Written evidence from Statewatch (NBB0052)

Statewatch is a non-profit-making voluntary group founded in 1991 comprised of lawyers, academics, journalists, researchers and community activists. Our European network of contributors is drawn from 18 countries. We undertake and encourage the publication of investigative journalism and critical research in Europe in the fields of the state, justice and home affairs, civil liberties, accountability and openness.

We welcome the opportunity to provide input to the Joint Committee on Human Rights call for evidence for legislative scrutiny of the Nationality and Borders Bill. We echo the concerns of many organisations working on human rights, particularly the human rights of migrants and asylum seekers. As an organisation with expertise in the fundamental rights implications of digital structures and data processing, *Statewatch* calls the attention of the Committee to the following:

- How the proposed Article 60 of the Nationality and Borders Bill would impact on rights to a private and family life (Article 8 ECHR), freedom from discrimination in the enjoyment of human rights (Article 14 ECHR), and the UK's obligations under the Geneva Convention.

Overview

Section 60: Electronic travel authorisations

Section 60 of the Nationality and Borders Bill states:

> *"(1) The Secretary of State may make regulations about electronic travel authorisations.*
>
> *(2) The regulations may in particular make provision—*
>
> *(a) requiring an individual to have an electronic travel authorisation before travelling to the United Kingdom,*
>
> *(b) imposing civil penalties on owners of ships or aircraft which carry individuals in breach of a requirement to have an electronic travel authorisation,*
>
> *(c) about biometric information to be provided with an application for an electronic travel authorisation, and*
>
> *(d) about the recognition of electronic travel authorisations issued in the Channel Islands and the Isle of Man."*

The purpose of such a scheme would be to evaluate the eligibility of travellers who do not require a visa to enter the UK and prevent them from travelling should they not meet the desired requirements – in the words of the Home Office, "block the entry of those who present a threat to the UK."[1] Other countries operating such schemes include the USA (Electronic System for Travel Authorisation, ESTA), Canada (Electronic Travel

[1] https://www.gov.uk/government/publications/the-nationality-and-borders-bill-factsheet/nationality-and-borders-bill-factsheet

Authorisation (ETA) and Australia (Electronic Travel Authority, ETA). The EU is also in the process of developing a European Travel Information and Authorisation System (ETIAS).

Such systems, generally speaking, require that travellers fill out an online form with various items of personal data (e.g. name, address, occupation, education level, family details), and to make a number of declarations (e.g. whether they have any criminal convictions, or whether they have ever been involved in any form of terrorist activity). This information is then cross-checked against other national or international databases (e.g. those run by Interpol), and applications may also be subject to algorithmic profiling.[2] It is generally stored for a number of years and can be made accessible to other bodies, such as law enforcement agencies, subject to certain conditions. The introduction of such a scheme would represent a new barrier to international mobility, effectively introducing a form of visa for tens of millions of people that do not currently require one.

There is little public information on the effectiveness of these schemes. A 2016 report by the US Government Accountability Office cites a claim by the Department for Homeland Security's Assistant Secretary for International Affairs that over 165,000 ESTA applications had been denied since 2008 by cross checking applications with data on lost and stolen passports, "potentially preventing criminals or terrorists from using stolen passports to illegally enter the United States." The same official is reported as saying that "since 2008, CBP has denied over 4,3000 ESTA applications for national security concerns as a result of vetting against the Terrorist Screening Database and other terrorism-related databases."[3] However, it is unknown how many of those refusals were incorrect (and whether they were subsequently subject to successful appeal), nor what the number of refused ESTA applications is as a proportion of the total number.

The regulations provided for by Section 60 would be made by the affirmative resolution procedure. Statutory instruments subject to the affirmative resolution procedure may be the subject of debate in a Delegated Legislation Committee (DLC); they also require the assent of both houses if they are to become law. However, it is not possible for MPs to make amendments to the proposed instrument and it is extremely rare for statutory instruments to be rejected.[4] We are concerned that introducing an electronic travel authorisation scheme through such a procedure will not allow for the scrutiny and debate required, given the implications of such a scheme for the rights of tens of millions of foreign nationals.

The right to a private and family life (Article 8 ECHR)

The type of scheme proposed by the Bill would require the processing of a significant amount of personal data on vast numbers of people. It is also clear that the scheme may require the processing of biometric data, a particularly sensitive form of data that requires "specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms."[5]

---

[2] https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/

[3] https://www.gao.gov/assets/gao-16-498.pdf

[4] A 2013 report noted that just 16 of 165,000 (0.01%) of SIs were rejected over a 65-year period. https://regulation.org.uk/library/2013_The-Devil-is-in-the-Detail-exec_summary.pdf

[5] Recital 51, General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Any processing of personal data must be both necessary and proportionate. It must be asked what need there is for an electronic travel authorization system: can it be demonstrated that visa-exempt travellers present a particular "threat to the UK"? If so, what is the scale of that threat and does it justify impinging upon the rights of every visa-exempt traveller? Given the existence of other schemes that play a similar role (for example, requirement for airlines to communicate Passenger Name Record data to the authorities prior to departure), what would the added value be in introducing an electronic travel authorisation? The government must demonstrate that there is a clear need for such a scheme, something that it has not yet done.

Should such a scheme be proven necessary, it must then meet the requirement of proportionality – that is to say, the data processing must not go beyond that which is necessary to attain the desired ends. Herein lies the risk of the affirmative resolution procedure: it would not allow for meaningful parliamentary scrutiny and debate over the substance and functioning of an electronic travel authorisation scheme, leaving the Home Office with significant discretion.

This gives rise to significant concerns, given the way the Home Office has dealt with the personal data of citizens and non-citizens alike (in particular with regard to the Windrush scandal and, in a matter particularly relevant for this case, in its use of an algorithm that discriminated on the basis of nationality to assist in processing visa applications[6]). In the context of the Home Office's data strategy, which foresees a significant increase in data-sharing between the bodies and agencies of the Home Office and other government departments, MPs should be cautious about granting the Home Office such a level of discretion over the parameters of an electronic travel authorisation scheme.

The right to freedom from discrimination (Article 14 ECHR)

Travel authorisation systems generally make use of profiling tools in order to inform decision-making about a person's eligibility to enter the territory. As noted above, it has been demonstrated that the Home Office has used racist, discriminatory algorithms for processing visa applications. The type of scheme being proposed provides ample scope for similar techniques to be applied, pointing again to the need for greater scrutiny both of the legislation establishing such a system, and – should it be approved – how it functions in practice.

Obligations to protect refugees and the prohibition on *refoulement* (the 1951 Refugee Convention)

The introduction of an electronic travel authorisation may create a barrier to those needing to flee countries owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion. Denial of an ETA to an individual needing to flee a country would compel them to undertake a more dangerous route, for example, by using the services of people smugglers.

The data-sharing involved in the travel authorisation system may in itself put a person at risk. Many such schemes involve cross-checking applicants' data with Interpol's databases on travel documents, which have been misused by states seeking to persecute their citizens

[6] Public Technology, 'Home Office halts use of visa algorithm after legal challenge to 'racist' system', https://www.publictechnology.net/articles/news/home-office-halts-use-visa-algorithm-after-legal-challenge-%E2%80%98racist%E2%80%99-system; Foxglove, 'We won! Home Office to stop using racist visa algorithm', https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm

abroad.[7] The design of a travel authorisation system must take these risks into account to ensure adequate safeguards.

Conclusions

The Joint Committee's call for evidence includes the following questions:

- Is Home Office decision making in immigration matters that raise human rights concerns sufficiently independent and rigorous to ensure that human rights are properly respected?
- Is the Bill otherwise compliant with the European Convention on Human Rights (ECHR)?

We do not believe that the Home Office can or should be trusted with the sensitive personal data of tens of millions of people who do not currently require any form of travel authorisation to travel to the UK. At a very minimum, MPs must demand proper legislative scrutiny over the proposed system in order to ensure that safeguards, checks and balances are properly accounted for in order to ensure that human rights are fully respected and that it is compliant with the ECHR.

Article 60 introduces a situation in which decision making on arrivals to the UK will be made by the same body, the Home Office, as the one establishing safeguards on the processing of biometric and personal data. This does not provide sufficient independence and risks jeopardising rights to freedom from discrimination and to a private and family life. The Bill is therefore not compliant with Articles 8 and 14 of the ECHR.

17/09/2021

[7] https://stockholmcf.org/wp-content/uploads/2017/09/Abuse-Of-The-Interpol-System-By-Turkey_September-20-2017.pdf