

Professor Tim J Wilson, FCSFS, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School – Written evidence (EBM0006)

1.. Introduction

1.1 This evidence is based on criminal justice research, chiefly: (a) cross-jurisdictional data sharing¹ and (b) the reliability of criminal evidence produced by AI/ML (Artificial Intelligence/Machine learning) learning trained applications.² This work is relevant to the informational, technological and ECHR/rule of law interfaces between electronic border management (EBM) and criminal justice. It may be helpful for the inquiry because the 'hard wiring'³ and use of international criminal justice cooperation appears to be much more transparent than EBM, especially in the UK ETA system.

1.2 The submission refers to the following topics/questions in the call for evidence: global trends; the purpose of electronic authorisation; potential risks; the impact on individuals and the CTA. The focus is selective, however, by considering aspects of those issues where access to detailed information about how electronic border management (EBM) is configured and is intended to work might assist independent inspection, democratic accountability and judicial supervision.

2. Global trends: the purpose of electronic authorisation and its wider context

2.1 EBM is a response to decades of intensified globalisation. Massive increases in international travel and, sometimes within borderless travel areas, has resulted in initiatives by wealthier countries to balance the economic and other benefits of this development by (a) managing greater exposure to a comparatively small - but hard to detect - risk of crime and terrorism (including state sponsored threats to asylum seekers in the destination country) and (b) balancing costs incurred and effectiveness of border management. EBM is critical for this balancing act by extending the time and location of non-visa border control to well before the day and place of departure, thus enabling more effective scrutiny for multiple purposes⁴ by properly trained/resourced professional staff.

¹ See, e.g.: Wilson, Tim J (2016), 'Criminal Justice and Global Public Goods: The Prüm Forensic Biometric Cooperation Model', *The Journal of Criminal Law*, 80 (5) 303-326.

² See, e.g., Tim J Wilson, Jesper Bergman, Adam Jackson and Oliver B Popov, 'Preventing machines from lying: why interdisciplinary collaboration is essential for understanding artefactual or artefactually dependent expert evidence' *the Journal of Criminal Law* (2024), online first at DOI: 10.1177/00220183231226087.

³ For a useful summary see: House of Commons Justice Committee, *Implications of Brexit for the justice system* (2016-17, HC 750) paras 6-18. The term 'hard wiring' emerged during oral evidence on 10/01/1.

⁴ (a) Entry/re-entry control/exit (including migration policy enforcement); (b) criminal justice (e.g. the prevention of impunity from judicial decisions); (c) vulnerable person protection: safeguarding/child welfare (under both public and family law) preventing trafficking, both children and adults and dissidents/asylum seekers; (d) national security; and, especially during pandemics, (e) public health.

2.2 As the term 'electronic authorisation' indicates, such arrangements are powered by the digitalisation of communication and personal information. Implementing or upgrading EBM is time consuming, expensive and difficult.⁵ There are also major limits to what is achievable, legally and operationally by computer science alone, and democratic and judicial supervision must keep pace with AI/ML to protect human rights, including data privacy. Effective supervision requires information about how electronic border control is configured and is intended to work. Its operation must be open to regular, well resourced (competency range as much as capacity) independent inspection.

2.3 There are two other significantly interrelated trends that have a major bearing on human rights, including those of UK citizens and residents.

(a) Border control cannot be 100% effective and therefore needs to be backed up by effective international criminal justice (CJ) cooperation measures (i.e. to access information that might identify suspects, facilitate the cross-jurisdictional surrender of suspects, pre-trial supervision and mutual recognition of penalties etc.). Even at the sub-optimal Brexit level continuation of UK-EU CJ cooperation under the Trade and Cooperation Agreement, this is conditional on effective domestic remedies for any ECHR breaches and a broader rule of law EC Data Adequacy determination.⁶

(b) There is also an obligation to provide reciprocal assistance to partner states who contribute to the effectiveness of border control. This includes a mutual interest in preventing and responding to crime and other threats and reporting signs of potential flaws in partner states' border controls.⁷ For individuals EBM (in contrast to passport authorised travel) is more intrusive and subject to frequent (every 2 or 3 years) data up-dating/refreshment. Reciprocity (especially more effective data sharing; though how is unclear⁸) may result in restrictions, sanctions and increased exposure to reopened UK investigations resulting because of offences committed elsewhere by UK citizens and residents.

The significance of mutual trust, including the effectiveness of human rights/data protection, not least in respect of departing citizens and residents, means that UK EBM is likely to remain differentiated between non-visa and visa entry, with scope to quickly withdraw non-visa entry or add additional targeted/general restrictions, e.g., in response to political developments and pandemics.

⁵In addition to the actual development of new systems, these may need to be integrated with other systems (including operationally fragile legacy systems) run by different contractors and physical infrastructure at the point of entry may need to be modified. See, e.g., [Digital Services at the Border \(nao.org.uk\)](https://nao.org.uk) and, for context about lengthy delays etc., [Biometrics | Homeland Security \(dhs.gov\)](https://www.gov.uk/government/news/biometrics-at-heathrow).

⁶ Tim J Wilson 'EU-UK criminal justice and security cooperation after Brexit: A perspective' *Forensic Science International: Synergy* 2021, Vol. 3,100144

⁷ [Former BA employee allegedly orchestrated £3m immigration scam from Heathrow check-in desk | Immigration and asylum | The Guardian](https://www.theguardian.com/uk-news/2022/feb/17/former-ba-employee-allegedly-orchestrated-3m-immigration-scam-from-heathrow-check-in-desk)

⁸ See, eg: 'any information supplied [about convictions] can be quickly checked against the ETIAS security database [Applying for ETIAS with a Criminal Record](https://etias.europa.eu/) . It is unclear (for both EU and UK EBM) (i) how extensive the records will be for third country residents and (ii) the circumstances when searching will be allowed.

3. Potential EBA risks: interoperable data sharing and data processing safeguards

3.1 Digitalisation and international data sharing are powerful tools for enabling better informed decision making but it is important that information appearing on computer screens is not automatically taken at face value. Administrative errors, such as linking biometric data to another person's alphanumeric data, can result in erroneous alerts and interoperability can perpetuate such errors in other states' databases. Regimes that systematically abuse human rights, including by extra-judicial killings, can manipulate data sharing with human rights compliant states by labelling dissidents as criminals or national security threats. Database interoperability also increases the risk of malicious state-linked hacking. Despite reforms in 2013 intended to address the political abuse of Interpol Red Notices transparency about processing is substandard and the system needs fundamental reform to avoid incorrect personal data being accessible internationally.⁹

3.2 Considerable concerns have been expressed in civic society¹⁰ and academic literature¹¹ about how the database interoperability – that must be a critical element of EBM - increases risks faced by vulnerable individuals. This is also significantly relevant for many other travellers, including citizens and residents departing from the UK. It is also unclear for UK EBM, how standard data processing safeguards – including the normal presumption against solely automated decisions and the different levels of safeguards between criminal justice/security processing (lower) and for entry/migration decisions (higher) - will be observed in practice and fully open to independent inspection.

4. The impact of EBA on individuals: criminal records

4.1 Home Office staff instructions mandate entry refusal following a conviction for a criminal offence in the UK or overseas that resulted in a custodial sentence of 12 months or more. The only stated exceptions are for conduct that is not criminal in the UK, 'including homosexuality or membership of a trade union'.¹² In contrast, Germany takes a discretionary approach that is engaged at a higher minimum sentence threshold and only for specified categories of offences.¹³

4.2 Such an approach compounds the effects of discrimination against third country nationals in the UK criminal justice system. During the period of UK EU membership, attempts were made to address such discrimination through a coherent and complementary legislative package. These measures disappeared with Brexit,¹⁴ thus increasing the prospect that national status alone might tip

⁹ [Fundamental rights and the interoperability of EU information systems: borders and security | European Union Agency for Fundamental Rights \(europa.eu\)](#); [Joint submission to European Commission on cross-border sharing of data for mixed criminal law and immigration control purposes | Privacy International](#); and [Ensuring the rights of EU citizens against politically motivated Red Notices | Think Tank | European Parliament \(europa.eu\)](#).

¹⁰ See, e.g., Privacy International submission at n5 above.

¹¹ See, e.g., Elrick, L. (2021). Finding the Balance between Security and Human Rights in the EU Border Security Ecosystem. *European Journal of Law and Technology*, 12(1), 1-42.

¹² [Grounds for refusal: criminality \(accessible\) - GOV.UK \(www.gov.uk\)](#).

¹³ [Applying for ETIAS with a Criminal Record](#).

¹⁴ Tim J Wilson, 'Prisoner Transfer Between the UK and EU27: A "Striking" Omission from the

criminal justice decisions towards a disposal above the entry threshold level. Contrary to the UK's international obligations,¹⁵ women prisoners are particularly at risk in this respect.¹⁶ More generally the thinking behind the Home Office rules fails to acknowledge substantial international differences in sentence severity/criminalisation and Alexei Navalny would have had to be denied entry.¹⁷

4.3 It is unclear whether the mandatory/low-threshold conviction rules are built into ETA system code and incapable of being changed without expensive and time-consuming contractual changes.

5. *The limitations of EBM effectiveness: identity misappropriation*

5.1 The more intrusive and regular data refreshment approach of ETA, ETIAS and similar systems are intended to enhance security. How these arrangements are linked to a passport holder's demographic profile, however, could be a significant weakness. UK passports are issued on the production of a birth certificate (orderable online) and with a generally unverifiable/unverified attestation of identity. The risks posed by this were illustrated by how undercover police officers, mimicking a process publicised in a novel and film, stole the identity of dead children.¹⁸

5.2 Just as personal data will be refreshed every two/ three years for ETA and ETIAS, perhaps the UK governments could better guarantee the demographic profile encapsulated in a passport if it is linked with dynamic citizenship records (eg health, social welfare/state pension contributions/payments and US style annual tax returns universal passport holder obligation).¹⁹

6. *Home Office capability and cooperating with the inspectorate*

6.1. Estimating the accuracy of facial recognition algorithms used in e-gates is a complex subject that uses different measures. Results will vary between laboratory and operational conditions, different releases of propriety software, variations in the operating environment, operator changes to the classification thresholds (i.e. the correlation threshold set to register a positive result and thus opening a gate) and the facial characteristics and stance of gate users.²⁰ When questioned by Immigration and Borders inspectors about such issues,²¹ however, statements about performance appear to me to have reflected generalised results for the best performing algorithms originally published in high quality US

TCA?' in Gemma Davies and Helena Farrand-Carrapico (eds.) *UK-EU Police and Judicial Cooperation Post-Brexit* (forthcoming).

¹⁵ *United Nation Rules for the Treatment of Women Prisoners and Non-Custodial Measures for Women Offenders* (The 'Bangkok Rule's) (New York, 21 December 2010).

¹⁶ *Still No Way Out: Foreign national women and trafficked women in the criminal justice system* (London, PRT, 2018).

¹⁷ Sentenced in 2022 to 9 years imprisonment for (fully UK equivalent offences) fraud and contempt. [Alexei Navalny sentenced to 9 more years in prison after fraud conviction | Alexei Navalny | The Guardian](#).

¹⁸ M Creedon, *Operation Herne: Report 1 - Use of covert identities* (Derbyshire Constabulary, 2013).

¹⁹ The data itself would not be transferable to another state.

²⁰ Wilson et al. 2024, n.2 above

²¹ ICIBI, *An inspection of ePassport gates (June 2020 – January 2021)*

National Institute for Science and Technology (NIST) algorithm testing under highly standardised/clearly artificial laboratory conditions.²²

6.2 More operationally orientated discussions with inspectors about e-gate performance rightly acknowledged that the algorithms are improving rapidly, and false negatives, which annoy travellers, far exceed false positives that would breach entry security. Possibly there is a risk of cognitive bias (much researched in equivalent criminal justice contexts) in such circumstances. Staff dealing frequently with false negatives may be conditioned by this into treating a correct rejection as just another false negative. It might be better to step back to other NIST related criminal justice research that suggested that a single forensic facial examiner working with a high-quality algorithm was more accurate than combination of even two examiners. As the inspectors noted this is provided for but not always used. EBM more generally perhaps needs to be seen as enabling a better collaboration among humans and between humans and machines than earlier border control systems.²³ This perhaps runs counter to an almost default assumption that all technological investment will generate substantial staff savings. This assumption largely stems from research into the economic impact of AI/ML in the manufacturing and services industry. Recent research has suggested that— at least in the area studied - – that ‘routine tasks do not necessarily disappear ... and challenge the assumption that automation and digitalisation contribute to productivity in exclusively positive ways’.²⁴

6.3 It is difficult to understand why the Home Office routinely declined to allow the Inspectorate general access to information about contractual arrangements with suppliers, citing 'commercial sensitivity'.²⁵ They were denied access to details of the service level agreements (SLAs) or key performance indicators (KPIs) and the financial consequences of not meeting those requirements.²⁶ Public sector clients are not under any kind of duty to hide how performance is judged or to keep confidential details of actual failures and their financial consequences. Indeed, such behaviour might be challenged (possibly in court in some jurisdictions) as complicity with a contractor to evade the latter's' fiduciary duties to shareholder and potential investors. It would also contradict the obligation to disclose non-performance deductions to Parliament, either directly²⁷ or via the NAO.

7 The Common Travel Area (CTA)

7.1 The absence of UK access to the main EU criminal justice/security/border control databases (SIS II, ECRIS and ECRIS-TCN) under the Trade and Cooperation Agreement, appears to leave Ireland exceptionally vulnerable, as an

²² See, eg: Mei Ngan et al., *NISTIR 8331 Draft Supplement - Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms* (2022)

²³ P Jonathan Phillips et al., 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms', *Proc Natl Acad Sci U S A*, .2018 Jun 12;115(24):6171-6176

²⁴ Ribeiro et al., 'The Digitalisation Paradox of Everyday Scientific Labour: How Mundane Knowledge Work is Amplified and Diversified in the Biosciences' (2023) 52 *Res Policy* 104607.

²⁵ <https://committees.parliament.uk/writtenevidence/128522/pdf/> on 05/02/24.

²⁶ ICIBI, *A re-inspection of ePassport gates* (2024) para 7.15 and *An inspection of ePassport gates (June 2020 - January 2021)* page 2 and para 6.3.

²⁷ For example, in response to several PQs about financial penalties imposed under Home Office prison management contracts in the 1990s.

EU MS, to the arrival of some non -UK citizens who would otherwise have been denied entry had they not travelled there via the CTA from the UK.

14 March 2024