ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Photo by Darko M. on Unsplash

PRIVACY INTERNATIONAL'S SUBMISSION ON HUMAN RIGHTS VIOLATIONS AT INTERNATIONAL BORDERS: TRENDS, PREVENTION AND ACCOUNTABILITY

International (PI) welcomes the call of the Special Rapporteur on the human rights of migrants to assess the human rights impact of current and newly established border management measures with the aim of identifying effective ways to prevent human rights violations at international borders, both on land and at sea.

The issues highlighted in the call for submissions are ones that PI has been investigating, reporting and monitoring as part of our campaigns demanding a human rights approach to migration[1] and challenging the drivers of surveillance[2] amongst other domains of work that PI has focused to expose corporate and government data exploitation and surveillance. This work aligns with the UNSR's recent set of recommendations for "the development of a human rights-based, gender-responsive, age- and child-sensitive approach to migration and border governance, that ensures the human rights of migrants, including those in an irregular situation, are always the first consideration".[3]

This submission introduces some of the key developments we have been researching and reporting in the United Kingdom (UK). The issues raised and examples presented provide an

[1] PI, Protecting Migrants at Borders and beyond, https://privacyinternational.org/protecting-migrants-borders-and-beyond (accessed 3 March 2022).
[2] PI, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance (accessed 3 March 2022).
[3] A/HRC/47/30

insight into trends which we have observed on a global level around the deployment of data-intensive and technologies at the border and in immigration enforcement which we would encourage the UN Special Rapporteur to investigate further.

Recommendations

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

- Analyse and assess existing regulation and governance of digital technologies deployed in the context of immigration enforcement and border enforcement and administration, asylum and other international protection procedures for non-nationals including exploring:
    - how and if such technologies are being deployed in accordance with human rights standards, in compliance with a legal framework, appropriate safeguards, and are subject to effective oversight and remedial mechanisms;
    - the discriminatory impact associated with the deployment of new technologies in particular on marginalised communities and people in vulnerable situations.
- Review and assess the lawfulness of the practices such as the seizure and extraction of data from the phones of migrants and whether there are appropriate safeguards in place.
- Review the collection and use of location data, gathered as a result of the use of GPS tracking tags for immigration bail purposes, in particular measures such as those in place in the in the United Kingdom including:
    - whether the imposition of 24/7 location tracking for immigration bail, which facilitates live location tracking and historical location tracking for up to six years after the tag is removed, is in accordance with human rights standards;
    - how and if the use of location data gathered via the imposition of GPS tags, for immigration decision making, is in accordance with human rights

standards, in compliance with a legal framework, appropriate safeguards are in place and is subject to effective oversight and remedial mechanisms;

- Explore and assess the legality, proportionality and necessity of the use of aerial surveillance of borders as a means to track and monitor migrants arriving by sea in the context of border enforcement.

INTRODUCTION

To respond to migration flows – voluntary or forced – governments worldwide have prioritised an approach to immigration that criminalises the act of migration and focuses on security with the aim of controlling, reducing, or preventing entry into their borders and then subjecting to surveillance measures migrant and refugee populations living on their territory. Increasingly these approaches have been formalised and coordinated as part of a broader strategy to digitise immigration enforcement and border management.[4]

Digital technologies deployed in the context of border enforcement and administration and immigration enforcement reproduce, reinforce, and compound existing human rights violations.[5] Large amounts of data are being requested from migrants, from their fingerprints to their digital data trails, while they are often put in a situation of constant surveillance, to identity their credibility and worthiness, and to monitor, track, and profile them. Life-changing decisions are being made based on the data being collected but also inferred and observed, and yet there are limited safeguards in place to regulate and

[4] PI, Demand a Humane Approach to Immigration https://privacyinternational.org/what-we-do/demand-humane-approach-immigration (accessed 3 March 2022).

[5] PI, Fundaciòn Datos Protegidos, Red en Defensa de los Derechos Digitales (R3D), "Joint submission to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance", June 2020, https://privacyinternational.org/advocacy/3939/pis-joint-submission-un-special-rapporteur-contemporary-forms-racism-racial (accessed 3 March 2022); 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", May 2020, https://privacyinternational.org/advocacy/3756/pis-submission-un-working-group-use-mercenaries-role-private-companies-immigration (accessed 3 March 2022)

oversee the use of tech and data processing in immigration processes. 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.[6]

This is creating a hostile environment in which migrant and refugee populations are subject to invasive and sustained surveillance and monitoring both at the border and as they live as foreign nationals in a respective country. This is also having a chilling effect on the process of migrating and ensuring regular, safe migration routes, as well as the ability to enjoy safely and securely other fundamental rights such as the right to access health care, to access social protection, to access justice, to name a few, which is impacting their ability to enjoy their fundamental rights safely and with dignity, including to participate in public life.[7]

THE EXAMPLE OF THE UNITED KINGDOM

In the following section we provide further details on recent or current border management legislation/policies/measures, (including those temporary measures as part of

[6] Cage, "Nationality and Borders Bill expands 'draconian' Schedule 7 stop powers to 'criminalise' migrants", Press Release, 4 February 2022, https://www.cage.ngo/nationality-and-borders-bill-expands-draconian-schedule-7-stop-powers-to-criminalise-migrants (accessed 3 March 2022)

[7] PI, "The Hostile Environment is incompatible with public health: PI joins the Vaccine For All campaign", 4 February 2021, https://privacyinternational.org/news-analysis/4424/hostile-environment-incompatible-public-health-pi-joins-vaccine-all-campaign (accessed 3 March 2022); PI, "Covid-19 doesn't discriminate based on immigration status - nor should the Home Office", 20 March 2020, https://privacyinternational.org/advocacy/3490/covid-19-doesnt-discriminate-based-immigration-status-nor-should-home-office (accessed 3 March 2022); PI, "Privacy International is joining migrant organisations to challenge the UK's "immigration control" data protection exemption - find out why!", 19 July 2019, https://privacyinternational.org/news-analysis/3064/privacy-international-joining-migrant-organisations-challenge-uks-immigration (accessed 3 March 2022)

a state of emergency), with the view to control, reduce or prevent migrant arrivals in the United Kingdom.

Nationality, Borders and Immigration Bill

The UK seeks to amend the Terrorism Act 2000 via the Nationality and Borders Bill[8] to extend the powers in Schedule 7 to apply to anyone held for immigration processing arriving via small boats i.e., after crossing the channel. Under the proposed legislation, counter-terrorism police officers would be able to question, detain and search anyone, including their phones and other electronic devices, being held for immigration processing within five days of their arriving in the UK aboard "any floating vessel or structure".

Concerns have been expressed that this would discriminate against certain groups of migrants with travellers from Muslim and ethnic minority backgrounds already being disproportionately subject to such measures[9] and that it would also be used to further criminalise migrants.[10]

Mobile Phone Extraction

The UK, via various provisions in the UK Police, Crime, Sentencing and Courts Bill ['PCSC'] Bill'[11] is seeking to include immigration officers amongst those who can exercise powers to extract information from electronic devices (MPE).

[8] Nationality and Borders Bill, https://bills.parliament.uk/publications/44307/documents/1132 (accessed 3 March 2022)
[9] PI, "Submission for the UN report on the right to privacy and artificial intelligence", June 2021, https://privacyinternational.org/advocacy/4538/privacy-internationals-submission-un-report-right-privacy-and-artificial-intelligence (accessed 3 March 2022)
[10] Simon Hooper, "UK Nationality and Borders Bill: Refugees to face Schedule 7 counter-terror searches", Middles East Eye, 1 February 2022, https://www.middleeasteye.net/news/uk-nationality-borders-bill-refugees-face-counter-terror-searches, (accessed 3 March 2022)
[11] See: Part 2 and Section 37, Police, Crime, Sentencing and Courts Bill, https://bills.parliament.uk/bills/2839 (accessed 3 March 2022)

Extraction of data from devices constitute a considerable interference with the right to privacy – with such tactics providing access vast quantities of data including call records, contents of emails, SMS and other messages, photographs, web browsing history, geolocation data, or data from applications.[12]

There are two overarching reasons why this is problematic:

1. The sole provision in the PCSC Bill to extract information rests on voluntary provision and agreement, which fails to account for the power imbalance between individual and state. This is particularly acute for migrants in vulnerable circumstances and facing language barriers.
2. Immigration Officers are not digital forensic experts. This impacts the reliability of evidence whether used for intelligence gathering, decision making or criminal investigations. The 'Immigration Enforcement Digital Device Extraction Policy' states that "Criminal and Financial Investigation/Immigration Enforcement" do not have ISO 17025 accreditation and have not been accredited to the Forensics Regulators Codes of Conduct."

Not only have such tactics been found to be highly intrusive and a violation of one's privacy given the way our devices store large amounts of information about us and provide an insight into our lives[13] but it is also important to reflect on how phone seizures can cause asylum seekers substantial distress, leaving them without means of communication for months, and taking away photographs and other memories of family and friends.

The use of this power must be seen in context. The Home Office has admitted, in recent judicial review proceedings, to operating a secret and blanket policy of seizing mobile phones of all migrants who arrived in the UK by small boat between April 2020 and

[12] For more on what is mobile phone extraction see: https://privacyinternational.org/taxonomy/term/431
[13] R v Vu 2013 SCC 60, [2013] 3 SCR 657 at [40] and [41], https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13327/index.do (accessed 3 March 2022)

November 2020.[14] During the course of proceedings it came to light that the Home Office has also self-referred itself to the UK Information Commissioner's Office for breaches of the Data Protection Act 2018.

We know that in 2020 alone immigration officials conducted 4,925 mobile phone extractions.[15] In response to a FOIA submitted by Byline Times, the Home Office acknowledged that 7,167 "kiosk data extractions" had taken place between 1 July 2019 and 31 May 2021.

We have asked on several occasions during the legislative process for the UK government to remove the inclusion of Immigration Officers from the provisions in the PCSC Bill relating to seizure and extraction of mobile phones,[16] and recently we intervened in judicial review to support asylum seekers against the UK Home Secretary's seizure and extraction of their mobile phones to highlight the human rights implications of such tactics.[17]

[14] PI, "PI intervenes in judicial review to support asylum seekers against the UK Home Secretary's seizure and extraction of their mobile phone", 31 January 2022, https://www.privacyinternational.org/news-analysis/4782/pi-intervenes-judicial-review-support-asylum-seekers-against-uk-home-secretarys (accessed 3 March 2022)

[15] PI, "Why Forensics Matter: Immigration officers and the quality of evidence in the UK", 20 January 2022, https://privacyinternational.org/news-analysis/4740/why-forensics-matter-immigration-officers-and-quality-evidence-uk (accessed 3 March 2022)

[16] See: PI, "The new Policing Bill fails to provide sufficient safeguards around extraction of victims' data", 17 March 2021, https://privacyinternational.org/news-analysis/4465/new-policing-bill-fails-provide-sufficient-safeguards-around-extraction-victims (accessed 3 March 2022); PI, "Policing Bill: An unsatisfactory debut on the statute books for mobile phone extraction", 29 June 2022, https://privacyinternational.org/news-analysis/4586/policing-bill-unsatisfactory-debut-statute-books-mobile-phone-extraction (accessed 3 March 2022)

[17] PI, "PI intervenes in judicial review to support asylum seekers against the UK Home Secretary's seizure and extraction of their mobile phone", 31 January 2022, https://www.privacyinternational.org/news-analysis/4782/pi-intervenes-judicial-review-support-asylum-seekers-against-uk-home-secretarys (accessed 3 March 2022)

GPS tags and location tracking

On 31 August 2021, the UK government brought into force Schedule 10 of the Immigration Act 2016, which introduced mandatory electronic monitoring (EM) using GPS tags[18] for every individual categorised as a Foreign National Offender, and EM as a condition of immigration bail became mandatory for all those in England and Wales subject to either deportation proceedings or a Deportation Order at the point of release from prison or Immigration Removal Centre .i.e., there is no judicial discretion. [19]

According to paragraph 4(1) of Schedule 10 the purpose of EM is to detect and record a person's location, presence and absence from location at "specified times, during specified periods of time or while the arrangements are in place".

The Home Office guidance on Immigration Bail, a policy document, provides additional detail relating to proposed use of location data.[20] According to this document, trail data i.e., location history, may be accessed by the Home Office "where it may be relevant to a claim by the individual under Article 8 ECHR" and "to be shared with law enforcement agencies".

Privacy International obtained the Data Protection Impact Assessment (DPIA) from the Home Office related to the "GPS Satellite Tracking Datasets, owned by Ministry of Justice" dated 29.08.2020. This states that: "GPS tracking will trace and record the locations of all wearers at all times and will be held by the supplier." It states that the number of tag wearers is expected to rise from 280 to 4500. Data will be retained for 6 years from the point the individual is removed from the tag.

[18] To learn more about GPS trackers and how they work, see: PI, "Electronic monitoring using GPS tags: a tech primer", 9 January 2022, https://www.privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer (accessed 3 March 2022)
[19] The Immigration Act 2016 (Commencement and Transitional Provisions No. 1) (England and Wales) Regulations 2021, 2021 No. 939 (C. 50), https://www.legislation.gov.uk/uksi/2021/939/made/data.xht (accessed 3 March 2022)
[20] UK Home Office, Immigration bail, Version 11, 31 January 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051204/immigration_bail.pdf (accessed 3 March 2022)

Furthermore, the DPIA states that data sharing will take place between the Police, Home Office and Ministry of Justice, which details the number of 'tagged' cases 'showing name, nationality, DOB and address'. This will enable data analysis by these authorities.

The intention to use location data to make decisions in immigration applications is a concern for a variety of reasons.

GPS tags provide a deep insight into one's life and can reveal intimate details to the person analysing the data. This type of constant surveillance has been reported to negatively impact tag wearers leading to feelings of increased anxiety and individuals might not want to spend time with a friend who is wearing a GPS tag. [21] Therefore it risks having a strong chilling effect.

The use of such tools could lead to spurious, unfair, and somewhat arbitrary decisions about asylum seekers who use Article 8 of the UK Human Rights Act (which is about the 'respect for your family and a private life') as the basis of their asylum claim. For example, the Home Office could use location data to argue 'you talk about your family life, but we can see that you never take your children to school', 'you are never at home at weekends, so you're clearly not spending time with your family' etc. So, there is a grave potential for location data to be used by the Home Office to make spurious inferences and turn down applications.

[21] Jane Kerr, Ellie Roberts, Malen Davies, Merili Pullerits, "Process evaluation of the Global Positioning System (GPS) Electronic Monitoring Pilot, Qualitative findings", NatCen Social Research, Ministry of Justice Analytical Series 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779199/gps-location-monitoring-pilot-process-evaluation.pdf (accessed 3 March 2022)

Drones and Aerial Surveillance

There has been increasing use of drones to surveil the borders across the world including in the European Union[22] and the UK. In the case of the UK,[23]this first came to light in December 2019 when the BBC revealed that a single unmanned aircraft (an AR5, manufactured by Tekever) had been spotted flying from Lydd Airport to monitor people attempting to cross the channel from France by boat.[24] This drone embeds a range of high precision video, imagery and sensors.

In July 2021 we reviewed the use of drones on the UK border. A £1 million contract was awarded in 2020 to an Israeli defence company (Elbit Systems) to demonstrate and develop drones to enhance coastal surveillance operations.[25] The call for tender sought a company to "assess the potential use of UAV to augment current and future aerial surveillance capability by reducing, enhancing or replacing existing delivery methods."[26]

The use of satellite and aerial surveillance pose multiple and varied challenges for the migration sector and for the protection of the rights of migrants. The developments in the technologies that fall under this type of surveillance raise broader concerns, for example, to automated decision-making, use of facial recognition technology and data sharing.[27]

[22] PI, "Space: The Final Frontier of Europe's Migrant Surveillance" 26 July 2021, https://privacyinternational.org/news-analysis/4601/space-final-frontier-europes-migrant-surveillance (accessed 3 March 2022)
[23] See: PI, "Electronic monitoring using GPS tags: a tech primer", 9 January 2022, https://www.privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer (accessed 3 March 2022)
[24] BBC News, "Drones monitor south coast of England for migrant boats", 5 December 2019, https://www.bbc.co.uk/news/uk-england-kent-50673241 (accessed 3 March 2022)
[25] Drone Demonstration and Development Project, Maritime & Coastguard Agency, Published om 2 July 2020, https://www.contractsfinder.service.gov.uk/Notice/713d488e-6c55-4293-9a10-9759a2191dad?origin=SearchResults&p=1, (accessed 3 March 2022)
[26] PI, "Dear Home Secretary: Channel crossings are already inviable for asylum-seekers and human rights" 17 August 2022, https://privacyinternational.org/news-analysis/4124/dear-home-secretary-channel-crossings-are-already-inviable-asylum-seekers-and (accessed 3 March 2022)
[27] PI, "Electronic monitoring using GPS tags: a tech primer", 9 January 2022, https://www.privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer (accessed 3 March 2022); Statewatch, Border surveillance, drones and militarisation of the Mediterranean, 6 May 2021, https://www.statewatch.org/analyses/2021/border-surveillance-drones-

As has been explored in relation to the use of drones in warfare, surveillance and targeting is on the one hand more individualized and personalised, but on the other hand more and more dehumanised.[28] This relates not only to the physical distance from those who are being monitored but also that software can be similar to that of gaming systems as targets transformed from living people to insignificant icons on computers.

These developments come at a time when the Home Office is continuing to take measures to make the crossing of the Channel "inviable",[29] and the number of children arriving on small boats is reportedly increasing, many unaccompanied and potential victims of trafficking arriving via small boat are said to have been failed by the Home Office.[30]

and-militarisation-of-the-mediterranean/ (accessed 3 March 2022); Hannah Tyler, "The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions", 2 February 2022, Migration Policy Institute, https://www.migrationpolicy.org/article/artificial-intelligence-border-zones-privacy (accessed 3 March 2022)

[28] Alexandra Funk, "Drones in Contemporary Warfare: The Implications for Human Rights", 7 July 2016, LSE Blog Post, https://blogs.lse.ac.uk/humanrights/2016/07/07/drones-in-contemporary-warfare-the-implications-for-human-rights/ (accessed 3 March 2022)

[29] PI, "Dear Home Secretary: Channel crossings are already inviable for asylum-seekers and human rights" 17 August 2022, https://privacyinternational.org/news-analysis/4124/dear-home-secretary-channel-crossings-are-already-inviable-asylum-seekers-and (accessed 3 March 2022)

[30] May Bulman, "Scores of refugee children illegally detained after crossing Channel", The Independent, 5 February 2021, https://www.independent.co.uk/news/uk/home-news/children-refugees-channel-detained-home-office-b1798100.html (accessed 3 March 2022)