Privacy International's response to the call for input for the UN Secretary-General's report on the human rights of migrants

26 May 2023

1. Introduction

Privacy International (PI)[1] welcomes the opportunity to provide input to a report by the UN Secretary General (UNSG) on the human rights of migrants (the Report). We note that the Report will cover all aspects of the UN General Assembly Resolution on the protection of migrants (A/RES/76/172) dated 16 December 2021 (the Resolution).

Our input focus on the use of digital technologies in the context of border governance. This is an issue PI and our global partners have been exploring for many years with a particular focus on how these developments are impacting the rights of migrants.[2]

In particular, the submission focuses: first, on the ways in which states are adopting data-intensive ID systems; second, on the adoption by national immigration enforcement agencies of other privacy-intrusive modes of surveillance and control, including tracking by way of 24/7 Global Positioning System (GPS) technology and mobile device data extraction; third, on how the intensification of border surveillance technologies facilitate further human rights violations; fourth, on the impact of border externalisation and transfer of surveillance capabilities to other countries; fifth, on access to existing databases for other purposes and mission creep; and finally, on the increasing dependency on private companies to perform migration and border management duties.

We recommend that the upcoming Report of the Secretary General on the rights of migrants:

[1] Privacy International (PI) is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.[1] PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and the UN Refugee Agency.

[2] See PI, "Migration and Borders", https://privacyinternational.org/learn/migration-and-borders; PI, "Demand a Humane Approach to Immigration", https://privacyinternational.org/what-we-do/demand-humane-approach-immigration

1. Examines the use of new and emerging technologies at borders and assesses their implications for the human rights of migrants;
2. Adopts a wide approach to the understanding of borders, taking into account considerations about border externalisation and border digitalisation;
3. Urges states to ensure that the deployment of digital technologies to manage migration occurs strictly in accordance with human rights standards, including the rights to privacy and data protection of migrants;
4. Recommends on states to ensure that their use of digital technologies in border enforcement and administration does not results in exclusionary and discriminatory impacts on migrants;
5. Urges states to cease using intrusive surveillance technologies, such as GPS tags and mobile phone extraction, in violation of the principles of legality, necessity and proportionality against migrants;
6. Urges states to systematically conduct human rights due diligence, including regular comprehensive human rights impact assessments, when designing, developing, purchasing, deploying, and operating existing and emerging technologies for migration and border control purposes;
7. Calls on states to ensure that all projects financing border externalisation are carried out in accordance with international human rights standards, and that human rights impact assessments are conducted prior to the approval of any project;
8. Recalls the responsibility of all business enterprises to respect human rights, and states' duty to protect human rights even when outsourcing surveillance and border control functions to the private sector;
9. Requires that a public private partnership collaboration is carried out in accordance with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights;
10. Calls on states to separate national immigration enforcement and administration from the delivery of essential services to enable a truly migrant-inclusive, non-discriminatory social protection system.

1. Data intensive registration and identification systems and their impact on migrants

Governments around the world are using migrants as the testing ground for the mass deployment of novel technological innovations including the adoption of digital registration and identification systems, which among others record and store data relating to people's immigration status. They commonly function by assigning a card with a unique identifier to migrants (often using biometric data)[3] and requiring identity authentication within the system in order to access public services, employment, and participate in civic spaces.

These systems are increasingly digital-only. By way of an example: the UK's European Union Settlement Scheme ("EUSS") requires individuals to input biometric facial imaging data together with personal data including date of birth, details of identification

[3] PI, "A Guide to Litigating Identity Systems: Biometrics" (2020) https://privacyinternational.org/report/4157/guide-litigating-identity-systems-biometrics

documents from the country of origin, and personal contact information (such as telephone numbers and email addresses)[4]. Providing this data is both a requirement to secure immigration status in the UK, following the exit from the EU, and to prove one's status to employers and landlords in order to access work and housing, for example. An individual's status is provable by way of an automatically generated "share code" that can be provided to the landlord and/or employer charged with verifying whether they have leave to remain in the UK[5]. With little or no legislative scrutiny, this digital infrastructure has since been extended to other forms of immigration status in the UK[6].

PI has drawn attention to these developments in a number of previous submissions to the UN High Commissioner for human rights, including our response to the call for input to a report on the right to privacy in the digital age as part of our broader work on the deployment of digital identification systems[7]. Through this work we have identified at least two key problematic features in the functionalities and implementations of these systems relating to the human rights of migrants. Firstly, they frequently perpetuate the existing exclusion of certain individuals and communities, in direct contradiction to their stated purposes and with discriminatory outcomes. Secondly, the systems pave the way for surveillance and unlawful exploitation and processing of sensitive personal data with significant implications for the fundamental rights of individuals and communities in particular communities at increased risk of being monitored and surveilled such as migrants. This is particularly the case in, but not limited to, contexts where there are no or weak legal and regulatory frameworks to protect people and their rights such as data protection laws.

The below information and analysis remain grounded in these two issues and build on earlier submissions. It further underlines novel evidence arising from PI's work,[8] as well that

[4] UK, "View and prove your immigration status: get a share code" https://www.gov.uk/view-prove-immigration-status.
[5] Ibid.
[6] Jablonowski K., "Digital Immigration Status: from Logics of Inscription to Logics of Control" in Lessard-Phillips, L., Papoutsi, A., Sigona, N., and Ziss, P. (eds), Migration, Displacement and Diversity: The IRiS Anthology. Oxford Publishing Services, 2023.
[7] PI, "Response to the Call for Input to a Report on the Right to Privacy in the Digital by the UN High Commissioner for Human Rights" (June 2022) https://privacyinternational.org/sites/default/files/2022-06/PI%20submission%20to%20OHCHR%202022%20report%20final.pdf
[8] See PI, "Privacy International Participates in Global Virtual Summit on Digital Identity for Refugees" (2019) https://privacyinternational.org/node/2994; PI, "The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change" (2021) https://privacyinternational.org/long-read/4651/eu-externalisation-migration-control-and-id-systems-heres-whats-happening-and-what; Privacy International's contribution to Global Virtual Summit on digital identity (April 2019) https://privacyinternational.org/sites/default/files/2019-05/Global%20Virtual%20Summit%20submission-%20Privacy%20International.pdf

of its global partners[9] and other CSOs,[10] to document the impact of registration and identification systems on the rights of migrants.

The exclusionary impacts on migrant populations of identification systems

As our global partners in Colombia, Dejusticia and Fundacion Karisma, have noted in their respective submissions to the UN's Special Rapporteur on the Human Rights of Migrants, Colombia's new regularisation scheme is preventing some Venezuelan migrants from being granted immigration status in the country[11].

In 2021, the Colombian Ministry of Foreign Affairs created the Temporary Protection Statute for Venezuelan Migrants (ETPMV), empowering the state to create a scheme for the registration and identification of migrants from Venezuela. Registration under the scheme is a requirement in order to receive a residence permit, the Temporary Protection Permit (TPP), which authorises the person who bears it to reside in the country for 10 years, and to access the work, health, pension, education, and financial systems. The scheme excludes several Venezuelan migrants from registering despite their physical presence in Colombia and the stated purpose of the ETPMV and TPP if they do not comply with the requirements established in Article 4 of Decree 216 of 2021. For example, the scheme's enabling power prohibits the registration of Venezuelan migrants who arrived in the country via irregular means after February 1, 2021[12].

In line with paragraph 11(g) of the Resolution, which urges states to combat discrimination against all migrants, PI submits that these practices risk direct and indirect discrimination including based on immigration status contrary to national and international human rights laws enshrining the principle of non-discrimination. Not only is differential treatment built into the identification scheme, it also risks further discriminatory consequences after the point at which an individual is no longer able to register. Access to healthcare and other essential services will be conditional on migrants submitting their biometric data to the state as required by the registration scheme. The collection of such data raises additional

[9] PI, "When ID leaves you without identity: the case of double registration in Kenya" (2021) https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya; Karisma, "Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos" (2021) https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/; Dejusticia, Karisma, "Lo que no puede quedar por fuera del Estatuto Temporal de Protección para personas migrantes venezolanas" (2021) https://www.dejusticia.org/lo-que-no-puede-quedar-por-fuera-del-estatuto-temporal-de-proteccion-para-personas-migrantes-venezolanas/; EDRi, "Technologies for border surveillance and control in Italy" (2022) https://edri.org/our-work/technologies-for-border-surveillance-and-control-in-italy/

[10] HRW, "UN Shared Rohingya Data Without Informed Consent" (2021) https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

[11] Dejusticia, "Response to the Questionnaire from the Special Rapporteur on the Human Rights of Migrants" (February 2023) https://www.ohchr.org/sites/default/files/documents/issues/migration/cfis/regularization/submissions-regularization-dejusticia.pdf; Fundación Karisma, Response to the Questionnaire from the Special Rapporteur on the Human Rights of Migrants (February 2023) https://www.ohchr.org/sites/default/files/documents/issues/migration/cfis/regularization/submissions-regularization-fundacion-karisma.docx

[12] Dejusticia, "Response to the Questionnaire from the Special Rapporteur on the Human Rights of Migrants" (February 2023) https://www.ohchr.org/sites/default/files/documents/issues/migration/cfis/regularization/submissions-regularization-dejusticia.pdf

concerns about the exploitation of sensitive personal data – as detailed further in the following section - in particular given that the data processing for the ETPMV and TPP are occurring in a legal void.[13] Furthermore as noted by Dejusticia, the individuals who are likely to be excluded from registration are usually in positions of greater vulnerability through lack of access to the necessary technology or information[14].

The above example demonstrates the risk of the introduction of such systems without necessary steps to rectify the previous failures of identification schemes for migrant populations – in particular that the introduction of such systems without adequate infrastructure and safeguards is likely to have catastrophic consequences for large numbers of vulnerable individuals.

Data protection and the mass processing of sensitive data through identification systems

The risks inherent to the introduction of data-intensive, digital identification systems, which frequently rely on algorithmic and automated decision making, are also that systemic deficiencies will be replicated across databases with implications for data privacy and other fundamental rights and freedoms. These risks run in parallel and interrelate with the dynamics of exclusion set out above. As above, these risks are particularly pronounced in states with limited or no data protection standards and other relevant laws and regulations, nevertheless there are also documented issues in states with data protection regulations and infrastructures to enforce them.

For example, we have concerns as regards the capacity of digital identification systems to ensure the accuracy of the personal data that they hold. In respect of the biometric data sharing program between the governments of Mexico and the US, a report of the US's Department of Homeland Security found errors in 825,000 entries in a border crossing database[15]. Given the significant legal effects that could result from false identification on such a database, failures to maintain accurate data engages other fundamental freedoms such as the right to liberty and security or freedom of movement. The potential for inconsistencies and inaccuracies to stem from the automated processing of personal data raises additional issues. In the case of the EUSS, mentioned above, the scheme "*is comprised of several databases and algorithmic logics that determine which personal data and what immigration status is displayed during a check*"[16]. Several errors have been identified since the commencement of the digital only status, with the consequence that non-British citizens were left unable to prove their lawful immigrations status[17]. If algorithms are employed without additional human scrutiny, and immigration administration bodies

[13] ibid; Karisma, "Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos" (2021) https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/
[14] ibid.
[15] PI, "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) https://privacyinternational.org/sites/default/files/2020-06/PI%27s%20joint%20UN%20submission%20on%20race%20border%20tech_final.pdf
[16] Jablonowski, K., Digital Immigration Status: from Logics of Inscription to Logics of Control (2023), supra.
[17] Ibid.

continue to collect and retain sensitive personal data in large-scale identification systems, such issues are likely to persist if not amplified.

There are also concerns with such identification databases being used for other purposes beyond migration management in contravention of fundamental human rights of migrants and others. For example, as documented by our global partners Hermes in Italy where biometric data collected during disembarking operations or at the time of arrival of migrants on Italian territory are stored in a database (AFIS) that also contains data on potential criminal suspects. The same database is used to identify matches by the Italian National Police putting migrants at a higher risk of being wrongfully targeted by law enforcement authorities.[18]

Governments are not the only actors demanding and processing personal data of migrants, asylum seekers and refugees. Humanitarian and development agencies have long processed their personal data from enrolment/registration to identification and authentication.[19] There have been documented risks of how this data may be used by governments in ways that put individuals at risk have been exposed, for example in relation to data collected by UNHCR on Rohingyas refugees.[20] In the context of Kenya, there were thousands of Kenyan citizens stuck in legal limbo, unable to obtain national IDs because their fingerprints had been captured in refugee databases.[21]

2. The adoption of privacy-intrusive policies by immigration authorities

In addition to the constellation of issues surrounding border externalisation, we note with concern that borders are no longer physical only, and now extend inwards into the wider management of immigration enforcement by governments. National immigration enforcement bodies are for example turning to invasive forms of technology to track and profile migrants. We have observed that such practices are impacting particular groups of migrants – including persons coming to seek asylum and non-citizens who have previously committed criminal offences.[22] Such mechanisms of surveillance have the potential for function creep and are often resulting in serious mental health consequences for those subjected to them.

---

[18] Hermes, "Technologies for Border Surveillance and Control in Italy Identification, Facial Recognition, and European Union Funding" (2021) https://www.documentcloud.org/documents/21200979-technologies-for-border-surveillance-and-control-in-italy-identification-facial-recognition-and-european-union-funding?responsive=1&title=1

[19] PI, "Privacy International's contribution to Global Virtual Summit on digital identity" (2019) https://privacyinternational.org/sites/default/files/2019-05/Global%20Virtual%20Summit%20submission-%20Privacy%20International.pdf

[20] HRW, "UN Shared Rohingya Data Without Informed Consent" (2021) https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

[21] Weitzberg, K., "In Kenya, thousands left in limbo without ID cards", Coda Story, 13 April 2020, https://www.codastory.com/authoritarian-tech/kenya-biometrics-double-registration/; PI, "When ID leaves you without identity: the case of double registration in Kenya" (2021) https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya

[22] UK Home Office, Immigration bail Version 15.0 (2023) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1132640/Immigration_bail.pdf

While the examples raised above in relation to the data intensive ID systems and spreading of surveillance technologies outside the borders are also examples of this phenomenon, hereinafter, we focus on two examples of this phenomenon which PI has actively sought to document, research, and challenge – namely GPS monitoring of migrants and the extraction of data from mobile devices seized from migrants.

GPS monitoring and the surveillance of migrants

In the UK, the Home Office has recently introduced highly-intrusive Global Positioning System (GPS) devices[23], which monitor an individual's location 24/7 in real time, to monitor migrants.[24] In June 2022, the UK authorities announced a pilot policy to tag non-offenders who claimed asylum after having entered the UK via "dangerous and irregular routes"[25]. As the "regular" routes to seeking asylum in the UK have been virtually annihilated,[26] this means virtually any asylum seeker can be subject to tagging.

Until November 2022, the devices were all non-removeable ankle tags. However, since then the UK authorities have begun to roll out devices that are not attached to the individual but must be carried by the person at all times.[27] These new devices require the individual to input biometric fingerprint data upon random requests, up to five times a day.

PI is concerned about the deployment of increasingly intrusive surveillance technologies on migrant populations once they cross national borders. In the UK's case, GPS tracking is far more invasive than previous tracking methods as it constantly collects and retains personal locational data rather than assessing whether an individual is present or absent from a certain location. This invasive practice is currently subject to complaints and legal claims for breach of public law, human rights and data protection laws.[28]

In the US, immigration authorities are deploying analogous GPS tracking programmes, which also use both ankle devices and hand-held ones that incorporate biometric scanners.[29] As of April 2022, 216,000 migrants were subject to such conditions despite the

[23] PI, "Electronic monitoring using GPS tags: a tech primer" (2022) https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer

[24] The Home Office has used electronic monitoring (EM) to track migrants since 2004. An EM condition can be imposed on anyone in the UK on immigration bail, which is granted to migrants who are not in immigration detention and who do not have leave to remain in the UK https://www.legislation.gov.uk/ukpga/2004/19/section/36;

[25] UK Home Office, "Immigration bail conditions: Electronic monitoring (EM) expansion pilot" (2022) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082956/Immigration_bail_conditions_-_Electronic_Monitoring__EM__Expansion_pilot.pdf

[26] UNHCR UK, "UK asylum and policy" (2023) https://www.unhcr.org/uk/uk-asylum-and-policy

[27] UK Home Office, Immigration bail Version 15.0 (2023) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1132640/Immigration_bail.pdf

[28] PI, "Challenge to the UK's GPS tagging of migrants", https://privacyinternational.org/legal-action/challenge-uks-gps-tagging-migrants; Lewis D., "Permission to Apply for Judicial Review Granted for Duncan Lewis Challenge to GPS tracking by the Home Office" (2023) https://www.duncanlewis.co.uk/news/Permission_to_Apply_for_Judicial_Review_Granted_for_Duncan_Lewis_Challenge_to_GPS_tracking_by_the_Home_Office__(31_March_2023).html

[29] Aguilera J., "U.S. Officials Deploy Technology to Track More Than 200,000 Immigrants, Triggering a New Privacy Lawsuit", Time, 18 April 2022, https://time.com/6167467/immigrant-tracking-ice-technology-data/.

presence of other means of maintaining contact with migrants including reporting requirements.[30]

Both in the UK and the US, the use of GPS tagging in immigration enforcement is said by governments to constitute a humane alternative to detention. However, research by civil society organisations has demonstrated that individuals experience tagging as akin to imprisonment and a form of psychological torture.[31] In light of the serious implications for the wearers' mental state and the possibility of furthering immigration control purposes by less intrusive means, we believe that the deployment of blanket 24/7 GPS surveillance on migrants constitutes a breach of the right to privacy.

Phone seizures and data extraction

Increasingly public authorities have been (or have until recently been) operating phone seizure and data extraction policies in relation to asylum seekers who are deemed to be arriving in the country via "irregular means".[32] The concerns we have with the adoption of such surveillance practices are very similar to the issues we have identified in relation to the ongoing use of GPS tracking on migrants. These technologies increasingly available to border officials are extremely intrusive.[33] They enable the authorities to download an individual's contacts, call metadata, text messages, stored files (such as photos and videos), location data, and many other types of intimate and sensitive data. Individuals are sometimes left without their phones, and hence without any contact with their families and friends, for months – and do not know what happens to their phones or the data extracted from them (sometimes they are not even informed that data will or can be extracted).

Moreover, the uses of this data by immigration enforcement bodies have gone far past the stated purposes of the policies without sufficient legal basis. In Germany, the policy permitted immigration officers to use extracted data for evidential purposes in asylum proceedings.[34] The assumption that obtaining data from digital devices leads to reliable evidence is flawed, even more in the case of asylum seekers: in the course of a long and dangerous trip, they may have swapped phones, they may have accessed certain sites or liked certain social media activity for a whole variety of reasons, and they may have been in touch with people whose name spelling appears on watchlists for a whole variety of reasons. A parliamentary inquiry found in relation to the German policy that the use of

[30] Ibid.
[31] BiD, Medical Justice & Public Law Project, "Every Move You Make: The Human Cost of GPS Tagging in the Immigration System" (2022) https://hubble-live-assets.s3.amazonaws.com/biduk/file_asset/file/682/GPS_Tagging_Report_Final.pdf
[32] PI, "At the border, asylum seekers are "guilty until proven innocent"" (2020) https://privacyinternational.org/long-read/3938/border-asylum-seekers-are-guilty-until-proven-innocent
[33] See PI, "Privacy International's submission to UNSR: "Human Rights Violations At International Borders: Trends, Prevention And Accountability" (2022) https://privacyinternational.org/advocacy/4931/privacy-internationals-submission-unsr-human-rights-violations-international-borders; Meaker M., "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
[34] Society for Civil Rights e.V. (Gesellschaft für Freiheitsrechte e.V.), "Refugee Phone Search", https://freiheitsrechte.org/en/themen/digitale-grundrechte/refugee-daten

mobile phone data rarely ever leads to adverse information being found.[35] The policy was challenged in court, which found the blanket phone seizure policy to be unconstitutional and in breach of the right to privacy.[36]

In the UK a similar policy was deployed between April and November 2020. The policy deployed compulsory searches, seizures, and data extraction in relation to asylum seekers who arrived in the UK on small boats. The policy was challenged, and the judgment held that the searches of migrants were proceeding without lawful basis and that the blanket and secret policy of seizing mobile phones constituted an interference with the right to private and family life as protected by Article 8 of the European Convention on Human Rights.[37] Despite these clear warnings about the human rights implications of a policy of discretionary or compulsory phone seizure, it appears to be continuing, including in countries such as Norway, the Netherlands, and Austria.[38]

3. Intensification of border surveillance measures without human rights safeguards

PI and its partners have documented an alarming increase in the use of surveillance technology by national bodies on physical borders and in frontier zones since the UN Secretary General's 2020 report on the human rights of migrants.[39] We note that this is a distinct, but interrelated, issue to the deployment of measures such as GPS monitoring and biometric identification systems that come into play once migrants have crossed physical borders. The mechanisms introduced make use of many different technologies and impact migrants with multiple different immigration statuses – including both individuals without regular status and those who have leave to remain in their host countries.

In its report titled "Technologies and Human Rights in the Triple Border Area", published on 1 February 2023, our partners, TEDIC (Paraguay) and Data Privacy Brazil Research Association documented the growing use of technologies to monitor borders in the Triple Border Area (TBA) between Argentina, Brazil, and Paraguay[40]. The report utilises case studies, including a project that deploys facial recognition technology (FRT) to control migration flows between Paraguay and Brazil (SMARF).

SMARF employs algorithms to match an individual's face to their immigration status. TEDIC documents show no human rights impact assessments were undertaken prior to the introduction of the scheme, and that the project lacks a privacy policy. The report also notes through interviews with border officials that the data collected by SMARF is retained

[35] *Ibid.*
[36] Delcker J., "German court rules search of refugee's phone was illegal", Deutsche Welle, 16 February 2023, https://www.dw.com/en/german-court-rules-that-search-of-refugees-phone-was-illegal/a-64685681
[37] R (on the application of HM, MA & KH) v Secretary of State for the Home Department [2022] EWHC 695 (Admin)
[38] Palmiotto Fr. and Ozkul D., "Like Handing My Whole Life Over" The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures", Verfassungsblog, 28 February 2023, https://verfassungsblog.de/like-handing-my-whole-life-over/
[39] UNHRC, "Report of the Secretary-General on human rights of migrants" (A/HRC/45/30), 03 September 2020 https://www.ohchr.org/en/documents/reports/human-rights-migrants-report-secretary-general
[40] TEDIC, "Technologies and Human Rights in the Triple Border Area: An exploratory Study in the Security Programmes Muralha Inteligente (Brazil) and the Automated Migratory System for Facial Recognition" (1 February 2023) https://www.tedic.org/wp-content/uploads/2023/02/Technologies-and-Human-Rights-in-the-Triple-Border-Area.pdf

in a database without accompanying data protection safeguards on how long it can be retained, and without a comprehensive data protection law in place that could guide public institutions on a set of minimum standards.

Furthermore, in a context of algorithmic management of data and the operation of data sharing with law enforcement bodies, there are insufficient safeguards "*in how these automated systems can impact vulnerable communities, such as racial and ethnic minorities, LGTBQI+ groups, and others*"[41]. An emphasis on "techno-solutionism" and efficiency appears to be at the forefront of how these systems are being framed, discussed, and understood. Such discourses are at odds with a risk-centred approach that could in turn foster the adoption of data protection and human rights safeguards in the use of technologies such as FRT at the border.

4. Border externalisation and surveillance technologies in migration management

PI has undertaken research and legal action in relation to the provision and funding of intrusive surveillance technologies as part of border externalisation initiatives by both national and intergovernmental bodies, including the European Union (EU).[42] Our investigations have shown that several foreign aid schemes, including the EU Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa (EUTF), involve the transfer of surveillance capabilities to partner countries.[43] This also links to our above evidence regarding the establishment of biometric identification schemes given that the funding initiatives and transfers of surveillance capabilities were in part designated for the establishment of exactly such programmes.

In particular, we have found that funding through the EUTF was directly allocated to supporting the acquisition by non-EU member states of surveillance technologies whose purpose was wholly or in part to track migrants, such as surveillance drones, cameras and software, wiretapping centres, or IMSI catchers in Niger.[44] The EUTF also provided funding and equipment for the establishment of national biometric-based identification schemes. This infrastructure would also facilitate the returns from the EU of migrants. The transfers of surveillance infrastructure at the heart of the complaint were often reliant on public-private partnerships with lucrative contracts given to European security and technology firms.[45] Finally, there are links between the funding and infrastructure provided and violations of human rights and data protection standards carried out by authorities of the receiving countries. Despite obligations under EU law for EU bodies to promote and

[41] Ibid.
[42] PI, "Challenging Drivers of Surveillance", https://privacyinternational.org/challenging-drivers-surveillance
[43] PI, "Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes" (2020) https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes
[44] "IMSI" stands for "International Mobile Subscriber Identity", a number unique to each SIM card. Once a phone is tricked into connecting to an IMSI catcher, it reveals this unique number. Once the police have it, they can easily determine the phone holder's identity. PI, "Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls" (2020) https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border
[45] PI, "Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds" (2020) https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

safeguard human rights and the rule of law in all their dealings with third countries, the relevant institutions involved failed to carry out any (or did so in an inadequate way) human rights impact assessments, including data protection impact assessments.[46]

Our investigations culminated in a joint complaint to the European Ombudsman (the Ombudsman) in respect of the EUTF and several other EU foreign aid programmes[47]. On 28 November 2022, the Ombudsman upheld the complaint in a decision that found that "*the Commission was not able to demonstrate that the measures in place ensured a coherent and structured approach to assessing the human rights impacts*". The Ombudsman recommended that the European Commission now require that an "*assessment of the potential human rights impact of projects be presented together with corresponding mitigation measures.*"[48]

PI, together with other civil society organisations, filed similar complaints against European External Action Service (EEAS) and Frontex leading the Ombudsman to open additional inquiries, in relation to their compliance with human rights standards when providing among others technical assistance provided to non-EU countries, such as training in surveillance techniques and the provision of surveillance equipment and other related support[49]. The complaint questioned amongst others the training support that the Libyan General Administration for Coastal Security (GACS) has received on maritime law enforcement in the Central Mediterranean Sea. Shortly after opening of the inquiry, a Human Rights Watch (HRW) Report found that data collected by Frontex-operated drones and chartered aircraft rendered the agency complicit in maritime interceptions and human rights abuses perpetuated by the Libyan authorities.[50]

5. Access to data and mission creep risks for migrants' data

Another significant concern relevant to the use of digital technologies in the context of immigration enforcement and border management is the increasing re-purposing of the collected information through data-sharing arrangements in place within states and intergovernmental institutions. This phenomenon is not a new one and PI has been advocating against it for some time,[51] however as with many of the issues identified above,

[46] PI, Complaint to the European Ombudsman under Article 228 TFEU: EU Transfers of Surveillance Capabilities to Third Countries, submitted jointly with Access Now, Border Violence Monitoring Network, Homo Digitalis, the International Federation for Human Rights, and Sea-Watch, 19 October 2021, https://privacyinternational.org/sites/default/files/2021-10/21.10.19_EU_Ombudsman_Complaint_Final.pdf
[47] Ibid.
[48] European Ombudsman, Decision on how the European Commission assessed the human rights impact before providing support to African countries to develop surveillance capabilities (case 1904/2021/MHZ), 28 November 2022, https://www.ombudsman.europa.eu/en/decision/en/163491
[49] PI, "EU Ombudsman opens inquiries into FRONTEX and EEAS on their support to develop surveillance capabilities in non-EU countries" (2022) https://privacyinternational.org/press-release/4962/eu-ombudsman-opens-inquiries-frontex-and-eeas-their-support-develop-surveillance
[50] HRW, "EU: Frontex Complicit in Abuse in Libya - Aerial Surveillance Is Enabling Interceptions, Return of Migrants to Harm" (2022) https://www.hrw.org/news/2022/12/12/eu-frontex-complicit-abuse-libya
[51] See section "Challenge to data sharing between public authorities" in PI, "How Privacy and Data Protection Law Can Help Defend Migrants' Rights" (2022) https://privacyinternational.org/long-read/4790/how-privacy-and-data-protection-law-can-help-defend-migrants-rights

it has been accelerating in recent years as databases become increasingly interoperable and concerted efforts by authorities to achieve that.

For example, already in 2004, the European Asylum Dactyloscopy Database ("EURODAC") was established to facilitate the application of the Dublin Regulation, which determines the EU Member State responsible for examining an asylum application. In 2009, EU Member States proceeded to decide that EURODAC should made accessible for law enforcement purposes in order to fight terrorism, a purpose for which the data processed was never intended, as noted by the European Data Protection Supervisor ("EDPS") in its Opinion on the matter. The EDPS's opinion also raised that the use of EURODAC for law enforcement purposes, and specifically for terrorism, means that a particular vulnerable group in society, namely applicants for asylum could be exposed to further risks of stigmatisation, even though they are "not suspected of any crime" and "are in need of higher protection because they flee from persecution."[52]

In 2019, the EU Interoperability Regulations [(EU) 2019/817 and (EU) 2019/818)] formally established a framework for interoperability between EU information systems in the areas of police and judicial cooperation, asylum migration, borders and visas. Amongst others, the Interoperability Regulations result in the storage of personal and biometric data of all non-EU citizens who come to the EU to work, study, and seek asylum among other things – in three centralised databases[53]. One of the stated purposes of this centralisation relevant to border governance is the linking of law enforcement and immigration data in order to improve the EU's response to irregular migration and serious criminality, including terrorism.

Civil society organisations have advocated against this trend for various reasons, including that it is discriminatory as it only applies to non-EU citizens[54]; it unjustifiably conflates immigration and criminal law purposes[55]; and it may be incompatible with a number of data protection principles including data minimisation and purpose limitation[56]. This is because data initially gathered for one purpose (immigration administration) may then be used for another (law enforcement processing) in ways that are often unforeseeable to the individual in question.

In January 2023, the European Commission proposed an initiative to extend data interoperability through a "security information sharing system between frontline officers in the EU and key partner countries"[57]. As per PI's joint submission to the proposal's

[52] European Data Protection Supervisor, Opinions, C92/1, 5 September 2012, https://edps.europa.eu/data-protection/our-work/publications/opinions/establishment-eurodac-comparison-fingerprints_en
[53] PICUM, "How do the new EU regulations on interoperability lead to discriminatory policing?" https://picum.org/wp-content/uploads/2020/04/INFOGRAPHIC.-Interoperability-Systems-and-Access-to-Data_WEB_RGB.pdf
[54] Ibid.
[55] PICUM, Statewatch, "Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status", November 2019, https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf
[56] Ibid.
[57] European Commission, "Security-related information sharing - reciprocal access for frontline officers in the EU and key partner countries" (January 2023) https://ec.europa.eu/info/law/better-regulation/have-

consultation, one of the purposes of this further interoperability initiative is to facilitate increased police identity checks and to "*repurpose the data collected for other means such as readmissions and deportations*"[58]. There is currently no legal basis for such an extension of data-sharing, which would represent an extension of the ongoing trend of border externalisation.

For example, granting access to the EURODAC fingerprint database to Western Balkan states would facilitate removals of asylum seekers to such states, which have been designated as Safe Third Countries for the purposes of EU asylum law on the grounds that this was a fingerprinted person's first country of asylum. This is despite the fact that they have not yet met the requirements for accession to the EU including compliance with the Common European Asylum System (CEAS)[59]. Compliance with the CEAS entails states meeting minimum reception standards including in relation to the provision of housing, food, accommodation, clothing, healthcare, and education[60]. A report by Refugee Rights Europe documented illegal pushbacks to various Balkan states.[61] These highlight the risks of data sharing agreements facilitating the commission of further human rights abuses against migrants, including denial to access to essential services, right to seek asylum and eventually potential returns to their countries of origin where they would be put further at risk in violation of the non-refoulement principle.

Another example is the UK's Department of Education (DfE) sharing data from national pupil database with immigration enforcement. In 2018 it began collecting data for the schools' census. The collection of children's data recorded in the national pupil database and including details such as age, address, and academic achievements. The DfE had allegedly abandoned that policy, but in January 2019, it admitted to continuing storing the data it had collected, and sharing the census data with immigration enforcement every month since 2015[62]. During the COVID-19 pandemic, PI found that these data sharing practices had a chilling impact on migrants accessing healthcare services, despite the UK's National Health Service (NHS) announcing that it would not share vaccination data with immigration enforcement[63].

---

your-say/initiatives/13243-Security-related-information-sharing-%E2%88%92-reciprocal-access-for-frontline-officers-in-the-EU-and-key-partner-countries_en

[58] PI, "Joint Submission to European Commission on cross-border sharing of data for mixed criminal law and immigration control purposes", submitted together with Border Violence Monitoring Network (BVMN), Statewatch, Euromed Rights, European Digital Rights (EDRi), Access Now, Refugee Law Lab (York University), Homo Digitalis and the Platform for International Cooperation on Undocumented Migrants (PICUM) (30 March 2023) https://privacyinternational.org/advocacy/5055/joint-submission-european-commission-cross-border-sharing-data-mixed-criminal-law-and

[59] Ibid.

[60] European Commission, Migration and Home Affairs, "Common European Asylum System", https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system_en

[61] Refugee Rights Europe, "Limits to access to Asylum along the Balkan Route" (2020) https://refugee-rights.eu/wp-content/uploads/2020/07/RRE_LimitedAccessToAsylumAlongTheBalkanRoute.pdf.

[62] PI, "UK Deparment of Education shares pupil data with immigration enforcement" (2019) https://privacyinternational.org/examples/3152/uk-deparment-education-shares-pupil-data-immigration-enforcement

[63] Gayle, D. "Schools census used to enforce immigration laws, minister says", The Guardian, 13 January 2019, https://privacyinternational.org/news-analysis/4424/hostile-environment-incompatible-public-health-pi-joins-vaccine-all-campaign

6. The role of private sector and regulation of public private partnerships

As exemplified in various of the above provided examples, states increasingly rely on the private sector to develop and implement technologies for migration management. For instance, in the above-mentioned Human Rights Watch report on drones operated by the European Border and Coast Guard Agency (Frontex) in Libya above, it is noted that the aircraft transmitting live data to Frontex is operated by private companies.[64]

PI and its partners have documented several cases where public authorities (including police forces, but also national and local authorities) partner with private companies in order to expand their surveillance capabilities and process mass quantities of personal data (including often biometric data, such as facial images).[65] These public private partnerships are taking on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services.

For instance, while governments bear the primary responsibility for the setting up of digital ID systems, private companies play a significant role in implementing these systems, not only by providing the relevant technologies, but by setting up and managing databases of whole populations. Notably, in December 2016 the French company Civipol was chosen to set-up databases to fingerprint everyone in Mali and Senegal. Going beyond fingerprinting, it is one of the two companies that are building a full biometric ID-system in Senegal. It also implements a similar project in Côte d' Ivoire. These projects are financed by the EU Trust Fund for Africa.[66] Resulting public private partnerships can introduce vast biometric programs, which are often developed without adequate due diligence and prior human rights impact assessments, including data protection ones.[67]

Similarly, there is a growing reliance by state authorities on the services offered by data analytics companies, which provide analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights, and thereby inform public decision-making. While per se data analytics tools do not necessarily raise human rights concerns, the way they are used do so. PI has raised concerns about data analytics practices, by companies such as Palantir, whose tools may pose a real danger to people in vulnerable positions such as at international border crossings.[68] Likewise, PI noted in previous submissions how Anduril, an American defence company specialising in

[64] HRW, "EU: Frontex Complicit in Abuse in Libya - Aerial Surveillance Is Enabling Interceptions, Return of Migrants to Harm" (2022) https://www.hrw.org/news/2022/12/12/eu-frontex-complicit-abuse-libya

[65] PI, "Public-Private surveillance partnerships", https://privacyinternational.org/learn/public-private-surveillance-partnerships

[66] PI, "Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds" (2020) https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

[67] PI, "Safeguards for Public-Private Surveillance Partnerships", https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[68] PI, "Who supplies the data, analysis, and tech infrastructure to US immigration authorities?" (2018) https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities

autonomous systems, had been contracted to expand the US's digital border security system on the US-Mexican border.[69]

Based on the United Nations Guiding Principles on Business and Human Rights, PI developed a set of safeguards for states and companies to mitigate the risks of human rights abuses resulting from PPPs that rely on the processing of personal data.[70] Such safeguards are particularly important in the case of migrants where (a) they are frequently in a position of vulnerability and (b) companies are increasingly developing and operating advanced surveillance technologies with public functions, without the same accountability under international law.

[69] PI, "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 (March 2020) https://privacyinternational.org/sites/default/files/2020-05/2020.3%20PI%20submission%20UN%20WG%20mercenaries.pdf

[70] PI, "Safeguards for Public-Private Surveillance Partnerships", https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships