Unchecked Power: the new Border Security Bill Undermines Privacy and the Rule of Law

Rights & Security International briefing on Clauses 23 – 26 and 47 of the Border Security, Asylum and Immigration Bill

In the Border Security, Asylum and Immigration Bill (BSIAB), the UK government has pledged to use counter-terrorism-style powers to crack down on so-called 'illegal migration'. However, applying flawed counter-terrorism approaches to target migrants who have faced exploitation by criminal networks and/or may have well-founded asylum claims is not only ineffective, but also likely illegal. The government's approach risks undermining human rights while failing to address the complexities of migration in a just, effective and sustainable way.

By implying that migrants and asylum-seekers are threats, the government is also using dangerous rhetoric of the kind that fuelled the serious anti-migrant violence (including arson and beatings) of summer 2024.

Summary

- Clauses 23 – 26 would grant police and other 'authorised persons' unrestricted access to the digital devices of people entering the country via irregular means. The government has not explained why it thinks it needs to carry out digital strip searches on migrants, many of whom are already vulnerable people. We regard such searches as excessive, and they would create serious risks that people will face unfair discrimination based on their religions, beliefs or opinions.

- Clause 47 would allow authorised persons to impose 'Interim Serious Crime Prevention Orders' (SCPOs). This 'pre-crime' clause would allow officials to treat migrants who have done nothing wrong as potential criminals, and do so without notifying the person affected, imposing life-altering restrictions on individuals who have not been charged with any crime.

In addition to creating legal problems, this clause would further stigmatise migrants – a group that is already vulnerable to attacks in the UK.

We recommend that:

- Robust safeguards and restrictions on access to the digital devices of people entering the country via irregular means be inserted within Clauses 23 – 26.
- Clause 47 5E and 47 5F be removed from the Bill.

Clauses 23 – 26

Clauses 23 – 26, if enacted, would put the UK on a collision course with the European Convention on Human Rights (ECHR).

Allowing the police to access potentially unlimited information stored on a person's phone, tablet or other digital device is highly problematic.

First, the government has not shown that it needs these powers.

Second, these devices will contain deeply personal information—messages, photos, medical information, financial details, contacts, and location history, for example. Giving the police and other 'authorised persons' unrestricted access to this data for all people who enter the country without having been given leave to enter or remain in the UK is manifestly excessive, amounts to mass surveillance (or, as others have termed it, a 'digital strip search'), and erodes the very foundation of the right to privacy. A power of this scope must meet strict principles of legality and necessity—but blanket device access risks excessive intrusion, often without sufficient justification.

Just as alarmingly, it would create a vast pool of data about people – and that data would then be vulnerable to exploitation by a range of bad actors in the future. It would only take one unscrupulous law enforcement agent, civil servant or private contractor to wreak serious harm on migrants and asylum-seekers on the basis of this information, such as by leaking it. The government could also easily use such a vast collection of data to engage in predictive policing through biased or otherwise problematic AI.

We further note that the vast majority of people against whom the police could use Clauses 23-26 are already vulnerable, and may have been fleeing conflict or other horrific experiences; some will also be victims of human trafficking or other exploitation. These individuals will be particularly impacted by the discouraging effect the Bill creates; if people know that their devices could be accessed at any time, they may be less likely to seek the help they need, communicate with family members or take other steps that could aid their safety and well-being.

There is a well-documented pattern of policing powers in the UK being disproportionately used against marginalised communities; the proposed powers allowing police unrestricted access to digital devices mirror the well-documented issues with stop and search powers. Unfettered digital access raises further concerns that:

- Minority groups may be more frequently targeted for device searches, exacerbating existing inequalities in policing.

- Survivors of sexual violence who have already faced invasive and unnecessary demands may be forced to hand over their phones and undergo treatment akin to 'digital strip searches', discouraging them from seeking justice.
- Protesters, journalists and human rights defenders could have their personal communications scrutinised, leading to potential harassment and suppression of dissent.

Once seized, a device's data could be stored, shared with foreign governments to achieve the policy goals of the ruling UK government (even if this puts people in danger), or even leaked, putting people at risk of identity theft, doxxing, blackmailing, homophobic or transphobic attacks, or other misuse by third parties.

<u>Clause 47</u>

47 5E Interim serious crime prevention orders

The government's proposal to introduce 'Interim Serious Crime Prevention Orders' (SCPOs) infringes on fundamental legal principles such as due process rights and procedural fairness. Like all 'pre-crime' measures, it also creates a risk that decisions will be grounded in racist, Islamophobic or other stereotypes.

SCPOs, as escribed in section 5 of the Serious Crime Act 2007, can place sweeping restrictions on a person's:

- Financial, property and business activities
- Communication and movement
- Use of digital devices

They are issued by a court and are intended to prevent future criminal activity.

However, these new interim SCPOs would expand the scope of SCPOs, allowing the government to impose these life-altering restrictions before any full legal determination has been made – including imposing them on people who have done nothing wrong.

Such a practice would stigmatise migrants and asylum-seekers in general, as well as the specific people affected. It would severely restrict people's freedoms and set a dangerous precedent of imposing legal restrictions on fundamental rights without due process.

47 5F Without notice applications

The proposal to allow 'without notice' applications for interim SCPOs further threatens procedural fairness: 'without notice' applications — where the government makes an application for an interim SCPO without giving notice to the person affected – strongly resemble no-notice deprivations of citizenship, which have been criticised by the courts.

The government should not normalise secretive, 'no notice' procedures and a lack of oversight.

Recommendations

- Insert robust safeguards and restrictions on access to the digital devices of people entering the country via irregular means within Clauses 23 – 26.
- Remove Clause 47 5E and 47 5F from the Bill.

About Rights & Security International

Rights & Security International (RSI) is a London-based charity working to end human rights abuses committed in the name of national security. We challenge religious, racial and gender bias in national security policies, advocate for government accountability and transparency, and promote justice for victims of human rights violations.