An infrastructural Brussels effect

The translation of EU law into the UK's digital borders

Computer Law & Security Review 55 (2024) 106057

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

An Infrastructural Brussels Effect: The translation of EU Law into the UK's digital borders

Gavin Sullivan [a,*], Dimitri Van Den Meerssche [b,1]

[a] Reader in International Human Rights Law and UKRI Future Leaders Fellow at Edinburgh Law School, The University of Edinburgh, Edinburgh, United Kingdom
[b] Senior Lecturer in Law and Fellow of the Institute for Humanities and Social Sciences at Queen Mary University, London, United Kingdom

ARTICLE INFO

Keywords:
Digital borders
AI and algorithmic governance
Data Infrastructures
Brussels Effect
PNR data
Infra-legalities

ABSTRACT

This article gives an account of the legal standards and safeguards that guide and constrain the current design of the UK's digital borders. Based on an empirical engagement with the development of *Cerberus* – an advanced risk-based analytics platform aimed at the detection of previously 'unknown' threats – the article presents a dual argument. On the one hand, it provides an account of the remaining salience and extraterritorial reach of EU law in setting standards for the collection, retention, processing and sharing of Passenger Name Records (PNR) data in the UK. This PNR data is a constitutive component of the digital border. Through the EU-UK Trade and Cooperation Agreement (TCA), the UK is now bound to comply with the rather stringent legal safeguards developed by the CJEU (in Opinion 1/15) on the retention and automated processing of PNR data. Our analysis shows the different channels through which EU law obtains this extraterritorial reach, how compliance can be monitored and enforced, and, crucially, how it has influenced and constrained the technical design of the UK's digital borders – a salient and unexplored phenomenon that we describe as an *Infrastructural Brussels Effect*. Yet, on the other hand, the article empirically shows that this is not merely a process of norm diffusion and extra-territoriality. Once legal standards become infrastructurally embedded in Cerberus, we witness normative translations and sociotechnical shifts with important legal and political consequences. Legal standards on 'reasonable suspicion' and the 'objective evidence' of 'risk', we argue, are given specific meaning through a logic of relational inference and algorithmic pattern detection (leading to forms of 'concern by association'). By studying the entanglements between legal norms and material infrastructures – an approach we describe as infra-legalities – these normative effects become visible and contestable, providing a productive site for the sociolegal study of law and algorithmic governance.

> 'I think the European Union Member States and the European Commission are very interested to know how we're solving the conundrum that they've posed to us'
>
> (Interview with UK Home Office, May 2023).

1. Introduction – norm diffusion and sociotechnical translation in the building of digital borders

In its 2025 Border Strategy, the UK government draws the contours of how its post-Brexit borders will be 'transformed'.[2] This strategy, launched in December 2020, sets out an ambitious 5-year strategic plan for harnessing advanced digital technologies to rebuild borders as 'resilient ports of the future' that facilitate better pre-emptive security. The strategy seeks to harness 'the power of technology and innovation' to create a contactless bordering system that will 'revolutionise crossing the border for traders and travellers' and 'improve the UK's ability to detect threats before they reach the border'.[3] This is a border that 'embraces innovation', 'extract[s] maximum value from border data', develops and relies on 'advanced detection technologies to identify threats', and

* Corresponding author.
E-mail addresses: g.sullivan@ed.ac.uk (G. Sullivan), d.vandenmeerssche@qmul.ac.uk (D. Van Den Meerssche).

[1] The co-authors contributed equally to the writing of the paper.
[2] HM Government, *2025 UK Border Strategy* (2020).
[3] *Ibid.*, 45, 20, 23, 13.

https://doi.org/10.1016/j.clsr.2024.106057

Available online 10 October 2024

'maximis[es] data driven, automated decision making'.[4] It hinges on an infrastructure through which all incoming and outgoing traveller data will be collected in advance of travel, fused together with other Home Office data, customs and freight data, terrorism watchlist data and other police and security databases (both domestic and international), and passed through a 'single window' for analysis using 'advanced analytics-enabled risk engines'.[5] The digital border thereby relies on the 'real-time sharing of data-driven risk insights across government departments'.[6]

Based on this collection and interconnection of data, the strategy promises to 'develop advanced new risking systems to target interventions more effectively, using emerging technologies like AI-driven decision making'.[7] These 'advanced risk analytics' will 'ingest data from a wide range of sources' and 'automate the risking process wherever possible'.[8] At the heart of this digital border infrastructure for risk analysis and pre-emption is the use of Advance Passenger Information (API) and Passenger Name Record (PNR) data. The strategy states that API data enables 'accurate demand modelling, watchlisting checks for known threats and the targeting of potential threats at the border'.[9] Potential or previously 'unknown' threats are primarily detected through the use of 'advanced risk analytics' tools to analyse PNR data.[10] The focus on both 'known' and 'unknown' threats is reflected in the design of two new UK border control systems: Helios (an updated and federated watchlisting system) and Cerberus [an advanced risk-based analytics platform collaboratively built with British Aerospace Engineering (or BAE)]. The design of Cerberus aligns with widely observed tropes of algorithmic governmentality: it displays an ambition to anticipate and pre-empt unknown risks through a distillation of data patterns.[11] The target of security interventions thereby emerges as a cluster of inferred attributes – or correlated 'characteristics' – that are relationally tied to 'anomalies' or 'abnormalities' detected in data through advanced analytics.[12]

Yet, in contrast to these imaginaries of a frictionless flow of data fuelling new modalities of algorithmic anticipation, the design and implementation of the UK's digital border – of both Helios and Cerberus – are fraught with frustration resulting from sociotechnical failure, internal administrative resistance, and legal limitations. In this article, as part of a broader research project on digital bordering, we pay attention to this final aspect: how collecting, sharing, and using data is legally limited in a post-Brexit landscape. In doing so, we focus specifically on how the access and exchange of PNR data – a key component of the UK digital border infrastructure – remains regulated and curtailed by EU law even after (and, as we argue, *particularly* after) the UK's exit. How is the development of advanced machine learning (ML) infrastructures like Cerberus enabled and constrained by legal norms? How are recent CJEU decisions on the legality of processing PNR data translated in technical use-cases for the development of systems like Cerberus based on artificial intelligence (AI)? Which institutional, sociotechnical, and regulatory processes are involved in this translation and in constructing this digital bordering capability? How are the post-Brexit relations between the UK and the EU shaping systems like Cerberus? What are the key questions we should be asking when we study this algorithmic border infrastructure in motion? These are salient and contentious legal and political questions. The debate on PNR data exchange goes to the heart of the tension between a post–9/11 security logic and the elaboration of privacy protection standards (where the CJEU has taken an assertive stance in recent decisions). It displays how private actors are enrolled in global security and counterterrorism projects and how this repurposing and circulation of commercial data is the source of geopolitical discord and struggle. Finally, and at the core of our argument, it reveals a dual dynamic where legal norms shape the design of sociotechnical systems (*the regulation of digital infrastructure*) and where the design and material practices of sociotechnical systems in turn mediates, translates or supplants these legal frameworks and produces distinctive normative effects (*digital infrastructure as regulation*).[13]

The 'conundrum' referenced in the epigraph points to the central puzzle of this article: how does EU law, in a post-Brexit sphere of presumed autonomy, regulate the design of the UK's digital borders and how do the choices made in this design process impact the meaning of these legal norms? On the one hand, the article provides an account of the enduring, perhaps expanded, normative power of EU law in relation to the UK's collection, retention and processing of PNR data.[14] To maintain access to EU PNR data, the UK, as a third country, now has to comply with the terms of the EU-UK Trade and Cooperation Agreement (TCA).[15] These

[4] *Ibid.*, 7, 20, 21.

[5] *Ibid.*, 21. This focus on interoperability and data sharing resonates with the legislative framework for the EU's digital borders. See Council Regulation 2019/817, OJ L 135/27 (establishing a framework for interoperability between EU information systems in the field of borders and visa); Council Regulation 2018/1240, OJ L 236/1 (establishing a European Travel Information and Authorisation System (ETIAS)).

[6] 2025 UK Border Strategy, *supra* note 2, 41.

[7] *Ibid.*

[8] *Ibid.*

[9] *Ibid.*

[10] PNR data is a key input in the 'advanced risk analytics engines' referenced extensively throughout the UK Border Strategy and analysed in this paper. On the use of PNR to detect previously unknown threats see, for example: European Commission, Passenger Data. Available at: bit.ly/3vWEEwD (last accessed October 2024). This discusses analysing PNR data to allow authorities 'to detect suspicious travel patterns and identify associates of criminals and terrorists, in particular those *previously unknown*'). Emphasis added.

[11] Cf. Louise Amoore, *The Politics of Possibility: Risk and Security beyond Probability* (2013); Antoinette Rouvroy and Bernard Stiegler, 'The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law' (2016) 3 *La Deleuziana – Journal of Philosophy* 6; Fleur Johns, 'Data, Detection, and the Redistribution of the Sensible in International Law' (2017) 111 *American Journal of International Law* 57; Claudia Aradau and Tobias Blanke 'Politics of prediction: Security and the Time/Space of Governmentality in the Age of Big Data' (2017) 20 *European Journal of Social Theory* 373; Dimitri Van Den Meerssche, 'Virtual borders: international law and the elusive inequalities of algorithmic association' (2022) 33 *European Journal of International Law* 171.

[12] This aligns with Louise Amoore, 'The Deep Border' (2021) *Political Geography* 1; Claudia Aradau and Tobias Blanke, 'Governing Others: Anomaly and the Algorithmic Subject of Security' (2017) 3 *European Journal of International Security* (2017) 1; Engin Isin and Evelyn Ruppert, 'The Birth of Sensory Power' (2020) 7 *Big Data & Society* 1; Marie Petersmann and Dimitri Van Den Meerssche, 'On phantom publics, clusters, and collectives: be(com)ing subject in algorithmic times' (2024) 39 *AI & Society* 107.

[13] This observation, at the heart of the article, builds on an emerging field of scholarship that studies infrastructure as legal and regulatory ordering. See: Benedict Kingsbury, 'Infrastructure and InfraReg: On Rousing the International Law "Wizards of Is"' (2019) 8 *Cambridge International Law Journal* 171; Gavin Sullivan, 'Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage', (2022) 49 *Journal of Law and Society* S31; William Hamilton Byrne, Thomas Gammeltoft-Hansen and Nora Stappert, 'Legal Infrastructures: Towards a Conceptual Framework', *German Law Journal* (in press); Fleur Johns, 'On Dead Circuits and Non-Events', in Ingo Venzke and Kevin Jon Heller (eds.), *Contingency in International Law – On the Possibility of Different Legal Histories* (2021); Gavin Sullivan and Dimitri Van Den Meerssche, 'The Legal Infrastructures of UK Border Control - Cerberus and the *Dispositif* of Speculative Suspicion', *German Law Journal* (in press); Dimitri Van Den Meerssche, 'The Multiple Materialisms of International Law' (2023) 11 *London Review of International Law* 197.

[14] This paper provides a sociolegal snapshot of emergent infra-legal dynamics in the current post-Brexit juncture, rather than a definitive normative account of enduring UK-EU regulatory relations on PNR data governance. For more detailed analysis of these relations see, for example: Valsamis Mitsilegas, 'Extraterritorial Immigration Control in the 21st Century: The Individual and the State Transformed' in Bernard Ryan and Valsamis Mitsilegas, *Extraterritorial Immigration Control: Legal Challenges* (2010) 39.

[15] Trade and Cooperation Agreement [2021] OJ L 149/719 (referred to below as 'TCA').

terms – and the relation between the EU and the UK is unique in this sense – directly incorporate the rather stringent standards of CJEU Opinion 1/15 on the envisaged PNR agreement between Canada and the EU.[16] To keep access to EU PNR data, one of the key figures behind the design of the Cerberus system noted, the UK has become 'a recipient of the extraterritoriality of EU law'.[17] In Section 2, we describe the operations of this dynamic – a specific form of the *Brussels Effect* – in the design of the UK's digital borders, and particularly in relation to the contentious questions of data retention and the automated processing of data.[18] This politically controversial process of norm diffusion resonates in the fraught negotiations over the access and exchange of PNR data more broadly.

On the other hand, when this framework of EU law is embedded in sociotechnical systems of decision-making, we observe salient normative translations. Our empirical engagement with the construction of Cerberus gives unique insight into the reach of EU law in shaping the material design of the UK's digital borders – a dynamic we describe as an *Infrastructural Brussels Effect*. This dynamic is reflected in the formation of the team responsible for the development of Cerberus, the legal constraints that determine this process, and the legal problems which it is designed to resolve. Yet, we simultaneously argue that key elements of this legal framework – such as the reference to 'reasonable suspicion' or the 'objective criteria' from which 'risk' can be 'inferred' – are substantively shaped and redefined in the practices of data analysis and ML from which 'patterns' and 'characteristics' of 'abnormality' can be distilled. Existing accounts have shown how EU law and regulation on the use of PNR data has shaped digital borders in the UK and elsewhere, revealing the legal governance of digital bordering infrastructures. Our sociolegal analysis in this paper seeks to go further, by showing how legal norms associated with the use of PNR data are reconfigured through the sociotechnical affordances of Cerberus – that is, to analyse the underexplored dynamics through which legal norms and principles are given effect and reshaped into novel regulatory amalgams through or by emergent digital infrastructure.[19] In Section 3, we describe these contentious dynamics of norm diffusion and sociotechnical translation in detail.

In addition to this substantive engagement on the adoption and translation of EU law in the design of Cerberus, this article also makes a broader methodological intervention on how to analyse and evaluate the relation between law and emergent forms of algorithmic governance.[20] This relation is often framed in terms of how law governs, or ought to govern, AI systems.[21] This literature, and the normative debates it sparks, are crucial but risk missing out on what we think is a key part of the algorithmic governance story. Law is not outside these sociotechnical arrangements governing AI systems from afar – it is an internal and co-constitutive element. It creates the conditions of possibility for algorithmic governance systems to emerge and it is reshaped through its relational entanglement within them – an entanglement that gives rise to distinctive and novel forms of regulatory ordering that require empirical exploration. To capture these co-constitutive relations, the article uses an infra-legalities approach.[22] This sociolegal, method assemblage is elaborated in detail elsewhere and only briefly referenced here. In short, it entails an 'ontological shift towards a world of process and relations' where algorithms or algorithmic systems do not appear as discrete objects with inner logics and bounded properties, but as relational compositions between human and non-humans elements through which agency emerges.[23] In this relational approach, law is not treated as a bounded normative phenomenon but engaged through the processes, techniques and relational networks that give it specific substance in practice.[24] Drawing from relational and materialist-orientated scholarship in Science and Technology Studies (STS), Critical Infrastructure Studies, Actor Network Theory and governmentality scholarship, an infra-legalities approach decentres the law and reorientates empirical focus towards emergent and dynamic processes of legal and regulatory ordering and sociotechnical practice.[25]

Exploring the forms of normative friction and translation these relations entail, in this article we ask how law is both reconfiguring and being reconfigured through AI-driven bordering infrastructures like Cerberus. This allows critical investigation of how law is metabolized and given effect through novel and emergent infrastructures of algorithmic governance, and of the political stakes involved in knowing and governing security risks in this way.

2. The Price of PNR data: from Brexit to the Brussels Effect

> 'if we hadn't had the agreement, we wouldn't have had any data'
> (Interview with UK Home Office, April 2022)

Systems such as Helios and Cerberus – the twin components of the UK's digital border innovation – display a remarkable data hunger. This is unsurprising considering the centrality of data analysis in the practices of pre-emptive security that manage and modulate the movement of goods and people.[26] In relation to this reliance on the frictionless flow of data, Brexit posed a specific problem. As a report by the EU Committee in the UK House of Lords noted in this context, 'the continued sharing of PNR data between the UK and EU Member States was of critical importance to law enforcement agencies'.[27] In the post-9/11 period, this data – originally collected for commercial purposes – has been repurposed as a 'criminal intelligence tool' used for both the pre-emption of 'known' threats and the detection of behavioural patterns signalling

[16] CJEU, Opinion 1/15 of the Court (Grand Chamber), 26 July 2017 (referred to below as 'CJEU Opinion 1/15').

[17] Interview with UK Home Office, May 2023.

[18] This is a reference to Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (2019). In this article we think with this trope beyond the substantive scope of Bradford's empirical analysis – reflecting on its workings in the sphere of global security governance in a post-Brexit context.

[19] Sullivan *supra* note 13. On regulation of/regulation through infrastructure see: Laura DeNardis and Francesca Musiani, 'Governance by Infrastructure', in Francesca Musiani et al (eds) *The Turn to Infrastructure in Internet Governance* (2015).

[20] This intervention is central to the UKRI infra-legalities project of which this empirical research is part of: www.infra-legalities.com (last accessed October 2024).

[21] This includes a variety of legal perspectives. See, for example: Eyal Benvenisti, 'EJIL Foreword – Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29 *European Journal of International Law* 9; Nathalie Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 *Internet Policy Review* 1; Simon Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (2021). A distinct strand of writing in this regard juxtaposes the logic of data-driven governance with the normative logic of the rule of law. See, for example, Mireille Hildebrandt, 'Law as Information in the Era of Data-Driven Agency' (2016) 79 *Modern Law Review* 1; Laurence Diver, 'Digisprudence: The Design of Legitimate Code' (2021) 13 *Law, Innovation and Technology* 325.

[22] Sullivan *supra* note 13.

[23] Taina Bucher, *If … Then: Algorithmic Power and Politics* (2018), 48.

[24] Alain Pottage, 'The Materiality of What' (2012) 39 *Journal of Law and Society* 167.

[25] See, for example: Geoffrey Bowker and Susan Leigh Star, *Sorting Things Out: Classification and its Consequences* (1999); Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (2007); Thomas Lemke, *The Government of Things: Foucault and the New Materialisms* (2021); Nikolas Rose and Marianna Valverde, 'Governed by Law?' (1998) 7(4) *Social and Legal Studies* 541.

[26] See, for instance: Amoore, *supra* note 11; Dennis Broeders and Huub Dijstelbloem, 'The Datafication of Mobility and Migration Management', in Irma Van der Ploeg and Jason Pridmore (eds.), *Digitizing Identities: Doing Identity in a Networked World* (2016).

[27] House of Lords, Beyond Brexit: Policing, Law Enforcement and Security, European Union Committee, 25th Report of Session 2019–21 (2021), 19. A former Head of UK Border Force described how PNR and API data had been 'of almost equal importance' operationally for counterterrorism purposes, when the UK was an EU Member State, as 'anything on SIS II" – that is, data shared via the Schengen Information System database.

risks as yet 'unknown'. It is also now the subject of global norms by the UN Security Council mandating its collection and analysis by states worldwide for counterterrorism and border security purposes.[28]

As an EU member state, the standards guiding the UK's access and use of this data were set out in the PNR Directive.[29] Yet, as a third country, these terms of data sharing had to be renegotiated precisely at a time when the CJEU was taking an increasingly assertive stance in setting the terms for the exchange of PNR data. In its negative evaluation of the envisaged agreement between Canada and the EU on the transfer and processing of PNR data (Opinion 1/15), the CJEU imposed strict restrictions on the retention and automated processing of data, and articulated conditions on oversight and the individual right to an effective remedy.[30] Considering the continued sharing of data between the EU and Canada, despite the absence of an updated agreement,[31] the UK is the sole country currently confronted with the stringent standards set out in Opinion 1/15. In this article, we focus specifically on the provisions related to automated data processing and data retention in light of their importance for the design of Cerberus as these were the key areas of concern that emerged from our empirical analysis of Home Office practice on this issue – as elaborated below and in the following section.

On the automated processing of PNR data, the TCA incorporates the standards set out in Opinion 1/15 (as recently elaborated and extended to the processing of PNR data inside the EU in the CJEU judgment *Ligue des Droits Humains*).[32] The TCA, first of all, incorporates the provision – already present in the envisaged EU-Canada agreement – that the UK 'shall not take any decision adversely affecting a natural person in a significant manner solely on the basis of automated processing of PNR data'.[33] Second, the TCA echoes Opinion 1/15 in setting specific rules regarding the databases as well as the 'pre-established models and criteria' that are being used for the automated processing of data. These models and criteria have to be 'non-discriminatory', 'specific and reliable' and – importantly – designed to 'arrive at results targeting natural persons who might be under a *reasonable suspicion* of involvement or participation in terrorism or serious crime'.[34] In *Ligue des Droits Humains,* the CJEU specified that the 'pre-determined' nature of the models and criteria would 'preclude[] the use of artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria'.[35] These restrictions, an interviewee from the UK Home Office observed, were 'flowing' directly from Opinion 1/15 'into our agreement with the EU'.[36] As we argue in the next section, the standards on automated processing set by the CJEU, via their adoption in the TCA, have thereby become 'business requirements' in the technical design of Cerberus.[37]

On the retention of PNR data, the incorporation of Opinion 1/15 in the TCA posed an even more urgent issue. Under the PNR Directive, the UK could maintain access to PNR data for up to five years.[38] This retention served a dual purpose: it enabled the performance of security checks and border control checks in light of historical data (as elaborated below), and it allowed for the systematic use of PNR data to define and verify pre-established models and criteria for automated processing.[39] Opinion 1/15, however, requires the immediate deletion of PNR data once passengers have left the country unless there is 'objective evidence' from 'which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure'.[40] Through the TCA, the UK is now bound by this obligation of immediate data deletion upon departure.[41] Yet, the TCA recognised that the UK's security systems were not adapted to this legal demand and, based on these 'special circumstances', granted a temporary derogation to integrate necessary 'technical adjustments'.[42] Having left the EU, in other words, the UK is now bound to the stringent standards of Opinion 1/15 and has to (re)design its technical systems, such as Cerberus.

Ironically, then, the post-Brexit position of the UK is not one of regulatory autonomy, but one heavily determined by what one interviewee within the Home Office described as the 'extraterritoriality of EU law … which we have adopted through the TCA because we had to'.[43] In its *Beyond Brexit* report, the UK House of Lords went even further,

[28] European Commission, On the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries, COM(2010) 492 (2010), 4. On this process of repurposing, see also: Elaine Fahey, Elspeth Guild and Elif Kuskonmaz, 'The novelty of EU Passenger Name Records (PNR) in EU Trade Agreements: On Shifting Uses of Data Governance in light of the EU-UK Trade and Cooperation Agreement PNR Provisions', (2023) 8(1) *European Papers* 273. On the UN Security Council's global legislation regarding PNR data, see: UNSCR 2396 (2017), para. 12.

[29] Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (EU PNR Directive) [2016] OJ L 119/132.

[30] CJEU Opinion 1/15, paras. 168-174, 190-211, 218-227, and 228-231. For an analysis of the importance of the opinion and the authority exercised by the CJEU in a post-9/11 era of digital surveillance, see Monika Zalnieriute, 'Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' (2018) 81 *Modern Law Review* 1046.

[31] European Parliament, Transfers of passenger name records (PNR) to Canada taking place despite the absence of an EU-Canada PNR Agreement, Parliamentary question E-000306/2022 by Sophia in 't Veld (Renew) (2022).

[32] CJEU, Judgment of 21 June 2022, Ligue des Droits Humains, C-817/19 (referred to below as 'CJEU, Ligue des Droits Humains'), paras. 193-213. This judgment, some scholars have argued, altered the PNR Directive 'beyond recognition'. Cf. Christian Thönnes, 'A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)' (23 June 2022) *Verfassungsblog*. It is important to trace the influence of these CJEU judgments to the EU PNR Directive as a key source of EU law influence. At this stage, in the wake of the judgment in Ligue des Droits Humains, key terms in this directive have become unsettled as new preliminary ruling requests are pending and member states continue to evaluate and debate the specific meaning of the judgment for their practices of data processing under the EU PNR Directive. These dynamics impact the fraught politics around PNR data transfers, with interviewees within the UK Home Office claiming to be addressing key concerns EU member states are only now fully facing.

[33] TCA, Article 551, para. 3. This provision echoes Article 15 of the envisaged EU-Canada Agreement as well as CJEU Opinion 1/15, para. 171.

[34] TCA, Article 551, para. 1 (emphasis added). Cf. CJEU Opinion 1/15, para. 172.

[35] CJEU, Ligue des Droits Humains, para. 194.

[36] Interview with UK Home Office, May 2023.

[37] Interview with UK Home Office, April 2022.

[38] It should be noted that the CJEU has judged this period of five years to go beyond what is 'strictly necessary' and indicated the need to delete data after six months unless, in analogy with Opinion 1/15, there exists 'objective evidence' from 'which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime'. See CJEU, Ligue des Droits Humains, paras. 254-260. This judgment is also informed by CJEU, Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18.

[39] Cf. CJEU Opinion 1/15, para. 198.

[40] *Ibid.*, para. 207.

[41] TCA, Article 552, para. 4.

[42] TCA, Article 552, para. 10-11. Importantly, even during this interim period there are strict safeguards in place: the data should be 'accessible only to a limited number of authorised officials and only where necessary to determine whether the PNR data should be deleted' (para. 11(a)). The 'deletion of the PNR data shall be ensured as soon as possible using best efforts', and all requests, access and refusal should be documented (para. 11(c-d)).

[43] Interview with UK Home Office, May 2023.

observing that 'now that the UK is a third country it will be held to higher standards by the EU in respect of data protection'.[44] It is important to situate these observations on the extraterritorial reach of EU law – as a particular instantiation of the *Brussels Effects* in the security sphere – within its broader geopolitical context. While we have signalled the fraught relationship between the EU and Canada in the wake of Opinion 1/15 – where PNR data continues to be shared in the absence of an updated agreement – the regulatory tensions and political discontent are perhaps most palpable in the PNR data negotiations between the EU and US.[45] At present, PNR data continues to be shared by the EU on the basis of a 2012 agreement, which defines the purposes for which this data can be used and sets standards including in relation to data retention, automated processing, non-discrimination, transparency, and redress.[46] The agreement automatically rolls over in periods of seven years 'unless one of the parties notifies the other … of its intention not to renew the Agreement'.[47]

Whilst this agreement has rolled over once, tension is rising in anticipation of the next renewal. In a 2021 joint evaluation, the European Commission reached the (rather unavoidable) conclusion that the agreement is 'not fully in line with Opinion 1/15′ on a number of levels, which include the retention of PNR data, the processing of sensitive data, notification to passengers, prior independent review of the use of PNR data, rules for domestic sharing and onward transfers, and independency of oversight mechanisms.[48] Current negotiations on the renewal of the agreement will inevitably test the limits of the EU's regulatory reach: while the European Commission has acknowledged the need for change to comply with the current state of EU law – in light of Opinion 1/15 – the US has clearly stated its unwillingness to accept any additional restrictions on the use of PNR data.[49] This reflects a broader phenomenon of geopolitical discord on how commercial data is mobilized for security purposes and integrated in systems of mass surveillance. The principled position and extraterritorial reach of the CJEU may, as Daniel Mügge argues, 'demarcate the outer limits of EU-external regulatory cooperation'.[50] In a dynamic described as an 'inadvertent Brussels effect', Mügge observes, 'other parties to regulatory negotiations might appreciate, however grudgingly, that certain safeguards in EU law may be unavoidable, no matter what they think of them'.[51] 'The EU's limited room for manoeuvre on some of these questions' may 'strengthen its bargaining position'.[52]

These inadvertent effects seem to capture at least part of the dynamic by which the EU extended its extraterritorial reach to the UK through the integration of Opinion 1/15 in the TCA. Commenting on the EU negotiation position, one interviewee from the UK Home Office accepted that 'that was your legal base, that was the agreement you were required by your law to agree'.[53] Yet, with the EU seeking to export its legal standards through every private entity that is carrying data abroad – in this case airline companies caught in the intricate web of jurisdictional conflict where data requested by third countries cannot be provided absent an agreement and appropriate safeguards – the reach of this extraterritorial power is being tested. As the interviewee noted: 'Brazil or the Emirates [might argue this is] something that the United Nations Security Council has said that we should all be doing to counter foreign terrorist fighters and serious crime [and] you're inhibiting us from doing it because [you're] exporting your legal framework into our jurisdiction'.[54] In this context, we observe how controversies over the exchange and use of PNR data forms part of broader jurisdictional and regulatory conflicts in the sphere of digital governance, counterterrorism and AI.[55] As the interviewee from the Home Office expressed it, the UK navigates these conflicts with the aim to 'return … the ability to determine its own data retention and data deletion practice rather than one we've adopted simply because [the CJEU] said it was a condition of [the EU's] agreement with third countries'.[56]

In relation to the extraterritoriality of EU law, as currently confronted by the UK, it is crucial to consider how these legal standards can evolve or be enforced in light of the UK's claim that is has extracted itself from the CJEU's jurisdictional reach.[57] It should be noted in this context that the TCA itself should not be seen as an 'adequacy decision' in terms of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) and that its execution is safeguarded by two separate decisions which stipulate that 'the United Kingdom ensures an adequate level of protection for personal data' in relation to both

[44] House of Lords, *supra* note 27, 31, para. 101. This is based on the observation that the UK 'will no longer be able to benefit from the national security exemption … that is available to EU Member States when their individual data retention and surveillance regimes are tested before the CJEU'. It should be noted, however, that the conditions under which EU states can access, share, use and retain PNR data have become much stricter since the judgment in CJEU, Ligue des Droits Humains.

[45] These tensions have ripples in relation to PNR agreements with other countries of the Five Eyes – including Australia – as well as negotiations on PNR exchange between the EU and Japan, and the EU and Mexico.

[46] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security [2012] OJ L 215/5.

[47] *Ibid.*, Article 26, para. 2.

[48] European Commission, Report from the Commission to the European Parliament and the Council on the joint evaluation of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, COM(2021) 18 (2021), 4. Importantly, this conclusion equally applies to the EU's PNR agreement with Australia, which was also included in the joint review and evaluation by the Commission and considered to fall short of the standards set out in 1/15. This conclusion was reiterated by the Council of the European Union. See General Secretariat of the Council, Draft Council Conclusions on the transfer of Passenger Name Record (PNR) data to third countries, in particular Australia and the United States, for the purpose of combating terrorism and serious crime, 12 May 2021.

[49] Kenneth Propp, 'Avoiding the Next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data' (1 July 2021) *Atlantic Council Issue Brief*.

[50] Daniel Mügge, 'Squaring the triangle of fundamental rights concerns' (12 May 2023) *Verfassungsblog*, 4.

[51] *Ibid.*

[52] *Ibid.*

[53] Interview with UK Home Office, May 2023.

[54] *Ibid.* On Security Council PNR governance for countering foreign terrorist fighters, see UNSC, *supra* note 28. In this context, absent a PNR agreement, airline companies – specifically those registered in the EU – are caught between the laws of third countries (requiring the sharing of PNR data) and EU law (prohibiting this data sharing).

[55] There is a vast literature on post-9/11 PNR data transfer politics, mostly in relation to EU-US arrangements for counterterrorism governance. For detailed analysis, see: Valsamis Mitsilegas, 'Immigration control in an era of globalization: Deflecting foreigners, weakening citizens, strengthening the state', (2012) 19 *Indiana Journal of Global Legal Studies* 3; Valsamis Mitsilegas, 'The criminalisation of travel as a global paradigm of preventive (In) justice: Lessons from the EU response to 'foreign terrorist fighters' (2023) 14(2) *New Journal of European Criminal Law* 183; Elaine Fahey, 'The life cycle of Passenger Name Records in European Union law – on the normalisation of crisis' (2023) 70 *Irish Jurist* 211. On competing regulatory models of data governance, see, for example, Matthew S. Erie and Thomas Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance' (2021) 54 *New York University Journal of International Law and Politics* 1; Anu Bradford, *Digital Empires – The Global Battle to Regulate Technology* (2023).

[56] Interview with UK Home Office, May 2023.

[57] On the enduring importance of CJEU jurisprudence for the UK post-Brexit, see House of Lords, *supra* note 27, 31; Nóra Ní Loideáin, 'Brexit', in Eleni Kosta and Franziska Boehm (eds.), *The EU Law Enforcement Directive (LED) – A Commentary* (2024).

domains.[58] Making the UK the only third country that is granted adequacy decisions under both the GDPR and the LED, the European Commission underlined that the UK might have left the EU but remains member of the European 'privacy family'.[59] Essential in this evaluation was not only the UK's status as a parliamentary democracy committed to the rule of law or the 'essential equivalence' between its data protection standards and those provided by the EU,[60] but also, and importantly, the commitment by the UK to the European Convention on Human Rights (ECHR) and its submission to the jurisdiction of the European Court of Human Rights (ECtHR).[61] Continued adherence to this human rights law regime, the adequacy decisions both underline, 'is therefore a particularly important element'.[62]

Yet, if the UK is indeed a member of the European 'privacy family', this entails a strongly supervised and surveilled form of membership. Both adequacy decisions contain a 'sunset clause' and only apply for a period of four years,[63] during which developments in the UK will be closely monitored.[64] In relation to the LED, the adequacy decision thereby identifies areas of 'special attention' such as the transfers of personal data to third countries and the effectiveness of the exercise of individual rights.[65] Considering the importance of adherence to the ECHR and ECtHR in the European Commission's evaluation, it is evident, as Nóra Ní Loideáin argues, that 'any significant divergences from the [ECHR legal order] may jeopardise the entire TCA and both EU-UK Adequacy Decisions'.[66] In its evaluation – 'on an ongoing basis' – of whether the UK to 'ensures an essentially equivalent level of protection',[67] the Commission will consider the evolution of EU law in the context of CJEU case law. This is highly relevant in relation to the recent judgment in *Ligue des Droits Humains,*[68] for example, which sets out detailed standards on data retention and automated processing of PNR data (as explored above and elaborated in the next section). These provisions establish a key oversight mechanism for the problems examined in this paper, to determine whether or how the Home Office complies with the requirements for processing PNR data.

In addition to the provisions on monitoring or suspension in the adequacy decisions themselves – which are given particular weight in the context of the 'sunset clause' – the CJEU also made clear that adequacy decisions can be legally challenged for failing to safeguard adequate levels of legal protection.[69] In this sense, the *Beyond Brexit* report by the UK House of Lords observed, 'despite the Government's claims that the UK has left the CJEU's jurisdiction, there is abundant scope for legal challenge on data protection grounds that could have implications for the UK'.[70] In other words, 'CJEU judgments in respect of UK data protection standards … may yet have an indirect but far-reaching impact'.[71] This is relevant not only in relation to practices of bulk data retention and surveillance but also systems of automated decision-making such as those envisaged in the Cerberus project. Finally, the TCA itself also includes a provision stating that 'in the event of serious and systemic deficiencies … as regards the protection of fundamental rights or the principle of the rule of law', the agreement can be suspended.[72] As we show in the following section, this rights compliance provision in the TCA is a key rationale shaping the socio-technical design of processes for analysing EU PNR data through the Cerberus system.

Our analysis in this section shows how the UK's dependency on EU PNR data gave rise to a distinctive post-Brexit legal regime which integrated standards emanating from CJEU Opinion 1/15 on automated processing of data and data retention as well as specific forms of oversight. This regime subjects the UK border control systems to stringent forms of monitoring and supervision. This shows the significant extra-territorial reach of EU law – a specific manifestation of the *Brussels Effect* in action – as developed in the jurisprudence of the CJEU. In the next section, we explore how, in the design of the UK's digital borders, these legal standards are translated as parameters of technical use through a process we describe as an *Infrastructural Brussels Effect.* We show how these legal standards are mediated and reconfigured as they become entangled with the UK's digital infrastructure for algorithmic border governance.

3. An infrastructural Brussels Effect? Normative translations and sociotechnical shifts

In the previous section we outlined the key features of the *Brussels Effect* enabling and constraining continued UK access to EU PNR data post-Brexit and showed how regulatory standards incorporated into the TCA work to effectively extend the CJEU's reasoning from Opinion 1/15 into UK jurisdiction. This account is broadly consistent with the existing legal literature on the *Brussels Effect*, which tends to conceptualise the extraterritoriality and movement of EU law as a strictly normative phenomenon and process of legal transplantation and regulatory globalisation. In this section, we extend this approach, analysing how the extraterritoriality of EU norms surrounding PNR data is given effect infrastructurally and enacted through distinctive socio-technical

[58] Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (referred to below as 'GDPR Adequacy Decision'); Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (referred to below as 'LED Adequacy Decision'). On the salience of this adequacy decision in the context of the Law Enforcement Directive (LED), see Laura Drechsler, 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context' (2021) 11 *International Data Privacy Law* 182.

[59] European Commission, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, bit.ly/3uFFVqB (last accessed October 2024). Cf. Ní Loideáin, *supra* note 57.

[60] GDPR Adequacy Decision, Recital 273; LED Adequacy Decision, Recital 157.

[61] While questions on the importance of the UK's adherent to the ECHR lie beyond the scope of this article, these provisions indicate how various oversight mechanisms – through the TCA, adequacy review and the ECtHR – are deeply intertwined in the post-Brexit context. For a helpful analysis of this interplay, see Steve Peers, 'So close, yet so far: The EU/UK Trade and Cooperation Agreement' (2022) 59(1) *Common Market Law Review* 49.

[62] GDPR Adequacy Decision, Recital 277; LED Adequacy Decision, Recital 161 (see also Recitals 8-10 and 19).

[63] GDPR Adequacy Decision, Recital 289; LED Adequacy Decision, Recital 173.

[64] GDPR Adequacy Decision, Recitals 281-287; LED Adequacy Decision, Recitals 165-171. Recital 165 states: '[T]he Commission is to monitor, on an ongoing basis, relevant developments in the United Kingdom after the adoption of this Decision in order to assess whether it still ensures an essentially equivalent level of protection'.

[65] LED Adequacy Decision, Recital 165.

[66] Ní Loideáin, *supra* note 57, 19.

[67] LED Adequacy Decision, Recital 165.

[68] CJEU, Ligue des Droits Humains.

[69] Ní Loideáin, *supra* note 57, 18. This has been stipulated in CJEU, Judgment of 6 October 2015, Schrems v Data Protection Commissioner, C-362/14; CJEU, Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited, C-311/16. This aligns with the observation by Fahey, Kuskonmaz and Guild that '[t]he oversight of international data transfer conducted by the CJEU in the Schrems II decision indicated a new era of engagement by the EU court on the governance of data flows'. Fahey, Kuskonmaz and Guild, *supra* note 28, 5. Cf. Lorna Woods, 'Data Protection, the UK and the EU: the draft adequacy decisions' (2021) *EU Law Analysis*.

[70] House of Lords, *supra* note 27, 31.

[71] *Ibid.*

[72] TCA, Article 693. For detailed analysis of this issue see: Valsamis Mitsilegas and Elspeth Guild, 'Police and Criminal Justice Co-operation after Brexit', (2023) 30(11) *Journal of European Public Policy* 2519.

arrangements for digital bordering in the UK. We describe this process as an *Infrastructural Brussels Effect* and argue that empirically analysing how EU legal norms are translated into sociotechnical infrastructures is important for three reasons. First, it foregrounds how material techniques or digital processes shape forms of regulatory ordering that are usually disregarded in normative accounts of legal change and governance.[73] Second, it draws attention to salient structure-making sites where political tensions and institutional frictions associated with algorithmic security and digital bordering are being played out via emergent sociotechnical design practices.[74] Third, it pushes us to analyse the recombinant techniques resulting from this *Infrastructural Brussels Effect* as new and distinctive forms of regulatory ordering and risk governance that are legally significant, but that operate through sociotechnical practices ordinarily conceptualised as extra-legal.

The infra-legalities approach used in this research is inspired by the relational process ontology of Actor-Network Theory, governmentality scholarship and Critical Data Studies and thus reorientates empirical focus towards emergent relations and practices.[75] Grasping the co-productive dynamics of law and data infrastructure is a form of action-based research that uses qualitative, sociolegal methods for studying sociotechnical and infrastructural processes in the making.[76] To do this, for this paper we used elite interviewing as a primary research method. Our empirical analysis builds on a number of semi-structured group interviews conducted in 2022–23 with senior Home Office policy officials responsible for PNR analysis and watchlisting as well as data engineers from the Home Office and BAE who are together building the UK's new digital bordering infrastructure. Research access was facilitated via the UKRI Infra-Legalities Future Leaders Fellowship project of the first author.[77] Interviews were conducted both in person (at the Home Office headquarters in London), including as group discussions, and online. All interviews were recorded and transcribed for analysis to identify cross-cutting themes and issues. Interview data was also triangulated via analysis of related policy documents and reports and academic literature. All quotes are anonymised to minimise the risk of participant reidentification and to protect confidentiality.

As we elaborate below, when algorithmic governance processes are entangled with conventional legal principles, one does not supplant the other. Rather, legal norms and sociotechnical practices associated with predictive analytics and machine learning are reconfigured into novel amalgams or constellations combining and rearticulating 'legal' and 'technical' elements. Crucially, these emergent governance assemblages generate distinctive regulatory effects and enact shifts in power relations that require empirical study to unpack.[78] Analysing these sociotechnical shifts as part of an *Infrastructural Brussels Effect,* in other words, helps show how legal and regulatory ordering techniques and digital bordering infrastructures are enmeshed and co-productive in practice.

As discussed above, the TCA incorporates key elements of Opinion 1/15 – later confirmed by the 2022 CJEU *Ligue des Droit* decision – regarding the retention and deletion of PNR data, as well as stringent rules on the automated processing of data.[79] On data retention, the TCA affirms the need for immediate data deletion upon departure.[80] This posed a clear problem: the UK structurally relied on the retention period of five years post-departure – set out in Art. 12 (1) of the PNR Directive – for their automated PNR data surveillance and analysis. This data retention is now only warranted for those deemed to present a public security 'risk', which must be based on 'objective evidence … from which it may be inferred that [they] may present a risk in terms of the fight against terrorism'.[81] Yet, under the TCA, as we noted, the UK is allowed to derogate temporarily from this provision while they make the necessary 'technical adjustments' that can enable their PNR processing systems to make this post-departure risk determination. The primary basis for this derogation were the 'special circumstances' of the UK – which had rapidly changed from being an EU Member State operating under the PNR Directive to a third country subject to different rules. As one senior Home Official put it: 'At the moment, our technical systems are not set up in a way that can fully comply with the requirements in the agreement. The special circumstances allow us a period of three years to enable us to bring our border systems fully in line with those new requirements'.[82] A central element in the design of Cerberus is therefore to develop technical tools to provide 'objective evidence' of 'risk' which would justify the retention of data after departure. The data thereby retained would, in turn, not only enable security checks considering a 'historical analysis' of individual behaviour, but also allow for the inference of patterns that feed into the models and criteria for automated risk assessment.[83]

On this automated processing of PNR data, the TCA is even more prescriptive. In short, the UK must ensure that 'any automated processing of PNR data is based on non-discriminatory, specific and reliable pre-established models and criteria'.[84] These models must allow the government to 'arrive at results targeting natural persons who might be under a *reasonable suspicion* of involvement or participation in terrorism'.[85] Opinion 1/15 further qualified and restricted the generalised prohibition on automated data processing, noting that automated PNR processing has significant margins of error and the degree of rights interference involved 'depends on the pre-established models and criteria and on the databases on which that type of data processing is based'.[86] As a result of this requirement, positive hits arising from automated PNR analysis must be subjected to 'individual re-examination by non-automated means' – for example, through human review –

[73] Anna Leander, 'Locating (New) Materialist Characters and Processes in Global Governance', (2021) 13 *International Theory* 157.

[74] Latour, *supra* note 25, 173. In this way our empirical study of the emergent Cerberus infrastructure in the UK's digital borders seeks to contribute to recent practice-based accounts of how PNR data analysis shapes security governance and knowledge production. See, for example: Georgios Glouftsios and Matthias Leese, 'Epistemic fusion: Passenger information units and the making of international security', (2023) 4991) *Review of International Studies* 125.

[75] Sullivan, *supra* note 13.

[76] *Ibid*.

[77] UK Research and Innovation (UKRI) Future Leaders Fellowship funding award, Dr. Gavin Sullivan (The University of Edinburgh), *Infra-Legalities: Global Security Infrastructures, Artificial Intelligence and International Law*, Grant Ref: MR/T041552/1. See: www.infra-legalities.com (last accessed October 2024).

[78] Pottage, *supra* note 24; Marianna Valverde, Ron Levi and Dawn Moore, 'Legal Knowledges of Risks' in Law Commission of Canada (ed.), *Law and Risk* (2005); Gavin Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (2020); Van Den Meerssche, *supra* note 11.

[79] TCA, Article 551 – 552.

[80] In Ligue a further restriction on deletion after 6 months is inserted. CJEU, Ligue des Droits Humains, para. 255.

[81] CJEU Opinion 1/15, para. 207; TCA Article 552, para. 4.

[82] Chris Jones, Europe Director, Home Office, House of Lords Select Committee on the European Union; Security and Justice Sub-committee (16 February 2021), Q. 42. Available at: bit.ly/3sXRgBU (last accessed October 2024).

[83] Cf. CJEU Opinion 1/15, para. 198 (on 'the systematic use of PNR data for the purpose of verifying … pre-established models and criteria [for] automated processing' or 'defining new models and criteria').

[84] TCA, Article 551, para. 1(a).

[85] *Ibid* (emphasis added).

[86] CJEU Opinion 1/15, para 172-173. As the European Commission states: 'pre-determined criteria, also known as targeting rules, are search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers which corresponds to certain abstract profiles, e.g. passenger travelling on certain routes … who bought their ticket in the last moment and paid in cash, etc'. European Commission, Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [Brussels, 24.7.2020 SWD (2020) 128 final], 11.

before adverse measures are taken against individuals.[87] To ensure targeting models and criteria are used in a non-discriminatory and lawful manner, their reliability must be subjected to review.[88] The TCA's focus on 'pre-established models and criteria' is a response to sociotechnical affordances of AI-based PNR data processing systems. It specifically seeks, as we noted above, to preclude the use of advanced machine learning capabilities that modify 'without human intervention or review the assessment process and … the assessment criteria' upon which PNR targeting decisions are based. According to the CJEU, the opacity of these AI capabilities makes it 'impossible to understand the reason why a given program arrived at a positive match', making PNR oversight, individualised review and the right to judicial remedy de facto redundant.[89]

Taken together, these legal restrictions on PNR data retention and automated processing raise concerns for the UK's use of PNR data and require a radical revision of its technical systems. The UK's retention of data for a period of five years meant, as one Home Office official put it, that 'you had a bucket of data. So, if you had a question, you could ask the question of the bucket, and if the answer is in bucket you can take it out'.[90] For the CJEU, the problem with this approach and lengthy retention period is that it facilitated 'a surveillance regime that is continuous, untargeted and systematic' for the 'very large part of the population of the European Union' that regularly uses air transport.[91] Yet it also facilitated the diachronic analysis of PNR data over time, or what one Home Office data scientist referred to in interview as 'historical analysis … to inform future detection' by using 'maximum contextualisation':

> The *historical* bit means, we look at what happened before, and we try to work out what's going to happen next … The *contextualisation* bit says, 'Here's [Peter], he's coming back from his summer holiday. What do we know about him? … What do we know about him today and previously? Is his behaviour today different to his peer group, or to himself? How is his behaviour today compared to his own behaviour historically?' [And] there's an implication there that you have to bring the data into one place, and you have to store it and analyse it over time. *And the 'over time' bit is really important.*[92]

For the Home Office officials we interviewed, removing possibilities for this historical PNR analysis threatened to undermine their ability to find the proverbial 'needle in the haystack' or person of security concern.[93] UK PNR targeting sifts and differentially governs passengers into categories of risk – separating 'reds' (or 'needles' who pose a risk or threat) from 'greens' ('people [who] don't do anything wrong' and who 'get through') and 'ambers' (who are not yet red because 'they haven't done anything illegal … but they're [also] not a green because they've done something abnormal').[94] The TCA rules on PNR data retention problematise this biopolitical classification and security intervention. As one Home Office data scientist put it, it is clear the TCA 'was not written by a data analyst, because a data analyst would … say: [the data] might not be red today, but if all your saying is that I can look at it once and once only, you're giving me no ability to contextualise beyond what I can see right now'.[95] Or in other words, which succinctly capture the perceived added value of generalised PNR data surveillance for UK border security officials used to having prolonged access to PNR data: 'if we delete the data just because someone is green today, it doesn't mean it will be green tomorrow'.[96] The TCA rules requiring immediate deletion upon departure in the absence of security 'risk' supported by 'objective evidence' thus present the UK Home Office with a novel set of border security governance and sociotechnical issues. As one Home Office policy official explained: 'How do you know, of the people who have come and left, who are the ones that pose the risk? … How do you develop the capability to ensure that you're retaining the data that *you don't know yet you're going to need to use at some point in the future*?'[97] In other words, what pre-emptive security techniques and practices can be developed to make the uncertain future risks of air travellers knowable - linked to the 'objective evidence' of potential harm - and amenable to security intervention and data retention in the present?

For the UK government, grappling with this anticipatory border security governance problem requires the development of more advanced digital technologies and use of predictive data analytics. Addressing the legal challenges posed by the TCA has thus become a key rationale for the accelerated development of Cerberus and a particular use case or add-on requirement for this critical infrastructure project. The development of this novel technical capacity has brought together high-level officials from Home Office data and technology teams, Border Security Policy teams, BAE data scientists and operational partners from UK security, policing and intelligence. As one participant in this process put it: '[t]here is a lot of nuance that came from the clauses within the legislation [ie, the TCA] … [so], the past 18 months [we] have been working through what exactly the words in the legislation mean in practice for our service system'.[98] This collaboration is directly aimed at developing a sociotechnical solution to address the TCA PNR data deletion problem in ways that build on and extend the UK's existing systems for analysing travel data to detect potential risks. 'What we've done', according to a lead data scientist developing Cerberus, 'is transpose [our senior Home Office policy expert's] deep knowledge of the legislation into business requirements that … the developers in our system then code into the system, to ensure we are deleting the right, the green sort of data, at the correct time'.[99] In this way, compliance with TCA rules on PNR data retention is providing the impetus for a powerful and distinctive UK digital bordering infrastructure that seeks to inscribe and operationalise legal norms as code. We argue that this sociotechnical process of norm 'transposition' and algorithmic regulation entails more than a neutral movement of knowledge or transplantation of practice from one context (legal) into another (technical).[100] Translating norms in this way is jurisgenerative: it is forging novel regulatory effects and legal interactions, reshaping security knowledge practices associated with digital PNR targeting and putting a distinctive *Infrastructural Brussels Effect* into action.[101]

One of the key effects of this infrastructural development, for example, lies in the fabrication of new techniques and practices for identifying and governing border security risks via algorithmic data

[87] CJEU Opinion 1/15, para 173.

[88] CJEU, Ligue des Droits Humains, para 193 – 213. The Court specifically notes (at para. 195) that the use of self-learning AI systems would render this lawfulness review 'redundant'.

[89] CJEU, Ligue des Droits Humains, para 194 –195.

[90] Interview with UK Home Office, April 2022.

[91] CJEU, Ligue des Droits Humains, para 110.

[92] Interview with UK Home Office, April 2022 (emphasis added).

[93] *Ibid.* On the operational value of historical PNR data analysis see, for instance: European Commission, *supra* note 85, 25, 30–33. On the 'needle in the haystack' metaphor, see Claudia Aradau and Tobias Blanke, *Algorithmic Reason: The New Government of Self and Other* (2022), 22.

[94] Interview with UK Home Office, April 2022.

[95] *Ibid.*

[96] *Ibid.*

[97] *Ibid*; Interview with UK Home Office, May 2023 (emphasis added).

[98] Interview with UK Home Office, April 2022.

[99] *Ibid.*

[100] On algorithmic regulation, see: Karen Yeung, 'Algorithmic Regulation: a critical interrogation', (2018) 12 *Regulation & Governance* 505. On the generative effects of translation and the movement of data between sites, see: Marieke de Goede and Gavin Sullivan, 'The Politics of Security Lists', (2016) 34(1) *Environment and Planning D: Society and Space* 67, 79; Sullivan, *supra* note 78, 103 – 130.

[101] See also Rocco Bellanova and Marieke de Goede, 'The Algorithmic Regulation of Security: an Infrastructural Perspective', (2022) 16 *Regulation & Governance* 102 (highlighting the generative effects of data infrastructures).

analysis. For the Home Office, identifying risk related to post-departure PNR data requires working with operational agencies and re-evaluating the reasons for their earlier border security interventions in order to define and extrapolate salient characteristics of the PNR data to inform targeting. This means asking: '[w]hat is it about the data that historically they have found themselves viewing? Does that give us any indication of the data we're going to be interested in, in the future?'.[102] According to Home Office experts we interviewed, up to fifteen 'characteristics' have been distilled as risk indicators to guide the automated analysis of PNR data in a way that gives specific meaning to the requirements of the TCA. These indicators compress the processes for 'maximum contextualisation' discussed above and function as selection criteria for data deletion: '[s]o, when we see a passenger who has exhibited this criterion, or who doesn't exhibit this criterion, and they've departed the country on this date, that's when the trigger for deletion through all the separate products within the Cerberus system has to happen'.[103] The substantive content of these behavioural 'characteristics' has not been disclosed for operational reasons, and the automated processes for selecting and deleting PNR data based on these features are still (at the time of writing) in the process of development.[104] Yet, it is important to underscore that these are new targeting capabilities, distinct from rules previously used by the Home Office in this setting and the 'pre-established models and criteria' envisaged in the TCA.[105] While these characteristics of risk were described to us as 'indicators', they are not based on fixed criteria with an independent causal relation to security risks. They are emergent and relational phenomena – drawn from and reshaped by the data they are generated from. These are novel techniques for digital bordering, forged through the translation of legal norms into the sociotechnical infrastructure of Cerberus, that are aimed at addressing the unique governance problems posed by the TCA. As the Home Office acknowledged, 'we are the only people in the world who are trying to work this out'.[106]

Another related effect of this infrastructural problem concerns how it is altering the conditions for border security knowledge required to justify governmental intervention. As discussed above, the TCA requires PNR data retention after departure to be based on the identification of 'objective evidence from which it may be inferred' that specific passengers pose a 'risk' of terrorism.[107] However, what this 'objective evidence' means or includes is not spelt out in the Agreement. It is understood by the CJEU to be something deductively 'revealed' by the 'checks and verifications' used by border authorities for PNR data analysis.[108] Yet, because the PNR selection scenario outlined above relies on speculative and pre-emptive logics – with the Home Office asking how characteristics of data they were once interested in might 'give us any indication of the data we're going to be interested in, in the future' – this discovery of 'objective evidence' is not straightforward. Connecting those selected for PNR data retention in the present with some unspecified future risk is rather based on potential inferences and characteristics drawn from heterogeneous data using algorithmic processes for pattern detection. Here, the translation of TCA norms into the emergent infrastructure of Cerberus is altering the conditions for border security governance in significant ways and reshaping conventions of legal practice. In effect, being selected as risky by algorithms that distil patterns and infer characteristics from vast volumes of data (including the historical data of others) is now being recast as 'objective evidence' of terrorist risk and the legal basis for reclassifying air travellers as potentially anomalous. This process of evidence discovery builds on, yet in salient ways departs from, the deductive logics of earlier rules-based PNR systems. It shows how material techniques for algorithmic data analysis are reshaping TCA norms on data retention in line with the affordances of technical systems like Cerberus, while remaining loosely tethered to established principles for establishing legal proof. In this context, the 'objective evidence' of terrorist risk is something 'abductively generate[d]' via algorithmic pattern recognition techniques that are fluid and dynamic, and obtaining evidence more closely resembles 'experimental processes of learning' through data than conventional forms of counterterrorism evidence discovery.[109]

This reliance on inferred patterns and characteristics does not only shape the data retention and deletion practices of Cerberus but its technical systems of risk-based border control more broadly. The TCA, in this context, seeks to impose strict conditions on automated PNR data processing – and mitigate the potential harms of unsupervised machine learning and the automated suggestion of rules – by imposing '*reasonable suspicion* of involvement or participation in terrorism' as the appropriate standard for the targeting of natural persons.[110] In the context of counterterrorism policing, 'reasonable suspicion' is ordinarily individualised and linked to information 'specific to the personal conduct of the person'.[111] Home Office guidance on the seizure of travel documents at the border, for example, stipulates that reasonable suspicion 'cannot be formed on the basis of assumptions about the … behaviour of persons … belong[ing] to particular groups or categories of people'.[112] Yet this familiar evidential standard is expansively reshaped when translated into the emergent sociotechnical infrastructure of Cerberus.

According to Home Office data engineers, the digital architecture of Cerberus relies on the construction of network graphs that enable PNR targeting of travellers by 'creat[ing] associations between different entities' that were otherwise unrelated.[113] This operative targeting logic of Cerberus was described to us as a form of 'concern by association', including between 'known' and 'as-yet unknown' risky people and things.[114] Such predictive systems are fundamentally relational in character, rather than grounded in the assessment of individualised personal conduct. As Salome Viljoen argues, they work by enacting 'population-level horizontal data relations' through algorithmic data analysis techniques that recast 'people as assemblages of their social relations and group behaviours', inferring 'patterns of behaviour derived from group-based insights' and then using these patterns as the basis for predictive targeting.[115] In this sense, the key question Cerberus addresses and uses as the ground for pre-emptive security intervention is not 'does this individual's personal conduct give rise to a reasonable suspicion of terrorism'? Rather, as one interviewee put it, Cerberus helps Home Office analysts to ask 'do they exhibit a pattern we are interested

[102] Interview with UK Home Office, April 2022.
[103] *Ibid.*
[104] Interview with UK Home Office, May 2023.
[105] TCA, Article 551, para. 1.
[106] Although, the EU and EU Member States are now faced with a very similar conundrum following the 2022 CJEU Ligue des Droit Humains decision which affirmed a six-month PNR retention period.
[107] TCA, Article 552, para. 4. The specific wording here mirrors that used by the CJEU in Opinion 1/15 (para. 207). In that case, the Court says the inference must be 'that the PNR data of one or more air passengers might make an effective contribution' to countering terrorism (para. 201). The CJEU Ligue des Droit Humains decision similarly refers to 'objective material from which it can be inferred that the PNR data could … contribute effectively to combating' terrorism' (para. 220). As noted above, Ligue des Droits Humains further restrains the retention of data beyond six months. Compliance with this judgment is key for the UK's adequacy assessment.
[108] CJEU Opinion 1/15, para. 204.
[109] Louise Amoore and Rita Raley. 'Securing with Algorithms', (2017) 48(1) *Security Dialogue* 3, 6.
[110] TCA, Article 551, para. (1)(a), emphasis added.
[111] Home Office, Code of Practice for Officers exercising functions under Schedule 1 of the Counter-Terrorism and Security Act 2015 in connection with seizing and retaining travel documents (2014). para, 20.
[112] *Ibid.*
[113] Interview with UK Home Office, April 2022.
[114] *Ibid.* See also: European Commission, *supra* note 86, 30.
[115] Salomé Viljoen, 'A Relational Theory of Data Governance', (2021) 131 *Yale Law Journal* 573, 610.

in' or do they indicate behaviour suggestive of 'abnormality' when analysed processually in relation to their own past behaviour, the behaviour of 'known' risky people and the behaviour of all other air travellers, in conjunction with intelligence-led insights on shifting patterns and trends shared between Passenger Information Units (PIUs)?[116] In this way, the scope and meaning of the legal requirements in Opinion 1/15 (on 'reasonable suspicion') are being stretched and reshaped in practice through the relational ontology of the Cerberus bordering infrastructure and its associational targeting processes for governing unknown threats. The TCA norms aimed at tempering the risks of automated PNR processing through familiar evidential standards are being reconfigured in ways that resonate with the sociotechnical affordances of advanced algorithmic pattern detection techniques.

In the previous section, we observed how the normative safeguards developed by the CJEU – in Opinion 1/15 and *Ligue des Droits Humains* – were extended and extrapolated to the UK through the TCA. In this section, we have shown, based on original interview material, how this extraterritorial effect of EU law posed particular problems for the design of the UK's digital borders in the post-Brexit landscape. This appears to be a story of the salience and transnational diffusion of EU law, and, indeed, this is an important part of the picture. Yet, as our empirical exploration reveals, this should not be the end of the analysis. Once these legal standards and safeguards become infrastructurally embedded – a process, as one interviewee noted, of 'cod[ing]' legislation 'into the system' – we witness a dynamic of normative translations and socio-technical shifts. In this sense, we argue that the standard of 'reasonable suspicion' and the demand for 'objective evidence' of 'risk' are given specific substance and novel meaning in the design and implementation of Cerberus – a project aimed to distil 'characteristics' of risk based on processes of relational inference and algorithmic pattern recognition (leading to forms of 'concern by association'). Again, it is important to underscore that this translation of legal norms into digital infrastructure is not a zero-sum matter of algorithmic governance supplanting the law. It is a recombinant process whereby legal techniques and principles are being rearticulated and reconfigured into distinctive forms of ordering through the sociotechnical assemblage practices and conditions that Cerberus is putting into effect.[117]

3. Conclusion

The global digitisation of border governance is unfolding apace, spurned by rapid advances in AI and ML capabilities for predictive analytics, international norms authorising the collection and transnational exchange of data for security purposes and the increasing desire of governments to extract 'all data as potential borders data' for governing unknown risks and threats.[118] PNR data is a crucial component of these bordering infrastructures and highly sought after by states for its perceived operational value in detecting suspicious or anomalous behavioural patterns and identifying those potentially 'associated with' terrorism. Brexit directly threatened the continued flow of this important security data from the EU to the UK, prompting the development of a unique regulatory framework and a set of interconnected legal and technical problems to resolve. This article has taken these unique developments as a departure point for exploring a small yet significant part of this regulatory problem space. It specifically analysed how EU norms and legal safeguards on PNR data processing for counterterrorism in the post-Brexit TCA are incorporated into the sociotechnical architecture and design of Cerberus – a UK critical national infrastructure project and flagship risk-based analytics platform of the UK 2025 Border Strategy.

Building on interviews with officials from the UK Home Office and BAE, two key arguments were advanced concerning this encoding of EU law into the UK's digital borders. First, we showed how despite the UK's departure from the EU, EU norms on the processing of PNR data for counterterrorism are being given heightened extraterritorial effect and reach in the UK through the design and development of Cerberus.[119] For the data engineers building this digital bordering infrastructure, legal principles from CJEU Opinion 1/15 as incorporated into the TCA are just another 'term of use' that the system designers must transpose to ensure continued access to PNR data.[120] However, our second key argument is that this transposition is not merely a process of norm diffusion or extraterritorial norm implementation. Our empirical analysis showed how this problem is facilitating the fabrication of novel techniques and practices for governing border security risks via algorithmic data analysis and reconfiguring familiar legal standards – in this case, on 'reasonable suspicion' and the 'objective evidence' of 'risk' – in ways consistent with the affordances of algorithmic pattern detection. In other words, the emergent data infrastructure of Cerberus and EU norms on PNR data are reassembling each other in distinctive ways through the sociotechnical practices of digital bordering.

Through these claims our paper sought to make three key contributions to academic debate and scholarship. First, we make an important empirical contribution to the literature on the analysis and exchange of PNR data for counterterrorism purposes. The EU's PNR data sharing arrangements with the USA, and the political and legal conflicts these have generated within and beyond the EU courts, have been the focal point of extensive legal scholarship. Yet the UK's novel post-Brexit PNR data sharing arrangements with the EU, and the specific regulatory and sociotechnical problems this arrangement is generating, have not yet been the subject of in-depth empirical study. This paper has sought to address this gap, whilst demonstrating how analysing the translation processes for encoding legal norms into digital infrastructures can be an especially productive site for socio-legal analysis.

Second, the paper contributes to existing legal literature on the Brussels Effect. Legal debates on this issue suggest that EU law is given extraterritorial effect via formal and immaterial processes of norm diffusion. However, our analysis has shown how material devices and sociotechnical practices – in this article, those associated with the design and operation of advanced forms of algorithmic governance – can also act as important conduits for extraterritoriality. We described this process as an *Infrastructural Brussels Effect* to underscore the importance of data infrastructures in reassembling legal principles and practices. The key implication of our argument is that legal Brussels Effect scholarship should be widened in scope to include material practices and techniques through which EU legal principles are given extraterritorial effect – in emergent digital infrastructures and rapidly expanding sites of algorithmic governance as well the dynamics of market competition and third country trade practice.

Third, as discussed above, our empirical analysis suggests this extraterritorial effect is not so much an instrumental process of norm transposition or of technological systems faithfully implementing EU law. Infrastructurally encoding EU norms into the sociotechnical architecture of Cerberus involve messy and generative processes of translation. These translation processes reconfigure legal standards into

[116] Interview with UK Home Office, April 2022; Interview with UK Home Office, May 2023.

[117] Alain Pottage, 'Foucault's Law by Ben Golder and Peter Fitzpatrick', (2011) 74(1) *Modern Law Review* 159, 167.

[118] Amoore, *supra* note 12, 2.

[119] While this article focuses explicitly on the exchange on PNR data and the legal framework surrounding this exchange, we should note that such extraterritorial reach is also anticipated and much debated in light the EU's recently adopted AI Act (AIA). The AIA does not only apply to developers of AI systems located within the EU but also to all AI systems that are put into service within the EU or from which the outputs are used in the EU. The extent to which emergent systems like Cerberus will be guided by the rules of AIA, therefore, currently remain uncertain. Cf: Nathalie Smuha, 'Biden, Bletchley, and the emerging international law of AI' (15 November 2023) *Verfassungsblog*.

[120] Interview with UK Home Office, April 2022

distinctive regulatory forms shaped by the affordances of algorithmic governance. The implication of this claim is that 'law' is not something applied onto a pre-existing social or material substrate that it purports to govern. Instead, legal ordering and the material practices of data infrastructures are entangled and co-productive, and so they need to be studied both relationally and empirically. This insight builds on and contributes to current legal theory debates on the importance of legal materiality and infrastructures as distinctive forms of regulatory ordering that operate outside the threshold of what is usually deemed to be 'law'.[121] Our analysis underscores the analytical value of using an infra-legalities approach to empirically study the translation processes, sociotechnical interfaces and contingent material practices through which norms and data infrastructures co-emerge and give shape to each other, particularly in advanced algorithmic governance settings.[122]

Current legal debates about AI are often posed in epochal and existential terms, with legal principles potentially supplanted through the increasing uptake of algorithmic systems for Big Data analysis. One of the key implications of this paper lies in its argument that relations between law and AI can be productively reconceptualised as site-specific empirical problems to be investigated in practice, not merely prompts for normative debate and theorising about how law ought to regulate technology. Our analysis suggests that legal norms are not so much supplanted by AI and algorithmic decision-making processes as reconfigured into novel material complexes or infrastructural assemblages that can be mapped and analysed via socio-legal study.[123] Unpacking and analysing these reconfigurations can help us understand how advanced algorithmic governance systems like Cerberus – with very different epistemological and ontological assumptions, novel decision-making processes and distinctive forms of agency – can be legally authorised and used to reshape border governance practices without new legal frameworks needing to be put in place.[124] It allows for critical and empirical engagement with emergent bordering assemblages that are redistributing institutional authority, intensifying data-driven surveillance and expanding the scope of pre-emptive security governance in potentially far-reaching ways. And it also underscores the importance of legal scholars studying algorithmic infrastructures in action - by decentring 'law', foregrounding the 'potentialities of "materiality"' in emergent infrastructural relations and practices and asking 'what becomes of 'law' if we try to hold those potentialities open'.[125]

Declaration of competing interest

For this paper, there are no conflicts of interests to report.

Data availability

The data that has been used is confidential.

Acknowledgements

This article developed from a paper presented at the workshop, 'Towards Autonomous Borders: Assessing the Human Rights and Rule of Law Challenges of the Deployment of AI systems for Migration Management' held at Queen Mary University of London on 29 March 2023. We wish to thank Niovi Vavoula and Alexandra Karaiskou for their invitation to attend this event, and the workshop participants for their helpful comments. The article is based on interviews undertaken in 2022 - 2023 with officials from the UK Home Office and British Aerospace Engineering (BAE). We are grateful for our participants generously agreeing to share their time and expertise on these issues. This research was supported by UK Research and Innovation (UKRI) Future Leaders Fellowship funding awarded to Dr. Gavin Sullivan (The University of Edinburgh), Grant Ref: MR/T041552/1.

[121] *supra* note 13.

[122] Sullivan, *supra* note 13; Fleur Johns, *#Help: Digital Humanitarianism and the Remaking of International Order* (2023).

[123] Nikolas Rose and Mariana Valverde, 'Governed by Law' (1998) 7 *Social & Legal Studies* 541, at 542.

[124] See, for instance: Home Office, Transparency Data, 6 September 2022: Cerberus Project Accounting Officer Assessment (updated 12 May 2023). Available at: bit.ly/3GjOPwC (last accessed October 2024) (arguing that 'The use of data within the system is based on a variety of established legislation and precedents governing the use of border movement data … As a result of these points, there is no new primary legislation required for Cerberus. The system and its use fall within the existing powers and remit of the Home Office').

[125] Pottage, *supra* note 24, 179–180. See also: Peer Zumbansen, 'Law's new cartographies: spatialization, digital borders and spaces of vulnerability' in Austen Parrish and Cedric Ryngaert (eds.) *Research Handbook on Extraterritoriality in International Law* (2023), 92.