds Surveillance Around the World: Here's What Must Be Done About It", 18 September 2019, https://privacyinternational.org/long-read/3221/eu-funds-surveillance-around-world-heres-what-must-be-done-about-it (accessed 19 March 2020).

collection systems.[40] These processes are conducted without the levels of transparency and oversight required.[41]

2. Discriminatory Impacts Arising from Use of Digital Technologies in the Context of Border Enforcement and Administration

The discriminatory impacts of digital technologies from biometrics, facial recognition to social media monitoring, amongst others are already well documented, and in a context of border and administration where people and communities are in the most vulnerable and marginalised positions the risks of discrimination, surveillance and exploitation are heightened. We have already hinted to some of the discriminatory impacts from the use of digital technologies above. The following section adds some further context.

From failures of biometric identity systems to inaccurate digital data trails and flawed profiling to discriminatory automated-systems, it is concerning that increasingly these mechanisms are used to make life-changing decisions about refugees, migrants, stateless people, non-citizens, and citizens perceived or treated as foreign without much consideration to the curtailment of fundamental rights and freedoms.

Building on some of the digital technologies deployed in border enforcement and administration outlined above, here are a variety of ways in which refugees, migrants, stateless people, non-citizens experience discrimination, are being profiled, and exposed to data exploitation and surveillance.

2.1. Legality, necessity and proportionality

One of our mains concerns is whether the use of the digital technologies presented in the first part of this submission is in accordance with law and to what extent their use is necessary and proportionate to the aims pursued by their deployment.

Under international human rights law, any interference with the right to privacy must be prescribed by law and must meet the principles of necessity and proportionality to safeguard against arbitrary interferences which undermine democracy and people's fundamental rights.

However, many of the above policies and practices often are often opaque and not subject to democratic scrutiny and oversight. In many cases this is often because governments deem immigration enforcement as being exempted from regulatory and legal obligations as they are seen as matters of national security. Furthermore, combined together these factors this means that there is a high potential for abuses and miscarriages of justice while access to remedies and redress is increasingly difficult.

---

[40] G. Zandonini, PI, "The European chase of Saharan smugglers", https://privacyinternational.org/long-read/3347/european-chase-saharan-smugglers (accessed on 07 May 2020)

[41] The European Court of Auditors has found that, while it is a flexible tool for providing assistance, its objectives are too broad, and the Commission has failed to appropriately measure the extent to which it has met its objectives. Further, the Fund lacks key transparency and oversight mechanisms because the European Parliament is only currently an "observer", European Court of Auditors, EU trust fund for Africa: flexible emergency tool, but lacking focus, 5 December 2018, https://www.eca.europa.eu/en/Pages/NewsItem.aspx?nid=11356 (accessed 14 May 2020).

2.2. *Discrimination*

Not only are such surveillance and data-driven immigration policies leading to discriminatory treatment of people and undermining peoples' dignity, but technological flaws also risk resulting in unfair and often erroneous decision making, particularly when automated.

The EU is moving towards the mandatory profiling of all 'regular' migrants, through upgrades to its visa processing database (the Visa Information System, VIS) and the introduction of a new European Travel Information and Authorisation System (ETIAS), akin to the US ESTA system. The profiling tools foreseen for both systems will work in the same way: statistics and information from EU and national authorities will be used to generate 'risk indicators' based on factors such as age range, sex, nationality, place of residence, countries being visited, level of education, purpose of travel and/or occupation.

The United Kingdom's 'hostile environment' for immigrants amounts most to devolving the requirement for asking for identity and status verification, away from the state to employers, landlords, and creating data-sharing initiatives for the immigration department with schools and health practitioners.[42]

2.3. Misinformation, stigmatization, and harassment of migrant rights defenders and journalists

Migrant rights groups in Mexico have reported the use of digital technologies to spread misinformation that stigmatizes migrants as criminals or carriers of diseases[43], including COVID-19. The stigmatization that coordinated digital misinformation campaigns has created, increases hostility towards migrants, including the risk of violence against them.

There are increasing reports of harassment against migrant rights defenders and journalists covering migrant caravans in Central America, Mexico and the United States, including digital threats, searches of digital devices[44] and even electronic surveillance[45] by authorities in the U.S. and Mexico.

3. Conclusion

[42] Privacy International, "Privacy International is joining migrant organisations to challenge the UK's "immigration control" data protection exemption - find out why!", https://privacyinternational.org/news-analysis/3064/privacy-international-joining-migrant-organisations-challenge-uks-immigration, 10 July 2019 (accessed on 13 May 2020)

[43] Diario de Chiapas. Peligroso foco rojo: Bomba de tiempo los migrantes asentados en Tapachula ante el coronavirus. April 28, 2020. Available at: https://diariodechiapas.com/opinion/peligroso-foco-rojo-bomba-de-tiempo-los-migrantes-asentados-en-tapachula-ante-el-coronavirus/123218

[44] See Frontline Defenders, Red TDT, LIS-Justicia en Movimiento & PRAMI-Universidad Iberoamericana. Defenders beyond borders: migrant rights defenders under attack in Central America, Mexico and the United States. September 2019. Available at: https://www.frontlinedefenders.org/sites/default/files/frontline_defenders_mexico_english_v2.pdf

[45] NBC-Channel 7. Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database. March 2019. Available at: https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438/

As outlined in our submission, an array of digital technologies being deployed in the context of border enforcement and administration and yet this is happening with little public scrutiny, often in a regulatory or legal void and without careful understanding and consideration to the impact on migrant communities at the border and beyond.

The above situation is having a huge impact on migrants through surveillance and data-driven immigration policies leading to discriminatory treatment of people and undermining peoples' dignity. These practices mean that migrants are bearing the burden of the new systems and losing agency in their migration experience, particularly when their fate is being put in the hands of systems driven by data processing and tech innovation. There is a need to demand a more humane approach to immigration based on the principles of fairness, accessibility, and respect for human rights.

We appreciate the intention of the UN Special Rapporteur on contemporary forms of racism, xenophobia and related intolerance to explore these issues further and we are looking forward continuing to engage with the UNSR on this and other processes to ensure we are all free to be human.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321

privacyinternational.org