

Ridgeway Briefing:

The securitisation of information under the UK's latest border security legislation

January 2026

Ridgeway Briefings offer analyses of emerging issues in international relations, security and development, prepared by Ridgeway's team of open-source analysts, linguists and subject-matter experts.

At a glance

- The UK Government's long-awaited Border Security, Asylum and Immigration Act 2025 came into force in December 2025.
- Alongside greater powers on electronic device seizure, the Act establishes new offences related to information used to support irregular migration journeys to the UK, indicating a hardening in Labour's approach to immigration enforcement.
- Possible effects of these new measures include (1) ambiguity for law enforcement implementation, (2) rights and protection challenges, and (3) data privacy and security risks.

Ridgeway analysis

UK immigration legislation is moving at an extraordinary pace. The Border Security, Asylum and Immigration Act 2025 (hereafter, the 'Act') marks an interesting shift in how information is becoming increasingly securitised – a shift that has wide-ranging implications for migrants, authorities, and researchers alike.

On 2 December 2025, the UK's Border Security, Asylum and Immigration Bill received Royal Assent. The Act consolidates and updates several earlier pieces of legislation concerned with border security and the disruption of organised immigration crime. Notably, the Safety of Rwanda Act 2024 has been repealed, while amendments have been made to several elements of the Illegal Migration Act 2023.

According to Home Secretary Shabana Mahmood, the Act provides law enforcement with "stronger powers than ever before". The new measures, falling across the following four pillars, indeed showcase the government's continued interest in tighter immigration enforcement and administrative control.

1) A new framework within which the Border Security Command can operate, with Commander Martin Hewitt positioned to work across government bodies, including the National Crime Agency, Immigration Enforcement, Border Force, intelligence and police.
2) Expanded data sharing capabilities to assist in the development of the intelligence picture of organised immigration crime and other threats.
3) New and enhanced powers to strengthen border security.
4) Measures to support and strengthen the UK's asylum and immigration system.

But beyond enhanced law enforcement, the Act indicates a shift towards the criminalisation of information use, made easier by expanded access to personal devices.

"Labour will stop the chaos and go after the criminal gangs"

The Labour government has made a host of pledges on immigration, so far with varying success. Their 2024 manifesto promised to "go after the criminal gangs who trade in driving this crisis" – meaning small boat arrivals across the Channel and the 'perma-backlog' of asylum claims. This narrative is evident across the new Act. The disruption of organised immigration crime as a means to curb 'illegal' migration remains the priority, including through adopting counter-terrorism style measures.

Labour's approach reflects a broader securitisation agenda. Although complex to quantify, the logic of securitisation is arguably flawed; irregular migratory flows are rarely stemmed through deterrence tactics alone. Even the government's own impact assessment on the 2023 Illegal Migration Bill recognised that deterrence policies "might not have the desired effect". Indeed, the dangers that asylum seekers face in their

country of origin often outweigh the perceived risks of an irregular journey, especially if there is a lack of technical or legal knowledge of how a destination country's immigration policy works in practice. The idea of a 'rational choice' hurdle might also explain why potential migrants remain undeterred; particularly in stressful circumstances, cognitive biases can convince individuals that their chances of success are stronger than they might be in reality.

Securitisation tactics can create other risks, for migrants and authorities. Heightened enforcement along one route may divert people to another. For example, the UK's crackdown on stowaways hiding in lorries or ferries led to a surge in small boat arrivals across the Channel, particularly from 2018 onwards. The latest statistics show us that small boat arrivals now account for 89% of all irregular arrivals. Refugee rights groups, such as the Migrants' Rights Network and Safe Passage, also claim that irregular arrivals to the UK will continue unless safe routes are opened up. New research by the Mixed Migration Centre also suggests that restricted access to regular migration routes is fuelling the demand for people smuggling.

Data: tool or target?

Given Labour's enduring narrative on organised immigration crime, much of the Act does not come as a surprise. Several measures do, however, represent a subtle evolution in the government's approach to immigration information governance – notably:

- the criminalisation of information use in relation to irregular migration journeys, and
- the expansion of powers on data collection through device seizures.

The collection, use and dissemination of information is critical for all actors involved in irregular migration. Data helps authorities and government to better understand irregular migration and organised crime activities and, accordingly, coordinate inter-agency responses and targeted policies. For migrants and potential migrants, information (accessed via official sources, information campaigns or community networks) can assist in migratory decision-making and highlight possible risks and opportunities. And for researchers, data (or lack of) can help reveal irregular migration trends and dynamics, analysis which can help to counter misinformation and lead to more evidence-led public debate and policymaking.

Various factors threaten to compromise this complex and multi-use information landscape. Given the clandestine and fast-paced nature of irregular migration, data accuracy is often low, and information easily obsolete. Inconsistencies also exist in the collection and interpretation of data, with different organisations and agencies operating in silo, with different priorities and capabilities.

In many ways, this new Act is seeking to grow the government's immigration evidence base, nominally to mitigate dangers from organised immigration crime. But this quickly expanding information landscape may come at a cost. Amplified powers to search for, collect and share information could pose enforcement, data security and protection risks – particularly when the information concerns vulnerable individuals.

Expanded device seizure powers

As part of the government's plans to "strengthen border controls, enhance data-driven enforcement, and improve inter-agency collaboration", the threshold for device seizure powers has been lowered significantly. Devices such as mobile phones and SIM cards can now be seized by a range of "authorised officers" without the need for an arrest.

Under Sections 22-29, the Act empowers official personnel to search for, seize, retain and extract data from electronic devices belonging to illegal entrants and arrivals where there is reasonable suspicion that the device may contain information that relates to an offence under Section 25 of the Immigration Act 1971 (helping an asylum seeker enter the UK). This power is ostensibly for the purpose of disrupting organised immigration crime such as people smuggling.

Criminalisation of information use

Section 16 of the Act establishes new offences related to information for use in an immigration crime, with a maximum penalty of five years' imprisonment. Under the new legislation, it is a criminal offence to collect, view or access information if there is "reasonable suspicion" that it could be used by someone organising or preparing to take a journey to the UK that could constitute an immigration offence. Namely, this would likely be unauthorised arrival and entry to the UK as defined by the Immigration Act 1971. Some exemptions are noted, such as information gathering for the purpose of journalism or academic research. People involved in smuggling networks will also be at a higher risk of criminal liability.

The provision appears to be directly inspired by Section 58 of the Terrorism Act 2000, which makes it an offence to "collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism [sic]". Section 16 also reflects the structure of a 'precursor' offence in counter-terrorism law which criminalises information gathering that could *theoretically* assist wrongdoing, meaning proof of someone's intent and connection to terrorism is not required.

I. Implications for law enforcement implementation

Such powers that criminalise the possession of information have been subject to scrutiny for their loosely defined offences. The wording of Section 16 is, too, sufficiently vague, and it is unclear what type of information might constitute a crime. For example, sharing contact details of a known people smuggler would likely count as an offence, as would a financial receipt for forged identification documents. But would downloading the next week's weather forecast for the Channel count? Or receiving a WhatsApp message that contains contact details of a UK relative or immigration lawyer? This ambiguity will likely embolden discretionary powers by authorities and could, paradoxically, lead to potential migrants actively avoiding information on how to avoid committing an offence.

Moreover, while the new device seizure powers are "primarily intended for use in high-risk operational settings such as small boat arrivals", there is plenty of room for discretion – especially given that authorities can now seize devices from "non-suspect" individuals. Seizures reportedly started on 5th January at the Manston Immigration Centre in Kent where technology is already available to download data from seized devices. A Home Office spokesperson has said that confiscated phones would be returned in "most cases", although it is unclear at this stage how the power will be used by officials in practice. The UK legal reform charity Justice have further expressed concern that the powers will "amount to blanket seizure of electronic devices… previously found to be unlawful". These operational challenges could both strain enforcement capabilities and lead to unforeseen legal challenges.

II. Rights and protection challenges

By criminalising broad swathes of information activity, the Act risks discouraging migrants from seeking out or sharing potentially life-saving information. Humanitarian organisations often depend on digital information channels to share guidance on asylum rights and routes or safety warnings – now possibly criminal acts under the new legislation, even when intended for protection. There are also concerns that 'precursor' offences severely constrain migrants' access to information, which come with implications for UK compliance with the core non-penalisation principle of the 1951 Refugee Convention.

Device seizure powers are not unprecedented in UK law. Similar powers on seizing mobile phones from people irregularly crossing the Channel were enforced by the Home Office between 2018 and 2020, before being ruled unlawful in 2022 on the basis that they violated Article 8 of the European Convention on Human Rights (respect for private and family life). But despite ongoing concerns today, the government's human rights memorandum for this recent legislation decided that the provision contained sufficient safeguards and that the intrusive measures are proportionate to the objective of curbing organised immigration crime.

The growing field of data justice exposes other ethical risks related to such forms of data extraction. Some research indicates that digital technologies in migration governance can increase the likelihood of human rights violations and the vulnerability of undocumented people, with private companies often developing and deploying these digital tools for profit.

III. Data privacy and security risks

The new powers on device seizure and information possession raise obvious data privacy concerns. Devices often contain sensitive personal information, such as messages, financial details and health records. The official guidance does highlight the need for officers to act with "care and proportionality… with particular caution when dealing with vulnerable individuals", but the powers do not fully or partially restrict search and seizure powers for any of the vulnerable groups named.

There are also data security risks for authorities themselves. The government has expanded powers to retain and share data under the new Border Security Command, including simplifying processes for sharing customs data between the Home Office, HMRC and other departments. These changes may help create a more comprehensive intelligence picture but may also lead to institutional vulnerabilities if robust protections and audit mechanisms are not in place. Indeed, the recently uncovered major personal data breach involving applicants to Afghan relocation schemes exposed both the human and political costs of a lapse in data security.

In summary, the Border Security, Asylum and Immigration Act 2025 is another cog in the ever-evolving UK immigration machine. With much of the legislation yet to be rolled out, the effects of the new offences and device seizure powers are so far unclear. But the measures are well worth watching: they could reshape how migrants and smugglers use information, test the limits of data security, and influence wider conversations about digital technologies and human rights.

About Ridgeway

Ridgeway delivers impactful research and analysis to a range of leading UK and international organisations. For over a decade, our open-source research and analysis have had far-reaching impacts for both public-and private-sector clients in the UK and across the world. Our team brings subject-matter expertise and drive for excellence to every project, with an ability to work in over forty languages. Ridgeway clients benefit from our deep, specialist knowledge and our ability to cut through the noise to deliver valuable, verifiable insight.

Contact us about our work or collaboration opportunities: info@ridgeway-information.com