Border Security, Asylum and Immigration Bill: Evidence for the House of Commons Committee Stage

Author: Sara Alsherif on behalf of Open Rights Group
March 2025

1. Introduction

Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. ORG has been following the UK government's surveillance proposals since our

inception, including the Regulation of Investigatory Powers Act 2000, the Data Retention and Investigatory Powers Act 2014, and the Investigatory Powers Act 2016. We have also worked on all of the data protection legislation proposed and enacted since GDPR.

2. Executive summary

Dangers to EU-UK cooperation

The Border Security, Asylum and Immigration Bill raise serious concerns domestically and for the joint UK/EU bodies established under the Trade and Cooperation Agreement (TCA) and the Windsor Agreement. Open Rights Group (ORG) will follow this submission with comprehensive technical analyses outlining how the Bill's provisions could undermine the UK/EU adequacy agreement.

These provisions authorise broad sharing of customs and transport data for national security and law enforcement purposes, effectively creating a multi-agency data pool. This can result in pervasive surveillance and mass profiling of migrants and asylum seekers, potentially undermining the robust data protection framework required under both UK law and the EU GDPR.

This briefing examines the new provisions in the Bill that expand the powers of the Border Security Commander, notably by formalising greater cooperation with national security agencies such as MI5, SIS, and GCHQ and enabling broad data sharing. In short, these measures risk extending counterterrorism-style investigatory techniques to migrants, refugees, and asylum seekers. The main concerns around this bill is that it shapes a new narrative around people seeking safety, criminalising their actions and violating their right to seek asylum in the UK, contrary to the international law.

Migrants are not criminals

Crossing borders is inherently a civil issue and should not be treated as a criminal offence unless an actual crime is committed. Penalising irregular migrants—individuals seeking safety, asylum, and protection from persecution—directly contravenes the UK's international legal obligations under Article 31(1) of the 1951 United Nations Convention Relating to the Status of Refugees.

This approach, of treating vulnerable people looking for safety as criminals, may result in invasive digital searches, discrimination of vulnerable groups, and reduced transparency and accountability. Moreover, while the Bill relies on existing oversight regimes (e.g. the Investigatory Powers Act 2016 and Data Protection Act 2018), it fails to introduce new, dedicated safeguards to protect the digital and human rights of those seeking protection.

3. Counter-terror powers applied to immigration lacks safeguards

Clause 5(3)–(4): counter-terror powers

The Bill mandates that the Border Security Commander establish formalised co-operation arrangements with MI5, SIS, and GCHQ. Although these agencies are explicitly excluded from the *"partner authorities"*[1] definition, the Bill requires them to provide support for border operations, thereby extending their counterterrorism capabilities into the sphere of organised immigration crime.

- This cooperation, particularly through data-sharing in clauses (27–33), means that investigative techniques initially designed for counterterrorism could be applied to immigration and gang-related crime.
- Migrants, refugees, and asylum seekers, who are already in vulnerable positions, might find themselves subject to investigative methods that are not traditionally used in ordinary criminal proceedings. This raises concerns that such individuals could be swept into regimes of surveillance and investigatory practices that lack the safeguards typically afforded under normal criminal law.
- The security apparatus (like GCHQ) might use secret methods and investigatory techniques that are difficult to scrutinise or hold accountable. Even if no new arrest or search powers are granted directly to intelligence agencies, their involvement in border operations implies that the powerful, covert tools of national security would be employed without the robust oversight that applies to standard law enforcement. There is a real risk that these methods will disproportionately affect migrants. If intelligence techniques are applied in the context of immigration enforcement, individuals seeking asylum or protection may be treated as potential criminals rather than vulnerable people fleeing persecution.
- The use of these powers in the immigration context may contravene the principle of proportionality under UK law2, as established in the interpretation of Article 8 of the European Convention on Human Rights (ECHR) and key judgments by the European Court of Human Rights.
- These clauses pose a serious threat to the EU-UK adequacy agreement, which hinges on robust data protection standards. If the UK's surveillance practices are seen as disproportionately invasive and lacking sufficient safeguards, the adequacy decision may be jeopardised, restricting the free flow of personal data between the EU and the UK.

[1]Chapter One: 3(6) from Border Security, Asylum and Immigration Bill: https://publications.parliament.uk/pa/bills/cbill/59-01/0173/240173.pdf

[2]Human Rights Act 1998: https://www.legislation.gov.uk/ukpga/1998/42/schedule/1

- We are concerned that the lack of bespoke oversight risks leaving affected individuals without an effective remedy, violating the right to a fair hearing. We strongly recommend scrapping clauses giving intelligence agencies such powers. This may lead to people who overstay their visas being subjected to antiterrorism measures with longer detention periods and less judicial oversight.

4. Disproportionate Data Sharing and Investigatory Powers

Clauses 19-23: broad powers to search and share information

Theses clauses define *"relevant persons"* (those entering the UK without proper documentation) and allows authorised officers to search, seize, and retain electronic devices (e.g., phones, laptops) of asylum seekers and migrants if they have *"reasonable grounds to suspect"* them of an offence. It grants broad powers to access, copy, extract information and use any data stored on these devices. The Bill also allows officers to retain data for as long as they deem *"necessary"*, with potential onward disclosure to other agencies.

- Our concern is that these clauses risk invasive digital searches. The broad definition of *"relevant articles"* and the broad authority to search persons for electronic devices, especially the power to access, copy, and use data stored on those devices, raise serious privacy concerns. For migrants, refugees, and asylum seekers (who may already be in vulnerable positions), these provisions could lead to disproportionate invasions of digital autonomy.
- While the Bill states that searches must be *"reasonable"*, the broad scope of digital data that can be accessed (often without judicial oversight at the point of search) means that sensitive personal information may be collected and retained without adequate safeguards.
- The Bill allows broad searches, without warrant, of migrants and asylum seekers' electronic devices. Migrants could be compelled to unlock their devices, violating privacy rights *(Article 8, European Convention on Human Rights)*. In 2022, the High Court ruled that the UK Home Office's covert and indiscriminate practice of seizing and searching migrants' mobile phones violated Article 8 of the European Convention on Human Rights, as well as UK data protection laws[3]. The High Court ordered the UK Home Office to provide remedy to the thousands of migrants affected by its unlawful policy and practice of seizing mobile phones from people arriving by small boats to UK shores[4].
- There is a risk that seizure and retention of devices could cut migrants off from

[3] England and Wales High Court (Administrative Court) Decisions: https://www.bailii.org/ew/cases/EWHC/Admin/2022/695.html

[4] UK High Court orders groundbreaking redress for thousands of migrants affected by unlawful phone seizures and data extraction: https://privacyinternational.org/news-analysis/4987/uk-high-court-orders-groundbreaking-redress-thousands-migrants-affected-unlawful

legal assistance, family, and support networks, increasing vulnerability.

- A key concern is that nearly every individual arriving by "small boat" with an electronic device may be presumed to hold relevant information, effectively leading to indiscriminate searches and seizures.

Clauses 27–33: data sharing powers clash with EU agreements

These clauses authorise broad sharing of customs and transport data for *"national security"* and *"law enforcement"* purposes. They allow intelligence agencies to receive data and enable further sharing between the Home Office, HMRC, and other agencies. Additionally, data obtained under clauses 19–26 may trigger intelligence involvement in operations when national security issues are identified. These clauses also facilitates the onward sharing of migrants' and asylum seekers' data domestically and internationally.

- These provisions would interact with Clauses 87-89 of the Data (Use and Access) Bill which, in the context of join processing operations between intelligence services and law enforcement, exempts data processing from data protection requirements by means of "designation notices" and "national security certificates". The compound impact of these provisions risks undermining the data protection standards that are fundamental to the joint UK/EU bodies established under the Trade and Cooperation Agreement (TCA)[5] and the Windsor Agreement[6]. These joint bodies depend on a secure, transparent, and proportionate data-sharing framework that complies with both UK data protection laws and the EU GDPR.
- The provisions enable the creation of a multi-agency data pool, which risks pervasive monitoring of migrants. This practice raises serious concerns under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which require data processing to be lawful, fair, and transparent.
- When digital devices are deemed suspect by default and subjected to broad search powers without stringent judicial authorisation, there is a real danger of disproportionate enforcement against vulnerable groups. This approach may

[5] The EU-UK Trade and Cooperation Agreement https://commission.europa.eu/strategy-and-policy/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en

[6] The Windsor Framework: a new way forward: https://assets.publishing.service.gov.uk/media/63fccf07e90e0740d3cd6ed6/The_Windsor_Framework_a_new_way_forward.pdf

conflict with the principle of data minimisation, a core tenet of the GDPR.

- The Bill's provisions target those who have entered the UK without proper leave, a category that includes many asylum seekers and migrants fleeing persecution. Using digital search powers in such contexts risks conflating humanitarian irregularity with criminal behaviour. When electronic devices and data are automatically deemed suspect, it creates a system in which vulnerable individuals may be treated as potential criminals or terrorists rather than people seeking protection.
- The Bill effectively creates a multi-way data-pooling system and enables mass profiling. Once customs/travel data is linked across the government agencies, it can facilitate more pervasive monitoring. This can lead to a chilling effect, especially if data includes details of group travel or diaspora communities. Legitimate associational or humanitarian activities might be subject to heightened scrutiny.
- Such provisions risk exposing sensitive personal and digital information about migrants to agencies that use counterterrorism tools that typically operate under a veil of secrecy.
- Such clauses risk violating the digital rights of those people seeking safety and treating them like criminals. Crossing borders is a civil matter, and cannot be treated as a criminal offence when the subject has committed no crime. Criminalising irregular migrants who enter the country seeking safety, claiming asylum, escaping persecution, and in need of protection is contrary to the international law that the UK is legally bound to Article 31(1) of the 1951 United Nations Convention Relating to the Status of Refugees states that:[7]:

"The Contracting States shall not impose penalties, on account of their illegal entry or presence, on refugees who, coming directly from a territory where their life or freedom was threatened in the sense of article 1, enter or are present in their territory without authorization, provided they present themselves without delay to the authorities and show good cause for their illegal entry or presence."

- We recommend adding that any data processing operation carried out under these provisions should comply with Part 3 of the Data Protection Act 2018, even where those data processing were being carried out by intelligence services.

[7]Convention relating to the Status of Refugees: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.23_convention%20refugees.pdf

Clauses 34-36, 42: biometric data stored and shared

These clauses about biometric information collection and retention authorise taking biometric data (fingerprints, facial scans) from migrants, including children over 16 years old, without parental consent. Additionally, the provisions allow for biometric data to be collected outside the UK and transferred to third countries or international organisations under exceptions within the UK GDPR. Crucially, they also permit the retention of this biometric information for up to five years, with the possibility of an even longer retention period under conditions that are not clearly defined.

- Collecting the biometric data from children over 16 without consent could violate child protection laws8.
- Retaining biometric data for five years or longer contradicts data minimisation principles under the UK GDPR. Data collection should follow proportionality principles; biometric data should only be collected when absolutely necessary.
- The concerns here that once seized, data can be retained for prolonged periods *"for use in proceedings"* or for *"accessing, examining or copying"* purposes. Without clear retention periods and strict data protection standards, sensitive data, including personal communications, biometric records, and other digital footprints, could be misused or inadequately secured.
- The extensive sharing of information between HMRC, border security, immigration authorities, and even international organisations creates vulnerabilities. The more widely data is circulated, the higher the risk of data breaches, unauthorised access, or mission creep, where data gathered initially for customs or immigration purposes is used for other, less justifiable purposes.
- The potential for data sharing with third countries/ foreign agencies poses risks of human rights abuses and can expose asylum seekers to hostile regimes. We strongly recommend that stringent measures are implemented to prevent the

[8]According to the guidance of the Information Commissioner's Office (ICO) on processing sensitive personal data under the UK GDPR, biometric data is categorised as special category data and requires explicit consent. The guidance stresses that when dealing with minors' data, additional safeguards must be implemented to protect their rights. Therefore, collecting biometric data from children over 16 without proper consent could breach child protection standards, as it fails to meet the stringent consent requirements and the enhanced safeguards necessary for processing such sensitive information. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/key-data-protection-concepts/
see also, Protection of biometric data of children in schools and colleges: https://assets.publishing.service.gov.uk/media/62d7d76c8fa8f50c012d14df/Biometrics_Guidance_July_2022.pdf

sharing of personal data with authorities in any country—whether it is the country of origin or habitual residence—where the individual may face persecution, and to for authorities to secure explicit, valid consent before any data is collected or disclosed9.

[9] Disclosure and confidentiality of information in asylum claims: https://assets.publishing.service.gov.uk/media/630f3a9be90e0729da484f35/Disclosure_and_confidentiality_of_information_in_asylum_claims.pdf#page=10&zoom=100,92,672

5. Indefinite Electronic Monitoring and Surveillance

Clauses 46-47: tagging and indefinite monitoring

This clauses introduce electronic tagging of individuals under certain circumstances, and courts can impose electronic monitoring as part of a serious crime prevention order (SCPO) (or an Interim SCPO) and compel disclosure of personal details such as addresses, phone numbers, social media usernames, gaming IDs, etc. SCPOs are civil orders but can have criminal-style restrictions imposed on a *"balance of probabilities"* standard. These mandates continuous electronic monitoring with a 12-month extension limit, allowing indefinite surveillance cycles.

- We are concern that human rights principles require that measures be proportionate, necessary, and subject to independent oversight. The Bill's provisions offer limited procedural safeguards (for instance, reliance on *"reasonable grounds"* rather than rigorous judicial oversight). Such a low threshold can lead to overly broad applications of state power.
- There are no clear definitions of what constitutes *"relevant"* digital material. This should be followed by transparent procedures that allow affected individuals (including asylum seekers and refugees) to challenge or seek redress for intrusive searches or data misuse. Individuals may inadvertently violate these orders and find themselves without adequate support to contest them, thereby reinforcing the criminalisation framework discussed above.
- Expanded surveillance powers criminalise migration, treating asylum seekers as security threats and criminals rather than individuals seeking protection without providing alternative safe routes. The Home Office's practice of GPS tagging, initially applied to migrants released on immigration bail and later expanded through a pilot scheme targeting asylum claimants arriving via dangerous routes, has led to the relentless, 24/7 monitoring of vulnerable individuals. This invasive practice not only results in the collection of vast amounts of highly sensitive personal data, but it also imposes severe restrictions on the lives of migrants, asylum seekers, and refugees, undermining their privacy and digital rights. The ICO's enforcement issued a notice and formal warning10 highlight systemic data protection violations inherent in this policy.

[10] ICO finds the Home Office's pilot of GPS electronic monitoring of migrants breached UK data protection law: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/03/ico-finds-the-home-office-s-pilot-of-gps-electronic-monitoring-of-migrants-breached-uk-data-protection-law/

Such a measure contravenes the principles of purpose limitation under the UK GDPR and fails to meet the standards of necessity and proportionality as demanded by the European Convention on Human Rights.

- The lack of transparency in how migrants' data is shared increases risks of misuse and risks the racial profiling and discrimination against migrants.

6. Conclusion:

Powers lack accountability and intelligence integration poses dangers

We applaud the government's commitment to upholding international human rights by repealing the entire Rwanda Safety Act. However, we are gravely concerned that the government has not taken the decisive step of repealing the entire Illegal Migration Act—contrary to their stance when in opposition—which continues to undermine the rights of vulnerable migrants.

This Bill represents a critical moment in fully embracing the rule of international law. While it is essential to disrupt the operations of human smugglers, it is equally imperative that we do not penalise or criminalise those fleeing war, death, and persecution. Migrants crossing our borders should be treated as individuals seeking safety rather than as criminals. In line with the human rights conventions to which the UK is committed, the way an individual enters the country must not be used as a basis for penalisation. Refugees and asylum seekers should enjoy the same rights regarding data handling as British citizens, ensuring that their digital and fundamental rights are fully protected. The government must seize this opportunity to establish a safe, direct route for those seeking refuge, thereby upholding international standards and safeguarding the dignity and privacy of all individuals.

The Bill's approach to bolstering national security by integrating intelligence capabilities into border enforcement risks sacrificing the rights of vulnerable people. Evidence shows that smugglers do not endanger themselves by embarking on these perilous journeys; instead, genuine asylum seekers, who may simply have digital records of their travel, are at risk of being unfairly criminalised. To dismantle the smuggling business model, the government must establish a safe, humane route for those seeking refuge.

Furthermore, the legal framework underpinning these measures is at odds with established human rights and data protection standards, notably those enshrined in the European Convention on Human Rights (ECHR) and the UK GDPR. This misalignment not only jeopardises digital privacy and accountability but also sets a dangerous precedent for the erosion of civil liberties in our immigration system.

Onward disclosure provisions risk repurposing data initially gathered for border security into broader law enforcement applications, which may breach the principle of purpose limitation under data protection law. UK case law, including rulings from the European Court of Human Rights, consistently mandates that state surveillance be both necessary and proportionate. Consequently, the Bill's expansive powers may well be deemed incompatible with these established legal standards.

The Bill sets up frameworks for inter-agency information sharing but relies solely on existing oversight measures rather than introducing bespoke controls designed specifically for the sensitive area of immigration enforcement. Applying counterterrorism techniques to migration without additional safeguards not only undermines UK domestic law and international human rights obligations but also risks creating an environment rife with human rights abuses against migrants and asylum seekers. Judicial precedents, notably *R (on the application of Privacy International) v Investigatory Powers Tribunal 11*, highlight the need for transparent and accountable oversight, underscoring that the lack of dedicated oversight for these expanded powers is legally problematic.

Although intelligence agencies are formally excluded from the "partner authority" designation—ostensibly to preserve their internal oversight—this exclusion does not prevent their methods from being applied in contexts affecting vulnerable individuals. As a result, techniques intended for high-level national security purposes might be inappropriately utilised in immigration enforcement, with serious implications for the rights of those seeking refuge.

[11]R (on the application of Privacy International) (Appellant) v Investigatory Powers Tribunal and others (Respondents): https://www.supremecourt.uk/cases/uksc-2018-0004

7. Recommendations

Remove unaccountable surveillance powers

- We strongly urge that the Bill be amended to remove unaccountable and invasive surveillance powers from its scope. This includes making sure that the powers to search, seize, retain, access, copy, and use data from electronic devices are strictly limited and applied only on a case-by-case basis with rigorous judicial oversight, rather than as a blanket measure.
- We strongly recommend that the Bill be amended to prohibit the use of surveillance measures such as GPS ankle tagging in immigration enforcement.
- We call to immediately cease the use of GPS tagging as a condition of immigration bail and in all contexts involving asylum seekers. Instead, the government should invest in developing safe and humane routes for people seeking refuge, ensuring that enforcement measures are both proportionate and respectful of fundamental rights.

Add safeguards for data collected or shared

- Collecting and sharing evacuee biometric data must be subject to stringent safeguards.
- Valid, informed consent should be obtained before any biometric data is collected or disclosed, and prohibit sharing this data with authorities in countries where the individual fears persecution.
- Biometric data must be gathered solely to ensure the individual's protection, not for broad security or intelligence purposes. This approach is vital to uphold digital rights and privacy, which align with international human rights standards.

Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH.