Law, technology and data-driven security

DOI: 10.1111/jols.12352

ORIGINAL ARTICLE

Law, technology, and data-driven security: *infra*-legalities as method assemblage

GAVIN SULLIVAN

Edinburgh Law School, The University of Edinburgh, Old College, South Bridge, Edinburgh, EH8 9YL, Scotland

Correspondence
Gavin Sullivan, Edinburgh Law School, The University of Edinburgh, Old College, South Bridge, Edinburgh, EH8 9YL, Scotland
Email: g.sullivan@ed.ac.uk

Abstract

As complex data-driven systems are increasingly used to know and govern global problems, the terrain for socio-legal studies research is rapidly changing. Both 'the social' and 'the legal' are transformed through processes of algorithmic regulation and automated decision making. In the security field, these changes are giving rise to novel global infrastructures for countering potential risks through the extraction, exchange, and analysis of vast amounts of data. This article critically examines the key methodological implications of these data infrastructures for socio-legal research and argues that confronting these challenges requires a different approach to research methods – one that studies regulation and data infrastructures *together*, that is empirically attuned to socio-material practices and emergent relations, and that is performative rather than representational in orientation. Drawing principally from actor–network theory, materiality-orientated socio-legal work, and critical security studies, this article outlines an experimental 'method assemblage' ('*infra*-legalities') for knowing and intervening in global security infrastructures and explores the main features of this research approach. The focus of socio-legal studies on 'law in the real

world' – and its associated epistemological and methodological assumptions – needs to be challenged and modified to grapple with the problems posed by global security infrastructures and algorithmic regulation.

1 | INTRODUCTION

We are living in an era of intensified datafication and planetary-scale computation, where security risks are increasingly countered through new forms of predictive data analytics made possible by advances in artificial intelligence (AI). Travel data from the global aviation industry is algorithmically analysed to identify suspicious patterns of behaviour and control the movements of 'risky' travellers before they fly.[1] The United Nations Security Council has called on all states to build systems for collecting and sharing biometric data for security purposes.[2] Internet platforms are using AI and automated decision-making (ADM) tools, augmented by a complex array of private rules, to detect and remove terrorist and extremist content online on an unprecedented global scale.[3] This rapid expansion in algorithmic security is fostering the development of what I term 'global security infrastructures'. These are novel governance constellations that allow diverse actors (states, private platforms, international organizations, and global governance bodies) to collaborate across borders through the extraction, exchange, and interconnection of vast amounts of data for countering potential threats using AI techniques, ADM processes, and forms of algorithmic regulation.[4] The implications of these infrastructures for how law and regulation is practised are not yet known. How the law should respond to technological change is a question often asked. However, broader issues about how regulatory practices are reshaped through global security infrastructures and what that means for how we do empirical research on such problems are equally important. As 'the social' is increasingly enacted via complex socio-technical systems, the terrain for socio-legal studies (SLS) research is significantly altered. And as security is increasingly performed via automated technological systems refined through the continual computational generation of knowledge and the use of design-based regulatory techniques, what constitutes 'the legal' in SLS research is also profoundly reconfigured.

In a Special Supplement of this journal published ten years ago on the relation between SLS, science and technology studies (STS), and actor–network theory (ANT), similar questions were posed. How do law, technology, and society 'interact to bring into being new socio-material realities' – that is, 'material structures that embody social relations and vice versa'?[5] What are the conceptual and methodological implications of these socio-material entanglements for SLS? This article resituates such questions in the global security infrastructure space and asks what such infrastructures mean for the ways in which we *do* or practise SLS research. I argue that

[1] L. Ulbricht, 'When Big Data Meet Securitization: Algorithmic Regulation with Passenger Name Records' (2018) 3 *European J. for Security Research* 139.

[2] UNSCR 2178 (2014), para. 3; UNSCR 2396 (2017), para. 15.

[3] B. Fishman, 'Crossroads: Counter-Terrorism and the Internet' (2019) 2 *Texas National Security Rev*. 82.

[4] On algorithmic regulation, see K. Yeung and M. Lodge (eds), *Algorithmic Regulation* (2019).

[5] A. Faulkner et al., 'Introduction: Material Worlds: Intersections of Law, Science, Technology and Society' (2012) 39 *J. of Law and Society* 1, at 9, 13.

confronting these challenges requires studying law or regulation and data infrastructures *together* as co-emergent by empirically following their interrelations. This requires a methodological practice capable of grasping the relationality, heterogeneity, and performativity of socio-technical infrastructures, devices, and data and their dynamic interconnections. It also requires us to map how ordering is being reconfigured through the socio-technical practices of algorithmic governance, rather than always 'presuming "law"' as a pre-existing category and privileged first principle of analysis from which the social is moulded.[6]

To address this problem, this article outlines a critical security method or research strategy for mapping data-driven global security infrastructures in motion ('*infra*-legalities') and explores its key elements. An *infra*-legalities approach looks *below* the law towards mundane socio-technical practices in global security governance, underscoring the important regulatory work that they perform. It also focuses on data infrastructures as key sites of enquiry, empirically mapping the socio-technical elements through which they are composed and highlighting their effects. Data infrastructures include algorithms and AI processes, but also all of the socio-technical practices through which diverse data traces are curated, transformed into databases, or made algorithm-ready.[7] These include socio-technical practices of data collection, classification, exchange, analysis, and modulation. Data infrastructures are therefore inextricably tied to practice and capable of being empirically studied as socio-technical assemblages. An *infra*-legalities approach analyses global security infrastructures by honing in on the governance work that they do through 'infrastructural inversion' – a method of foregrounding infrastructural elements and practices that have sunk into the background to show how they enact and shape relations.[8]

To follow how regulatory techniques and infrastructural practices interact to enact socio-material worlds and new forms of regulatory ordering, an *infra*-legalities approach adopts a relational ontology. This builds on insights from ANT and recent social research methodological debates, and catalyses a series of important methodological shifts that are unpacked and elaborated in this article. To grasp how digital devices create and shape social relations, this approach redistributes agency between human and non-human entities and focuses on human–machinic entanglements and the effects to which they give rise. With its relationality and empirical focus on emergent socio-materialities, this approach shifts the register of SLS law and technology research in significant ways. This article explores these methodological implications in depth and highlights the key advantages and insights that they bring.

Infra-legalities is advanced as a 'method assemblage' or a way of experimenting with the arrangement of concepts, methods, and empirical objects.[9] This draws from recent debates suggesting that methods do not merely *represent* the world;[10] on the contrary, they are performative, helping to *enact* and shape the worlds that they describe.[11] SLS has long critiqued

[6] A. Pottage, 'The Materiality of What?' (2012) 39 *J. of Law and Society* 167, at 181–182.

[7] T. Gillespie, 'The Relevance of Algorithms' in *Media Technologies: Essays on Communication, Materiality and Society*, eds T. Gillespie et al. (2014) 167, at 170–171.

[8] G. C. Bowker and S. Leigh Star, *Sorting Things Out: Classification and Its Consequences* (1999) 34–46.

[9] C. Aradau et al., 'Introducing Critical Security Methods' in *Critical Security Methods: New Frameworks for Analysis*, eds C. Aradau et al. (2015) 1, at 7; J. Law, *After Method: Mess in Social Science Research* (2004).

[10] C. Lury and N. Wakeford (eds), *Inventive Methods: The Happening of the Social* (2012); E. Ruppert et al., 'Reassembling Social Science Methods: The Challenge of Digital Devices' (2013) 30 *Theory, Culture & Society* 22.

[11] A. Mol, 'Ontological Politics: A Word and Some Questions' in *Actor Network Theory and After*, eds J. Law and J. Hassard (1999) 74; A. Mol, *The Body Multiple: Ontology in Medical Practice* (2002).

legal positivism and articulated progressive approaches to legal change. Reframing how we do socio-legal research as inventive practice allows us to extend this critique to research methodology and experiment with critical methods that are disruptive of the social worlds that we study. Such an approach goes against the current of empirical legal studies that assumes that SLS should provide an empirical foundation for understanding 'law in the real world'.[12] I argue that addressing the challenges of global security infrastructures does not require more faithful representations of the real; it demands creative ways of describing and intervening in the socio-materialities that they are enacting.[13] An *infra*-legalities approach has critical potential for grappling with this problem and making the stakes of global security infrastructures visible and contestable.

To develop these claims, the article is divided into three sections that each explore critical elements of an *infra*-legalities approach. First, drawing mainly from ANT, STS, and critical data studies, I discuss the importance of relational process ontology in the study of data-driven global security governance. Using empirical snapshots from algorithmic border security and the governance of terrorism online, I show how relationality reorientates SLS research methodologies towards studying emergent socio-technical processes and pushes us to widen the scope of empirical enquiry.

Second, I elaborate on the idea of socio-materiality and the redistribution of agency in governance towards human–machinic practices that this relationality entails. Using the 2025 United Kingdom (UK) Border Strategy as an example of global security infrastructure in action, I unpack and analyse three methodological implications that come with emphasis on socio-materiality: empirically attending to multiplicities, taking technological affordances seriously, and studying the fabrication of 'global' scale through multi-sited research.

Third, I extend a relational process ontology to the problem of social science research methods and analyse the implications of shifting from methods as representational tools for knowing the social world to methods as performative devices for enacting and intervening in the worlds that we study. I then explore two potential ways in which an *infra*-legalities approach can work as a method assemblage for critically intervening in global security infrastructures: mapping algorithmic violence and its infrastructural conditions of possibility, and experimenting with doing critique *through* infrastructure and staging dissensus in global security processes.

The article closes by framing *infra*-legalities as a critical security method that opens up potentially fruitful avenues for law and technology research.

2 | RELATIONALITY, SECURITY INFRASTRUCTURES, AND RESEARCH METHODS

The pervasive use of advanced digital technologies (including AI systems) has prompted legal scholarship that aims to temper the power of algorithmic governance by making its inner workings transparent or using law to create a system of 'algorithmic checks and balances'.[14] The urgent task confronting us thus involves opening up this opaque algorithmic 'black box' in order to make its computational processes intelligible and subject to critical scrutiny and regulatory oversight.

[12] H. Genn et al., *Law in the Real World: Improving Our Understanding of How Law Works: Final Report and Recommendations* (2006).

[13] J. Law and J. Urry, 'Enacting the Social' (2004) 33 *Economy and Society* 390.

[14] F. Pasquale, *The Black-Box Society: The Secret Algorithms that Control Money and Information* (2016); E. Benvenisti, 'Toward Algorithmic Checks and Balances: A Rejoinder' (2019) 4 *European J. of International Law* 1087.

However, the complexity of AI-led decision making and its global data infrastructures complicates this approach. Algorithms perform security governance not as discrete tools but as heterogeneous socio-technical infrastructures or assemblages that are constantly unfolding in practice.[15] Van Den Meerssche shows how European Union algorithmic bordering practices work through a combination of the iterative learning processes of algorithms, the diverse data continually ingested (including passenger data, criminal record data, and biometric data), the interoperability of various migration, policing, and counterterrorism databases, and the emergent patterns derived from 'tying heterogeneous digital traces together'.[16] The norms guiding AI-led decision making are mobile or 'continuously kept in play: as new patterns emerge in … data mining, the assignations of risk alter'.[17] Making risk scores for governing the border requires the alignment of a diverse array of infrastructural relations and 'datastructuring'[18] practices. These arrangements are continually in motion and recursively reconstituted through new data.

Even if we wanted to make the inner workings of such governance systems transparent by opening up the algorithmic 'black box', we may not able to do so. Regulation based on advanced machine-learning techniques is technically inexplicable. AI techniques based on deep neural networks, for example, 'involve hidden layers and highly complex architectures which are impossible to analyse' and thus explain.[19] In advanced machine learning (ML), the decisional rule guiding the generation of outputs 'emerges automatically from the specific data under analysis', making algorithms and the patterns or clusters that they govern live or fluid objects.[20] While the policy implications of this complexity are the subject of important debates, the methodological implications for how we research global data infrastructures and algorithmic regulation processes have been less frequently discussed.

The *infra*-legalities approach outlined here engages with these problems by adopting a relational ontology that reorientates focus towards emergent socio-technical relations and processes. This relationality, which is a defining component of ANT and material semiotics, opens up productive routes for grasping how AI systems and global security infrastructures produce regulatory effects and govern. For the purposes of this article, the key idea of a relational ontology is that the heterogeneous elements of data infrastructures (including human actors, machinic processes, institutional entities, discursive forms, regulatory orderings, data classification practices, and algorithmic outputs) are not defined in isolation from each other, but *in* and *through* their relational networks.[21] Alternatively, as Law puts it, 'realities, objects, subjects, materials and

[15] R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (2014).

[16] D. Van Den Meerssche, 'Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association' (2021) IILJ Working Paper 2021/2, 18, at <https://www.iilj.org/wp-content/uploads/2021/07/Van-Den-Meerssche-WP-2021-2.pdf>.

[17] Id., p. 17.

[18] M. Flyverbom and J. Murray, 'Datastructuring: Organizing and Curating Digital Traces into Action' (2018) 5 *Big Data & Society* 1.

[19] Cambridge Consultants, *Use of AI in Online Content Moderation* (2019) 26, at <https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf>.

[20] J. Kroll et al., 'Accountable Algorithms' (2017) 165 *University of Pennsylvania Law Rev.* 633, at 638. On clusters as live objects, see E. Isin and E. Ruppert, 'The Birth of Sensory Power: How a Pandemic Made It Visible?' (2020) 7 *Big Data & Society* 1, at 9–10.

[21] A. Cordella and M. Shaikh, 'Actor–Network Theory and After: What's New for IS Research?' (2003) European Conference on Information Systems 2003.

meanings … are all explored as *an effect of the relations that are assembling and doing them*'.[22] With a relational ontology, it is the dynamic interaction between infrastructural elements and their effects that are key. The methodological challenge involves mapping these emergent relations to understand their 'modes of doing' or what they enact and following how they make new forms of security knowledge and governance possible (or not).

A relational approach thus invites different methodological strategies and opens up promising avenues for doing SLS law and technology research. It prompts a shift in focus from institutions and actors to the relational effects of their interactions; from legal systems and norms to emergent practices of legal or regulatory ordering; and from algorithms and ADM tools knowable by examining their inner logics to heterogeneous socio-technical assemblages understood through their effects or what they *do* in specific settings.[23] Crucially, these shifts 'not only affect the analysis of the phenomena, but also the assumptions about the nature of the entities that constitute the phenomena'.[24] That is, relationality is not an analytical lens (allowing us to see dynamism better) or an epistemology (allowing better knowledge of plurality), but an ontology that recasts the social world as something messy, emergent, and enacted via practice. This relationality pushes SLS researchers to broaden the scope of research to include how realities, materials, objects, and regulatory forms come into being or are enacted – an approach that Mol calls 'praxiography'.[25] The aim is not merely to describe relational practices, but to explain their emergence and effects through the interaction of the actors involved. As Law argues, 'if we want to understand how realities are done or to explore their politics, then we have to attend carefully to practices and ask how they work … [and] get assembled in particular locations'.[26]

Consider, for example, a device such as the hash-sharing database of the Global Internet Forum to Counter Terrorism (GIFCT), which uses ADM to remove online content deemed 'terrorist' or 'violent extremist'.[27] Conventional legal accounts highlight the normative stakes involved, such as the adverse effects on online speech, and set out legal solutions for remedying such problems, or assess the database's effectiveness in removing terrorist and violent extremist content (TVEC) online.[28] Here, the database is conceived of as a tool, the actors are assumed to have stable identities and objectives, and the law is presented as a coherent apparatus that enables or constrains their actions in certain ways.

A relational approach situates this database within its emergent socio-technical assemblage and draws attention to the ways in which its various components and processes – private platforms, states, the GIFCT, security services, internet users, content moderators, software designers, algorithmic processes, data classification practices, rules and protocols, and targeted people – are interconnected and sustained to enact a global security infrastructure for targeting TVEC online.

[22] J. Law, 'Collateral Realities' in *The Politics of Knowledge*, eds F. Dominguez Rubio and P. Baert (2012) 156, at 157, emphasis added.

[23] T. Bucher, *If… Then: Algorithmic Power and Politics* (2018) 49.

[24] Cordella and Shaikh, op. cit., n. 21, p. 3.

[25] Mol, op. cit. (2002), n. 11. See also E. Grabham, '"Praxiographies" of Time: Law, Temporalities, and Material Worlds' in *Routledge Handbook of Law and Theory*, ed. A. Philippopoulos-Mihalopoulos (2019) 91; I. van Oorschot, *The Law Multiple: Judgment and Knowledge in Practice* (2021).

[26] Law, op. cit., n. 22, p. 157.

[27] GIFCT, 'What Is the Hash-Sharing Database?' *GIFCT*, at <https://gifct.org/?faqs=what-is-the-hash-sharing-database>.

[28] See for example H. Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 *SMU Law Rev*. 27, at 66–80. Bloch-Wehba proposes the application of global administrative law as a solution for enhancing legitimacy.

Creating new categories for targeting 'terrorism' and 'violent extremism', for example, requires new practices and techniques for 'making up people' and assembling heterogeneous infrastructures (of humans, institutions, experts, and socio-technical practices) for bringing these targeting categories to life.[29] This raises difficult normative questions: for example, where are the boundaries between extremism and lawful expression to be algorithmically drawn? It also gives rise to coordination problems: how can these new classifications be made algorithmically enforceable across platforms and jurisdictions? What socio-technical links must be maintained to enable this governance at scale?

An *infra*-legalities approach hones in on such questions and prises open this problem space differently than conventional accounts. Because the actors of socio-technical interplays 'achieve their form and attributes as a consequence of their relations with other actors', a relational approach asks how the actors – even powerful states, platforms, and digital technologies – are enacted or reconfigured *through* this infrastructural arrangement.[30] This does not mean that Facebook, the GIFCT hash-sharing database, and the UK Home Office all have the same or no power.[31] It means 'bracketing' assumptions about where power is to map how it is reshaped *through* this problem by following the actors' interrelations. Doing so brings a much more empirically rich, contingent, and lively regulatory landscape into being. Use of the hash-sharing database, for example, is bringing states and platforms, and the dynamics of global security and informational capitalism, into novel and productive relation. This is giving states greater indirect control over the internet's infrastructure, while opening up further opportunities for platforms to push back against regulatory oversight initiatives that are seeking to impose platform liability for online harms. Analysing the hash-sharing database's technical features reveals that 'hashes' in the database cannot be reverse engineered into human-reviewable content. This is confounding calls for external oversight and catalysing new alliances between human rights groups and platforms looking to build mechanisms for online content preservation and reform data protection laws.[32] Critique is being rechannelled through the infrastructure of the database, in other words, in ways that expand the powers of platforms and states and open up novel routes for public–private infrastructural control.

To follow these relational dynamics and effects, an *infra*-legalities approach asks different sorts of questions than those usually asked in SLS research. For example, how are boundaries (public–private, human–machinic, legal–non-legal) redrawn or stabilized through global security infrastructures?[33] How do they facilitate or suppress new forms of knowledge, power, and regulation, making certain versions of the world more present than others? How are devices such as databases assembling relations in ways that '(re)configure social spaces, (re)draw boundaries and (re)distribute meanings'?[34] Neither the actors nor the field assembled through the database

[29] I. Hacking, 'Kinds of People: Moving Targets' (2007) 151 *Proceedings of the British Academy* 285; E. Ruppert, 'Category' in eds Lury and Wakeford, op. cit., n. 10, p. 36, at p. 38.

[30] Cordella and Shaikh, op. cit., n. 21, p. 3, citing J. Law, 'After ANT: Complexity, Naming and Topology' in eds Law and Hassard, op. cit., n. 11, p. 1, at p. 3.

[31] For such critique, see J. L. Davis, *How Artifacts Afford: The Power and Politics of Everyday Things* (2020) 50–60.

[32] BSR, *Human Rights Impact Assessment: Global Internet Forum to Counter Terrorism* (2021) 38, 44, at <https://www.bsr.org/en/our-insights/report-view/human-rights-impact-assessment-global-internet-forum-to-counter-terrorism>; Human Rights Center, UC Berkeley School of Law, *Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes* (2021), at <https://humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf>.

[33] L. Suchman, *Human–Machine Reconfigurations: Plans and Situated Actions* (2007, 2nd edn) 259–286.

[34] A. Amicelle et al., 'Questioning Security Devices: Performativity, Resistance, Politics' (2015) 46 *Security Dialogue* 293, at 298.

remain stable throughout (as they do in existing scholarship). Both are reshaped through the shifting conditions of the database infrastructure itself. How are forms of algorithmic regulation used in global security, displacing accountability and redrawing lines of exclusion – or putting new processes for 'making up people' and governing them as risky into motion?[35] Understanding such effects requires empirically analysing this global security infrastructure and the interrelations between the actors, regulatory practices, and socio-technical processes that compose it as emergent or in motion. Here, technologies are not studied as tools, but as agential devices enrolling and reconfiguring actors into productive networks, shaping knowledge and governance, aligning interests, deflecting critique, and allowing novel forms of ordering to emerge.

3 | SOCIO-MATERIALITY AND DISTRIBUTED AGENCY: MAPPING MULTIPLICITIES, AFFORDANCES, AND SCALE

A second related element of an *infra*-legalities approach to global security concerns the redistribution of agency and the associated idea that the social and the material are co-produced in practice. In the relational ontology of ANT, 'the social' is reimagined as fluid, materially entangled and contingently assembled and 'materiality' as something composed through socio-technical relations.[36] SLS has long engaged with materiality, but this has often involved analysing law through 'the materiality of human social interactions'.[37] More recent ANT-inspired SLS research has shown how relational accounts of socio-materiality – where 'the agents, their dimensions and what they are and do all depend on the morphology of the relations in which they are involved' – alters our approach to both 'the social' and 'the legal' in SLS research and opens up novel lines of enquiry that bring SLS and STS closer together.[38] This approach bypasses conventional structure/agency debates and detaches agency from human intentionality. Instead, agency is tied to 'the effects a character (or actant) has on [the] relational processes' of the socio-technical infrastructures of which they are part or the difference that they make.[39]

If agency is not solely a human capacity but the effect of socio-material entanglements, then a less human-centred approach to studying regulatory and technological change is needed. For Ruppert and colleagues, this means 'attend[ing] to the lives and specificities of devices and data themselves: where and how they happen, who and what they are attached to and the relations they forge, how they get assembled [and] where they travel'.[40] For Pottage and ANT-inspired SLS scholars, it means decentring the law to map how legal practices are reconfigured by socio-material relations by doing research that takes 'materiality rather than "law"' as its starting point.[41] Both

[35] R. Bellanova et al., 'Toward a Critique of Algorithmic Violence' (2021) 15 *International Political Sociology* 121; Hacking, op. cit, n. 29.

[36] B. Latour, *Reassembling the Social: An Introduction to Actor–Network Theory* (2005) 1–17.

[37] N. Graham et al., 'Broadening Law's Context: Materiality in Socio-Legal Research' (2017) 26 *Griffith Law Rev*. 480, at 484.

[38] M. Callon, 'Actor–Network Theory: The Market Test' in eds Law and Hassard, op. cit., n. 11, p. 181, at p. 185–186. See also van Oorschot, op. cit., n. 25; G. Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (2020).

[39] A. Leander, 'Locating (New) Materialist Characters and Processes in Global Governance' (2021) 13 *International Theory* 157, at 162.

[40] Ruppert et al., op. cit., n. 10, p. 32.

[41] Pottage, op. cit., n. 6, p. 183. See also E. Cloatre and D. Cowan, 'Legalities and Materialities' in ed. Philippopoulos-Mihalopoulos, op. cit., n. 25, p. 433.

steps are critical in studying global security infrastructures in action, particularly those reliant on AI and ADM techniques. In what follows, I outline three methodological moves for engaging with socio-materiality when researching security assemblages: attending to multiplicities, taking affordances seriously, and doing transversal, multi-sited ethnography.

Empirically grasping global security infrastructures in motion requires attending to multiplicities – that is, following how socio-material practices enact different versions of objects and social relations and empirically tracing how these enactments hold together (or do not) via various forms of coordination. As Mol argues, 'Objects come into being with the practices in which they are manipulated. And since the object of manipulation tends to differ from one practice to another, reality multiplies.'[42] Different socio-material practices do not merely produce different perspectives on the same object, in other words, but enact ontologically different versions of the object itself. The key empirical challenge lies in grasping this multiplicity and following how singularity is achieved and potentially conflicting realities are 'smoothed away' in practice by making some realities present while interfering with others – an ethnographic research practice that Mol terms 'praxiography'.[43] Seaver develops this idea for ethnographically studying algorithmic systems in motion and showing that 'algorithms are not singular technical objects that enter into many different cultural interactions, but … unstable objects, culturally enacted by the practices people use to engage with them'.[44] Understanding algorithms thus requires attending to their multiplicity in practice, using 'polymorphous engagement' strategies to engage with informants and devices across different sites and following how different 'collectives of human and non-human actors emerge, solidify and evolve' through their use.[45]

The 2025 UK Border Strategy, for example, seeks to harness 'the power of technology and innovation' to create a contactless digital bordering system to 'revolutionise crossing the border for traders and travellers' and 'improve the UK's ability to detect threats before they reach the border'.[46] All incoming traveller data (including passenger data and biometric data) will be collected in advance of travel, fused together with Home Office data, terrorism watchlist data, and other policing and security databases (both UK and international), and passed to a 'single window' for analysis using 'advanced analytics-enabled risk engines'.[47] Using machine-learning systems like British Aerospace Engineering's (BAE) Cerberus data analytics tool, this analysis promises to allow real-time risk assessments and provide actionable risk scores for UK border staff to make data-driven targeted security interventions.[48]

A conventional interpretivist social science approach such as grounded theory might analyse this system from the assumption that all knowledge is socially constructed and technology is socially embedded; it is used by people with shared understandings and meanings in social contexts where the capacities for human action are shaped by the features of the technology. Here,

[42] Mol, op. cit. (2002), n. 11, p. 5.

[43] Id.

[44] N. Seaver, 'Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems' (2017) 4 *Big Data & Society* 1, at 5.

[45] Id., p. 6; A. Christin, 'The Ethnographer and the Algorithm: Beyond the Black Box' (2020) 49 *Theory and Society* 897, at 906.

[46] HM Government, *2025 UK Border Strategy* (2020) 20, 23, 13, at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945380/2025_UK_Border_Strategy.pdf>.

[47] Id., pp. 21–23.

[48] BAE Systems, 'Using Data to Secure the UK Border' *BAE Systems*, at <https://www.baesystems.com/en/cybersecurity/feature/using-data-to-secure-the-uk-border>.

the researcher aims to draw out the latent understandings and socially ascribed meanings of the data analytics technology to build generalizable theory with explanatory power that can account for how this bordering system works (or does not). Participants would be engaged via interviews to identify 'underlying uniformities and diversities', find objective knowledge in the subjective expressions, and build theory from the data.[49]

A praxiographic approach might instead ask how risks are inferred from data in the human–machinic processes that the 2025 UK Border Strategy puts into motion. How do the effects of the BAE computer scientists–Cerberus data analytics configuration, for example, shape or diverge from the socio-materialities enacted by frontline border staff using risk scores to make security interventions? How is algorithmic objectivity performed across different sites – in policy documents, within the Home Office, in the design and use of the BAE data analytics tools – and how are the human choices of algorithmic governance obscured? Data is modified as it moves between sites and is combined with other sources, allowing different forms of security knowledge and intervention.[50] This movement is not seamless; it requires socio-technical relations whose maintenance needs continuous work.[51] Attending to multiplicities means drawing out such differences and practices to follow how risks from one form of data (such as terrorism lists) are made interoperable or translated as they move between sites and are combined with other processes (such as in data fusion centres). Rather than focusing on how the inner logic of AI technology is given social meaning, a praxiographic approach decentres algorithms and focuses on the socio-materialities that they enact – for example, by analysing how 'existing arrangements are reconfigured as people position themselves with respect to algorithms and seek to enroll them in their institutionalised ways of doing things'.[52] Here, the aim of the research is not to produce generalizable theory, but to understand how socio-material processes are differentially enacted and sustained to allow new forms of security knowledge and governance and to open up spaces for critique, contestation, and problematization – as elaborated in more detail below.

Taking technological affordances seriously means grappling with how the 'design of our technological objects and socio-technical environment condition and constrain possibilities for action' by subjects.[53] Affordances are not intrinsic properties of objects, but relationships between objects and users, 'jointly determined by the qualities of the object and the abilities of the agent that is interacting'.[54] For the purposes of this article, technological affordances are important for at least two reasons.

First, if socio-material relations are shaped by their affordances, then understanding these conditions is key in grasping how security works in practice. Governance through infrastructure

[49] B. Glaser and A. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research* (1967) 114; M. Packer, *The Science of Qualitative Research* (2011) 69.

[50] M. de Goede and G. Sullivan, 'The Politics of Security Lists' (2016) 34 *Environment and Planning D: Society and Space* 67, at 79.

[51] R. Bellanova and G. Glouftsios, 'Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance' (2022) 27 *Geopolitics* 160.

[52] Christin, op. cit., n. 45, p. 906.

[53] I use Yeung's definition of 'affordances': how the 'design of our technological objects and socio-technical environment condition and constrain possibilities for action'. K. Yeung, *Responsibility and AI: Council of Europe Study DGI(2019)05* (2019) 74, at <https://rm.coe.int/responsability-and-ai-en/168097d9c5>. On taking technological affordances seriously, see also J. E. Cohen, 'Affording Fundamental Rights' (2017) 4 *Critical Analysis of Law* 78; M. Hildebrandt, *Smart Technologies and the End(s) of Law* (2015); L. Diver, 'Law as a User: Design, Affordance, and the Technological Mediation of Norms' (2018) 15 *SCRIPTed: A J. of Law, Technology & Society* 4.

[54] D. Norman, *The Design of Everyday Things* (2013) 11.

shifts depending on whether the device used is a watchlist, a database, an automated filtering tool (such as the hash-sharing database), a supervised ML system, or a neural net algorithm that learns independently. Watchlists, for example, work through a logic of addition that requires government officials and experts to nominate individual and groups for list inclusion using pre-specified listing criteria. Human review is needed for selecting, constructing, and maintaining security lists. Security lists are often public, targeting criteria are legally defined, and listing decisions are often challengeable via judicial review. Flagging 'risky' individuals via Passenger Name Record (PNR) data analysis using ML, however, has different affordances. Individuals are targeted via the automated detection of patterns from vast amounts of data. Patterns or clusters are not built from pre-existing terrorist profiles or aimed at targeting 'known' threats; they emerge from correlational associations drawn between heterogeneous data sources algorithmically analysed to detect previously 'unknown' risks. Clusters are fluid objects, continually recomposed as new data is ingested from constantly changing datasets.[55] As such, there is little scope for meaningful human or judicial review throughout the entire targeting process.[56] Thus, while lists and algorithms are used together in the 2025 UK Border Strategy, they configure, enable, and constrain human–machinic relations very differently. Taking affordances seriously allows us to 'move between the inside and the outside of technical objects' and empirically highlight these crucial differences.[57]

Second, in reconfiguring human–machinic relations in global security governance, affordances also reshape possibilities for legal accountability and challenge. With the automated analysis of PNR data, for example, the risk of discrimination cannot be mitigated simply by deleting sensitive data. ML techniques can readily infer race or ethnic origin from other data that can serve as statistical proxies for these protected characteristics, such as postcode information or mobility patterns.[58] Moreover, trying to ensure fundamental rights compliance in algorithmic PNR governance by keeping a 'human in the loop' to make final targeting decisions may mean very little if human operators cannot understand how the ML models produce specific outputs and are making targeting decisions from simplified information presented via algorithmically generated dashboards. Calling for algorithmic security techniques to be made human rights compliant without understanding their socio-technical affordances misses these points entirely and makes such compliance efforts likely to be ineffective from the start.[59] Addressing problems of accountability and rights compliance in global security infrastructures and algorithmic decision making thus requires an empirical grasp of 'the central role of sociotechnical configuration in affording and constraining the freedoms and capabilities that people in fact enjoy'.[60] Taking affordances seriously is therefore a key component in *infra*-legalities research.

A third methodological move for engaging with socio-materiality in global security infrastructures involves doing transversal ethnographic research to map how global governance is fabricated in practice from interconnected localized sites. In conventional legal research, 'the global' is often taken as connoting something above us and all-encompassing. Such an approach makes

[55] Isin and Ruppert, op. cit., n. 20, pp. 9–10; Van Den Meerssche, op. cit., n. 16, pp. 17–20.

[56] Ulbricht, op. cit., n. 1.

[57] M. Akrich, 'The De-Scription of Technical Objects' in *Shaping Technology/Building Society: Studies in Sociotechnical Change*, eds W. E. Bijker and J. Law (1992) 205, at 206.

[58] Ulbricht, op. cit., n. 1, p. 152. See also L. Amoore, 'The Deep Border' (2021) *Political Geography* 1, at 6, at <https://doi.org/10.1016/j.polgeo.2021.102547>.

[59] Benvenisti, op. cit., n. 14.

[60] Cohen, op. cit., n. 53, p. 84. See also Yeung, op. cit., n. 53, p. 74.

researching global security infrastructures difficult – how can we study something so seemingly expansive? Yet global processes are always made from local structure-making sites that can be empirically studied.[61] Scales of governance – whether local, national, or global – are never pre-given but always created through particular socio-material practices. Studying these practices to grasp how scale is made and managed offers insights into how power asymmetries are forged, demystifying relations of violence.[62]

Breaking down global security infrastructures in this way draws attention to local structure-making sites where knowledge is produced to map their connections and ordering practices.[63] The production of global scale – that is, how local sites and socio-material practices are interwoven to allow actors to know and govern global security problems – thus becomes a key problem to be empirically examined. For Ribes, the ethnographic study of infrastructures requires empirical analyses of 'scalar devices' – that is, 'the assembly of techniques, tools and representational conventions … used to know and manage scale'.[64] Large problems are always made knowable and governable via various inscription devices – including benchmark metrics, indicators, or dashboards – and their associated representational practices. Following how scalar devices are developed and used across global security infrastructures to generate knowledge, shape organizational action, and make security problems governable thus becomes a key methodological concern.[65] Multi-sited methods also push us to analyse 'relations that connect actors (both human and technological) across sites and scales' rather than studying global governance 'as interactions between already existing entities like organizations located at mutually exclusive scales'.[66] This approach emphasizes transnational movements, deterritorialized flows, and relationality between actors and prompts different questions about how socio-technical elements are interconnected to sustain global infrastructures in practice.

The 2025 UK Border Strategy, for example, is building a largely automated global infrastructure based on advanced risk analytics and 'real-time sharing of data-driven insights'.[67] However, to do so, diverse translation practices and scalar devices must be assembled. Interoperability between different information systems must be established, data formats need standardization across sites, and data-sharing practices must be put in place – between government departments, with international partners and commercial bodies such as private airlines. Dashboards visualizing risk insights from ML must be used to combine data into a simplified format for use. How do these practices allow actors to make the global scale of their enterprise knowable and actionable? What socio-technical conduits are needed for the exchange of aviation data from airlines to the Home Office? How is watchlist data and the biometric data of all passengers collected, combined with other sources, and analysed in practice? What devices, information-sharing protocols, and techniques need alignment for travellers to be made legible and governable via this AI-driven data

[61] G. E. Marcus, 'Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography' (1995) 24 *Annual Rev. of Anthropology* 95.

[62] B. Latour, 'Visualization and Cognition: Drawing Things Together' (1986) 6 *Knowledge and Society* 1, at 27.

[63] Latour, op. cit., n. 36, pp. 175–176.

[64] D. Ribes, 'Ethnography of Scaling, or, How to Fit a National Research Infrastructure in the Room' (2014) *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* 158, at 160.

[65] S. Scheel et al., 'Enacting Migration through Data Practices' (2019) 37 *Environment and Planning D: Society and Space* 579.

[66] S. Scheel et al., 'Doing a Transversal Method: Developing an Ethics of Care in a Collaborative Research Project' (2020) 20 *Global Networks* 522, at 527.

[67] HM Government, op. cit., n. 46, p. 41.

fusion process? An *infra*-legalities approach empirically hones in on these socio-material processes to follow how connections between sites are established and how diverse information is gathered, transmitted, made commensurable, and analysed to make data-driven global security governance possible.

4 | *INFRA*-LEGALITIES AS METHOD ASSEMBLAGE: ONTOLOGICAL POLITICS AND CRITICAL SECURITY METHODS

The previous sections explored the methodological implications of adopting a relational ontology and focusing on socio-materiality in the study of global security infrastructures. This section explicitly extends these insights to the politics of SLS research methodology itself. Doing so reconfigures the relationship between theory, methodology, methods, and the empirical world. I argue that an *infra*-legalities approach is more than a tool for *representing* and *knowing* global security infrastructures; it is a method assemblage or arrangement of concepts, methods, and empirical objects for *enacting* and *critically intervening in* emergent security processes.[68] This claim is developed in two moves. First, I reposition methods as performative devices and elaborate on the idea of 'ontological politics' and its methodological implications. Second, I sketch two potential ways in which an *infra*-legalities approach can work as a method assemblage to critically intervene in emergent security infrastructure processes.

4.1 | Performative research methods and ontological politics

In conventional social science research, methods are often presented as tools for gathering data and representing the empirical world. An *infra*-legalities approach challenges this assumption by starting from the idea that methods are performative – that is, they 'help to shape and enact … [or] bring into being and reproduce … the very realities they are meant to study and describe'.[69] This shift has important consequences for how SLS research is designed, justified, and done. It reverses the conventional 'cascading path' approach to social science research design that separates theory (where all of the critical research stakes are decided), methodology (where 'the set of ideas that informs, justifies and validates the aims and methods of research' is settled), and methods (where data gathering tools are selected).[70] In this common approach, methods tend to be subsumed to prior 'debates driven by a formulation of a problem question, an ontology, an epistemology and a conceptual toolbox' and are selected on the basis that certain methods logically fit with the particular theory or epistemology being used.[71]

However, if methods enact social worlds and research problems are transformed through changing relations in practice (including via our empirical investigations), then we cannot stay with approaches to method that purportedly leave 'the worlds they represent untouched'.[72]

[68] Aradau et al., op. cit., n. 9.

[69] Scheel et al., op. cit., n. 66, p. 525.

[70] Aradau et al., op. cit., n. 9, p. 2.

[71] C. Aradau and J. Huysmans, 'Critical Methods in International Relations: The Politics of Techniques, Devices and Acts' (2014) 20 *European J. of International Relations* 596, at 598.

[72] Id., p. 603. See also Aradau et al., op. cit., n. 9, p. 3.

Performative research methods are thus best understood as *compositional practices* or *method assemblages* – that is, devices for 'experimenting with an assemblage of concepts, methods and empirical objects'[73] and putting them into 'knowledge-generating action',[74] and engaging with research problems that 'are ever forming and transforming across a problem space … that is itself changing'.[75] Here, methods are less about representing an external world to discover generalizable truths than about making worlds happen through research in ways that 'no longer seek the definite, the repeatable, the more or less stable'.[76] This shift suggests that we are always entangled in and enacting multiple worlds through our research, and it renders our choice and use of methods an intensely political process. As Law and Urry put it,

> If method is interactively performative, and helps to make realities, then the differences between research findings produced by different methods … have an alternative significance. No longer different *perspectives* on a single reality, they become instead the enactment of different *realities* … It is a shift that moves us from a single world to the idea that the world is multiply produced in diverse and contested social and material relations. The implication is that there is no single 'world'.[77]

The idea of a social world that can be accessed and properly understood if only we follow the methodological rules is a mainstay of social science research that has long played a gatekeeping role. It also performs a legitimizing role for influential variants of empirical legal studies research that seek to ground law and society scholarship in the task of better understanding how law works in 'the real world', to inform the development of appropriate doctrine and policy.[78] A performative approach to methods challenges the key epistemological and ontological assumptions of this conventional social science and empirical legal studies scholarship because it accepts that our knowledge of the social world is both simultaneously *real* and a performative *effect* of our methods. This shift means acknowledging that our knowledge production is necessarily *partial* and *situated* and that we are always entangled within the assemblages that we study.[79] Once we move from a single world to multiple, conflicting worlds made through socio-material practices, there is no getting around this – as feminist technoscience and related SLS scholarship has shown. To pretend that there *is* a privileged impartial space for research would be to try to pull what Haraway calls the 'God trick'.[80] We might try to use reflexivity as a methodological self-accounting device to mitigate the bias resulting from this situatedness. However, as Barad argues, reflexivity itself remains tied to logics of representation and problematically assumes that research methods can

[73] Aradau et al., id., p. 7.

[74] Aradau and Huysmans, op. cit., n. 71, p. 605.

[75] C. Lury, *Problem Spaces: How and Why Methodology Matters* (2021) 5, 9.

[76] Scheel et al., op. cit., n. 66, p. 525; Law, op. cit., n. 9, p. 6. On compositional method, see Lury, id., pp. 5–9, pp. 143–199.

[77] Law and Urry, op. cit., n. 13, p. 397.

[78] See for example Genn et al., op. cit., n. 12; B. Tamanaha, *Realistic Socio-Legal Theory: Pragmatism and a Social Theory of Law* (1997). Current SLS debates show the field to be far more methodologically diverse than these realist approaches suggest.

[79] R. Coleman and J. Ringrose, 'Introduction: Deleuze and Research Methodologies' in *Deleuze and Research Methodologies*, eds R. Coleman and J. Ringrose (2013) 1, at 6.

[80] D. Haraway, *Simians, Cyborgs and Women: The Reinvention of Nature* (1991) 183–201. See also M. Mason, 'On "Objectivity" and Staying Native' in *Routledge Handbook of Socio-Legal Theory and Methods*, eds N. Creutzfeldt et al. (2019) 123.

'reflect (social or natural) reality' and 'have no effects on the objects of investigation' if they are properly shorn of our subjectivity and politics.[81]

If detachment is not possible, then we need to pose different questions to grapple with the politics of method. For Law and Ruppert, this means asking: 'What is it that our methods are doing? What do they imply? What kinds of worlds are they opening up to us? And what kinds of worlds are they closing off?'[82] Because methods always enact certain realities while obstructing others from coming into being, they have an ontological politics – that is, an inventive potential for making present and absent versions of worlds that needs to be reckoned with.[83] As Law and Urry put it, 'If methods produce reality … the question is: which realities? Which do we want to help make more real, and which less real? *How do we want to interfere*?'[84] Rethinking methods in this way highlights the onto-political stakes involved. In my research, it prompts me to ask: how might we assemble methods, concepts, and sites to know and critique emergent global security infrastructures in action? How best to interfere?

4.2 | *Infra*-legalities as a critical security method

The STS method of 'infrastructural inversion' on which an *infra*-legalities approach draws works by making visible infrastructural conditions that have sunk into the background. However, doing so is never neutral. It enacts an ontological politics. I briefly outline below two possible ways in which an *infra*-legalities approach might work as a method assemblage for intervening in emergent infrastructural processes.

First, an *infra*-legalities approach can map algorithmic violence and its conditions of possibility – that is, 'how algorithmic systems feed into specific forms of violence, and how they justify violent actions or redefine which type of violence is considered legitimate'.[85] Because global security infrastructures usually target 'risky' people, groups, or patterns, they are tied to forms of political, administrative, and legal violence in ways that other kinds of global infrastructure are not. By showing how infrastructural relations emerge and are sustained, and how data is connected and curated to enable new forms of security knowledge and governance, an *infra*-legalities approach is ideally suited to mapping the conditions of possibility for algorithmic violence. Furthermore, by describing how these processes are enacted via emergent relations and practices, an *infra*-legalities approach can also show the contingencies of security power and how it might be made otherwise. Engaging with the dynamics of algorithmic violence is especially important here because the conventional legal tools used to constrain security power, such as human rights, no longer have the critical purchase that they once did, and because novel forms of power are being assembled through algorithmic security infrastructures that are reshaping global inequalities and enacting new forms of violence that urgently need mapping and intervention.

The 2025 UK Border Strategy, for example, is building a pre-emptive security infrastructure for all travellers to the UK based on the 'biometric "binding" of face and fingerprints pre-travel, carriers checking permission before travel for all persons, "living-suitability" checks conducted

[81] K. Barad, *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning* (2006) 72.

[82] J. Law and E. Ruppert, 'The Social Life of Methods: Devices' (2013) 6 *J. of Cultural Economy* 229, at 233.

[83] Mol, op. cit. (1999), n. 11.

[84] Law and Urry, op. cit., n. 13, p. 404, emphasis added.

[85] Bellanova et al., op. cit., n. 35, p. 123.

through integrated databases', and the use of advanced risk analytics tools for identifying suspicious patterns.[86] However, providing real-time risk scoring requires new processes for travel, biometric, and government data collection and interoperable data exchange – not just in the UK, but all around the world. This expands sites for potential exclusion and creates 'differential distribution[s] of security/insecurity' and novel sites for digital experimentation that can have profound adverse effects.[87] Making UK databases interoperable with the databases of international partners also stretches the spatiotemporal scope of bordering capabilities, enables new processes for 'making up people' and targeting them as 'risky', and significantly expands possibilities for pre-emptive security intervention around the globe.[88]

The use of advanced ML systems also enacts novel bordering capabilities. Deep learning algorithms work by continually ingesting vast amounts of heterogeneous data (as their learning improves with greater 'depth') and rendering equivalent all spaces as computational 'feature space' (to build rules from data features 'not pre-programmed in advance'), which expands the capacity for border violence.[89] As Amoore argues,

> When border spaces become feature spaces (and all data therefore becomes potential borders and immigration data), the means of bordering a political community enters every available space – the city street, the university campus, the clinic – and the feature space continually yields new data for modelling.[90]

By governing algorithmic clusters rather than using targeting categories based on pre-formed profiles, such systems reconfigure race in border security, forging new forms of data-driven inequality and 'actively circumventing existing legal protections'.[91]

By empirically mapping these infrastructure-formation processes, an *infra*-legalities approach draws together and makes contestable particular assemblages of relations that are enacting global security. Furthermore, by making the power asymmetries and regulatory reconfigurations of AI-driven security visible as socio-material practices, this approach opens up avenues for critically engaging with security data politics and confronting the legal challenges that they pose.[92] By showing the socio-technical conditions and affordances of fusing biometric and travel data, for example, we open up possibilities for critiquing the administrative violence of UK border security in ways that human-rights focused approaches miss. By describing the forms of disenfranchisement and inequality that such processes enable and the forms of legal or political contestation that they foreclose, we draw a diagram of power through our research that is forensically valuable and usable. If ML enacts clusters that do not fit in established legal frames, we might show how this misfit is empirically 'smoothed out' in practice and recast as a technical rather than a legal

[86] HM Government, *Border Innovation Hub Workshop* (2021) 6.

[87] P. Molnar, *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up* (2020), at <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

[88] HM Government, op. cit., n. 46, p. 44; Hacking, op. cit., n. 29. On interoperability, see M. Leese, 'Fixing State Vision: Interoperability, Biometrics and Identity Management in the EU' (2022) 27 *Geopolitics* 113; Sullivan, op. cit., n. 38, pp. 103–126.

[89] Amoore, op. cit., n. 58, p. 4.

[90] Id., p. 5.

[91] Id,. p. 6. See also Van Den Meerssche, op. cit., n. 16.

[92] E. Ruppert et al., 'Data Politics' (2017) 4 *Big Data & Society* 1, at 2. They define data politics as 'the ways data is generative of new forms of power relations … at different and interconnected scales'.

or political problem. If ADM processes promise to simplify border security, we can follow how they alter decision making in practice and reconfigure capacities for human judgment. In shifting the register of SLS research in such ways, an *infra*-legalities approach can engage *critically* with algorithmic violence by highlighting its infrastructural conditions of possibility.

Second, an *infra*-legalities approach opens up space for doing critique *through* infrastructure – that is, experimenting with ways of highlighting contradictions and tensions in security infrastructures as contingent, socio-material practices and bringing the different worlds that they enact together into 'one and the same world', not to create unification, but to stage what Rancière calls 'dissensus'.[93] The *Counterterrorism Watchlisting Toolkit* of the Global Counter Terrorism Forum (GCTF), for example, enacts a globally interconnected watchlisting infrastructure that uses biometric and travel data sharing, terrorism list and database interoperability, and predictive analytics to identify known and unknown terrorists in ways that are purportedly compliant with human rights. However, my empirical engagement with listed people has shown that while states may offer effective remedies to their own nationals, most of those watchlisted are foreign nationals who have no effective legal rights of redress at all.[94]

Thus, this watchlisting infrastructure works by enacting two divergent worlds: a Westphalian world of territorially bounded states, where human rights are coterminous with national jurisdictions, and a globally de-territorialized digital control architecture based on the real-time exchange of data about 'risky' people who have no rights protections, where regulation takes place outside the scope of law.

An *infra*-legalities approach might use empirical insights to highlight the disjunct between these worlds, show the inequalities that it embeds, and make rights claims together with those affected – rights that they evidently do not have. This requires a double negation and staging of 'dissensus: putting two worlds in one and the same world'.[95] Dissensus, for Rancière, is always a mode of contesting 'the frame within which we see something as given', and the subject of rights is never present but always a 'process of subjectivization' for opening up a political dispute about 'who is included in their count'.[96] An *infra*-legalities approach is suited to this kind of critique because of its empirical focus on data politics and the experiences of marginalized people 'as entry points to assess digital technologies and data practices in terms of the injustices and power asymmetries they help to enact and sustain'.[97]

The training and evaluation of ML models in global security also relies on the curation of datasets and various forms of data classification labour. Yet both the training data and the classification practices that enable ML to generate data-driven insights are usually made invisible or naturalized in conventional accounts of algorithmic governance.[98] Platforms like *Facebook* spend billions each year on online content moderation and have 40,000 people working on 'safety and

[93] J. Rancière, 'Who Is the Subject of the Rights of Man?' (2004) 103 *South Atlantic Q*. 297, at 304.

[94] R. Kassem et al., 'Watchlisting the World: Digital Security Infrastructures, Informal Law and the "Global War on Terror"' *Just Security*, 28 October 2021, at <https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/>.

[95] Rancière, op. cit., n. 93, p. 304. On double negation, see D. Haraway, *When Species Meet* (2008) 17.

[96] Rancière, id., p. 302, p. 303.

[97] M. Leese et al., 'Data Matters: The Politics and Practices of Digital Border and Migration Management' (2022) 27 *Geopolitics* 9.

[98] E. Denton et al., 'On the Genealogy of Machine Learning Datasets: A Critical History of ImageNet' (2021) 8 *Big Data & Society* 1.

security' issues around the world – including hundreds of in-house counterterrorism experts and thousands of outsourced moderators in sites such as India, the Philippines, and Kenya to review and label algorithmically flagged content.[99] What would it mean to rethink transparency in the global governance of TVEC online infrastructurally by taking such infrastructural processes into account? To shift the debate from quantification-orientated and platform-led transparency reporting that purports to look *inside* ADM, to algorithmic accountability that looks *across* AI-driven security as socio-technical infrastructure to show how informational capitalism is connected with and reconfiguring the global governance of TVEC in practice?[100] Or how ongoing immiseration and relations of division or precarious labour in the global 'periphery' are material preconditions for enabling AI-led security regulation elsewhere?[101]

These moves require a mode of empirical mapping capable of staging this kind of dissensus. With its emphasis on socio-materiality and commitment to transversal methods, an *infra*-legalities approach to global security infrastructures has the potential to do this kind of immanent critique. This opens up a generative space for law and society empirical research, but not as we ordinarily know it. Reframing SLS methods in this way promotes sustained engagement and action in relation to problems of security violence and inequity, rather than dispassionate detachment and observation. It engages with questions of power, but in ways that move beyond the human-centred materiality of much SLS research to follow how human–machinic processes are interconnected with regulatory practices. Finally, it sheds itself of the realist epistemology that has long haunted SLS – of showing law's effects in 'the real world' – by embracing method as a performative practice of intervention and interference.

5 | CONCLUSION

The proliferation of global security infrastructures and increasing use of algorithmic regulation and forms of ADM is presenting novel political challenges, enacting new forms of data-driven global power and inequality and reconfiguring the terrain for SLS law and technology research in significant ways. This article has argued that confronting these challenges requires a different approach to research methods and has outlined *infra*-legalities as a particular SLS method assemblage for following how regulatory practices and global data infrastructures are entangled and co-produced in practice. Furthermore, it has explored the key conceptual and methodological implications that arise when doing SLS research in ways that are ontologically relational and orientated towards emergent socio-material practices.

This move problematizes the claim that methods are representational tools for extracting data and conventional assumptions separating and ordering theory, methodology, method, and empirics. Drawing from ANT, critical security studies, and feminist technoscience scholarship, the *infra*-legalities approach advanced here seeks to reframe methods as compositional practices and

[99] *Facebook*, 'Our Progress Addressing Challenges and Innovating Responsibly' *Facebook*, 21 September 2021, at <https://about.fb.com/news/2021/09/our-progress-addressing-challenges-and-innovating-responsibly/>.

[100] On looking inside/looking across, see M. Ananny and K. Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2018) 20 *New Media & Society* 973, at 974, 984. On conventional TVEC transparency reporting, see GIFCT, *Transparency Report* (2021), at <https://gifct.org/wp-content/uploads/2021/07/GIFCT-TransparencyReport2021.pdf>.

[101] K. Crawford and V. Joler, *Anatomy of an AI System* (2018), at <https://anatomyof.ai/>.

performative devices that enact and interfere in the worlds that we describe (and constrain) through our research. The idea of method as interference frees us from the task of discovering generalizable theory from empirical data and the 'architectural idea of building a coherent and stable knowledge mansion',[102] by emphasizing situated knowledge and our always 'partial connections' with the worlds that we study.[103] Furthermore, it opens up space for experimenting with method assemblages that 'challenge that which is taken for granted and attend to the complexity of the world' enacted by global security infrastructures.[104]

The *infra*-legalities approach that I have outlined speaks to recent calls for 'impure' SLS methodological experiments that are attentive to social 'mess' and situated ways of knowing.[105] It brings earlier SLS debates on socio-materiality into dialogue with the algorithmic regulation processes of the present and resonates with calls to more explicitly incorporate human–non-human relations into SLS research design to better engage with unfolding environmental crises.[106] This approach contributes to wider interdisciplinary social research methodology debates in which methods are repositioned as inventive practices[107] and pushes us to explore the critical potential of STS infrastructure studies and 'thinking infrastructurally' when putting law and technology research on algorithmic regulation into practice.[108]

As global governance is increasingly enacted through complex digital architectures and their socio-technical practices, I have argued that the focus for critical SLS research in this area needs to pivot towards these data infrastructure processes and their emergent relations. Recent theoretical debates on legal materiality hold much promise for grappling with the algorithmic security assemblages described in this article. However, to intervene in and shape the social problems with which it is concerned, critical legal theory cannot remain at the theoretical level, with research methods either disregarded or relegated to mere instrumental status. It requires translation into practical experiments that can change how we *do* empirical legal research by challenging the habits and assumptions of conventional social research methodologies and opening up different practices for assembling critical research methods that are attuned to the material complexities of the present. The *infra*-legalities approach outlined in this article seeks to contribute to this process of interference and compositional SLS research practice.

ACKNOWLEDGEMENTS

Thanks to Linda Mulcahy at the Oxford Centre for Socio-Legal Studies and Rachel Cahill-O'Callaghan at the Cardiff Centre of Law and Society for inviting me to participate in the 2021 Challenging Socio-Legal Methodologies Workshop and ensuing Special Supplement. This article was written while visiting the University Center for Human Values (UCHV) at Princeton University in 2021. I am indebted to Kim Lane Scheppele for facilitating this visit and to UCHV for their generous hospitality. With thanks also to Dimitri Van Den Meerssche for feedback on an earlier

[102] Aradau et al., op. cit., n. 9, p. 7.

[103] M. Strathern, *Partial Connections* (2005).

[104] Aradau et al., op. cit., n. 9, p. 7.

[105] D. Cowan and D. Wincott, 'Exploring the "Legal"' in *Exploring the 'Legal' in Socio-Legal Studies*, eds D. Cowan and D. Wincott (2016) 1, at 3; Law, op. cit., n. 9.

[106] Faulkner et al., op. cit., n. 5; Graham et al., op. cit., n. 37.

[107] Lury, op. cit., n. 75; Lury and Wakeford, op. cit., n. 10; P. Vannini (ed.), *Non-Representational Methodologies: Re-Envisaging Research* (2015).

[108] B. Kingsbury, 'Infrastructure and InfraReg: On Rousing the International Law "Wizards of Is"' (2019) 8 *Cambridge International Law J*. 171, at 177.

draft and to Fleur Johns for generative conversations that helped to shape the ideas of this article. This research was supported by UK Research and Innovation (UKRI) Future Leaders Fellowship funding [Grant Ref: MR/T041552/1].

How to cite this article: Sullivan G. Law, technology, and data-driven security: *infra*-legalities as method assemblage. *J Law Soc.* 2022;1-20.
https://doi.org/10.1111/jols.12352