Australian and New Zealand Journal of European Studies
https://esaanz.org.au/anzjes/
Vol17(1)
ISSN 1837-2147 (Print)
ISSN 1836-1803 (Online)

Comparing border digitisation and transparency in the EU and Australia

Louis Everuss
Jean Monnet Centre of Excellence, University of South Australia
louis.everuss@unisa.edu.au

Alycia Millar
University of South Australia, Graduate
alyciagmillar@gmail.com

Abstract
Governments are increasingly investing in advanced digital technologies to improve the efficiency and security of their sovereign borders. Research examining this trend has emphasised how digital technologies are reshaping the operation of sovereign borders, but few studies have compared the differing ways that legal contexts influence digital bordering technologies. This article undertakes such an analysis by studying two contexts in which governments are enthusiastically engaging in border digitisation: Australia and the European Union (EU). Our analysis is informed by materialist and science and technology studies (STS)-influenced understandings of the law, which positions legal instruments not as restrictive frameworks that are external to socio-material contexts, but as an embedded part of them. From this perspective, we suggest that there are noteworthy differences in how the legal instruments developed about digital border systems in the EU and Australia are potentially contributing to the production of those systems. In particular, we argue that the EU's legal instruments are far more conducive to the enactment of transparent digital border systems compared to those deployed in Australia.

Keywords: Borders, digitisation, digital technologies, transparency, legal frameworks, STS, EU, Australia

Introduction

From smart gates to algorithmic risk assessment systems, governments are increasingly investing in modern bordering technologies in an effort to reduce the cost of assessing travellers and enhance the security of their sovereign borders. Research examining this trend has emphasised how digital technologies are reshaping the operation of sovereign borders (Amoore et al., 2008; Everuss, 2021a; Everuss, 2021, 2024; Pötzsch, 2015), but few studies have compared the differing ways that legal contexts influence digital bordering technologies. This article undertakes such an analysis by studying two contexts in which governments are enthusiastically engaging in border digitisation: Australia and the European Union (EU) (Lisle & Bourne, 2019; Wilson & Weber, 2008).

Our analysis is informed by materialist and science and technology studies (STS)-influenced understandings of the law, which position legal instruments not as restrictive frameworks that are external to socio-material contexts, but as an embedded part of them (Cole & Bertenthal, 2017; Pottage, 2012). Central to this

approach is the understanding that legal instruments are 'actants', entities that have a degree of agency because they contribute to the production of people, objects, and ideas (Cole & Bertenthal, 2017; Latour, 2005). For instance, a law can contribute to the creation of a person, not by physically giving birth to them, but by shaping their roles, actions, power, identity; and subsequently, who and what they are. Researchers influenced by this line of theory see regulatory outcomes as produced by the wider socio-material assemblages in which legal instruments are enacted through their relationships with other assemblage actants (e.g. Bellanova & de Goede, 2020).

From this perspective, we suggest that there are noteworthy differences in how the legal instruments developed about digital border systems in the EU and Australia are potentially contributing to the production of those systems. In particular, we argue that the EU's legal instruments are far more conducive to the enactment of transparent digital border systems compared to those deployed in Australia. This difference in the transparency potentials of advanced digital systems is not a causal outcome of differing legal obligations and requirements, but a feature of the different types of relationships enacted between legal instruments and other bordering actants, such as border technologies and human workers. The stark difference between the transparency of digitised bordering in the EU and Australia shows that even with the involvement of 'black box' algorithms and the dynamic nature of complex systems that are constantly in processes of enactment (Amoore, 2020; Leese, 2014), legal instruments remain powerful actants that can promote or hamper public transparency.

Law and the transparency of digitised borders

This article examines how processes of embedding and co-creation occur when new bordering technologies are used by governments to monitor and control the movement of people across sovereign borders. The sovereign border being studied here is not the static and legally defined Westphalian sovereign boundary, but instead the on-the-ground border produced when a decision is made about whether a traveller can enter the political community (Agamben, 1998; Everuss, 2020a, 2020b). This sovereign decision is traditionally seen as performed by individual human agents, such as border guards or even ordinary citizens bureaucratically placed into the borderer role (Salter, 2008; Yuval-Davis et al., 2018). However, bordering is never conducted solely by an individual because it relies on networks of non-human as well as human actants that include immigration laws and infrastructure (Scheel, 2019; Lisle & Bourne, 2019).

While legal instruments such as laws, regulations and policy documents influence many aspects of digital border technologies, the particular feature being examined in this article is transparency. Border transparency can be conceptualised as the degree to which people subject to border decisions, and the public in whose name border decisions are made, are able to know how those decisions are enacted and the stated rationales behind them. A degree of border transparency is believed to be necessary for upholding natural justice for those subject to bordering and the democratic rights of those in whose name bordering occurs (Lodge, 2003; Marenin, 2006). At the same time governments are required to maintain a degree of border opacity or 'operational secrecy' because full transparency of bordering processes could undermine the ability of states to perform their borders and thus define and protect their political communities (Moses & De Koker, 2018).

However, digitisation has added significant weight to the opacity side of this balance by stretching bordering assemblages further into the private sphere where there are fewer public disclosure obligations and more organisational rights to commercial confidence (Everuss, 2024, p. 99). Additionally, border opacity has been enhanced by the use of advanced algorithmic systems, which are often described as having a 'black box' nature due to their complex and constantly changing forms (Leese, 2014). Nevertheless, as this article shows, stark differences in the levels of digitised border transparency are emerging between jurisdictions, which can be connected to the legislative instruments integrated into digitised borders.

This is not surprising as border transparency is regularly framed as causally produced by the establishment of legislative obligations, administrative mechanisms to perform those obligations, and judicial avenues for their enforcement (e.g. Milaj & Bonnici, 2025; Musco Eklund, 2024). Subsequently, border transparency is often seen as an inherent outcome of legal mechanisms, especially legislative instruments that define transparency obligations. However, another way to conceptualise legal instruments is not as external guardrails or legal transparency obligations, but as components within digital border systems that relationally produce border technologies and thus are produced by them, as well as other system actants. When viewed in this fashion, legal instruments impact technological transparency in how they influence and enact actants within, and outputs of, bordering systems. At the same time, legal instruments are given their form in the ways actants understand and treat them.

To elaborate on this, we draw on materialist and science and technology studies (STS)-influenced accounts of law that study regulation and the material subjects of regulation as part of the same complex systems (Cole & Bertenthal, 2017; Pottage, 2012). This theoretical framework draws on Science and Technology Studies (STS) theories, such as actor-network theory (ANT), to challenge the notion that discreate legal instruments have the power to regulate or govern (Cole & Bertenthal, 2017). Instead, by embracing the type of relational and flat ontology proposed by ANT scholars such as Bruno Latour (1984) and John Law (2008), regulation and governance is framed as enacted by assemblages formed from legal instruments, human operators, objects, ideas and other entities that produce one another (Pottage, 2012).

A leading proponent of this conceptualisation of the law is Gavin Sullivan (2022, p. 33) who promotes '[a]n infra-legalities approach [that] looks below the law towards mundane socio-technical practices in global security governance, underscoring the important regulatory work that they perform.' For example, in a recent article Sullivan (2025) studied the regulation of 'terrorist and violent extremist content' (or 'TVEC') online, not by state-based legal frameworks or even international norms, but through the operation of the international public-private 'hash-sharing database of the Global Internet Forum to Counter Terrorism (GIFCT)'. Instead of seeing legal regulation as something external to this infrastructural assemblage, Sullivan (2025, p. 49) argues that regulation is the outcome of it, as the GIFCT 'regulates data flows architecturally, through ex ante design interventions'.

A similar approach was taken by Rocco Bellanova and Marieke de Goede (2020, p. 102) in their analysis of how 'algorithmic regulation is enacted through the custom-built transatlantic data infrastructures of the EU–US Passenger Name Records and Terrorism Financing Tracking Program programs.' When Bellanova and de Goede

(2020, pp. 102–103) studied the regulation *of* algorithms they did not isolate their analysis to legal instruments. Instead, they analysed how

> [s]ocio-legal features that regulate and condition these security programs – including limitations concerning system access and privacy safeguards – have become built into their architectures. Interfaces, especially software systems, regulate who can access and share specific datasets, and under what conditions. Thus, these security programs are important examples of novel types of regulation of algorithms, whereby algorithms are a target of regulation (Bellanova & de Goede, 2020, pp. 102–103).

Thus, for Bellanova and de Goede the regulation of algorithms is best identified not in legal instruments, but in how infrastructures are enacted in relationship to legal principles. The law materialises not as abstract symbolic forms, but as features of border infrastructures and processes. In line with ANT, Bellanova and de Goede are framing the regulation of algorithmic systems as emergent – arising from the relational actions of actants as opposed to being set by top-down directives.

When viewed as part of socio-material assemblages that produce regulatory outcomes, laws and other legal instruments are being viewed as part of the flat ontology of a digital border system as opposed to an external framework dictating that system's operations. The key question is no longer whether a system follows the law, but instead how legal instruments are relationally co-produced alongside different elements of that system, consequently influencing its outcomes. Examining this question sheds light on the fact that the ability of laws to shape an outcome depends on their relationship with other actants, such as whether humans or algorithmic decisions decide to follow or care about them. It is this type of question that is analysed below to determine how the legal instruments present in the EU and Australia are impacting border transparency is differing ways.

1 The European Union

The common management of external borders is a shared objective of EU Member States that have fully implemented the Schengen acquis. Historically, this objective has been inhibited by differing bordering systems across Member States. The European Commission (EC) sees border digitisation as a technological means of overcoming nationally specific approaches to bordering (Martins et al., 2022; European Commission 2008). As such, a range of EU level digital border systems have been developed, including the Schengen Information System (SIS) containing profiles of third-country nationals and EU citizens over which there are security or border related alerts, the Visa Information System (VIS) containing information pertaining to short-stay (Schengen) visas, and the EU's Passenger Name Record (PNR) assessment system, which is involved in the assessment of plane passenger data. Additionally, several EU digital border systems are currently being developed and rolled out, such as the Entry/Exit System (EES) that will record border crossings and replace passport stamping at the Schengen Border and the European Travel Information and Authorisation System (ETIAS), which will provide an assessment system and register for visa-exempt travellers.

EU Regulations and Directives have been produced about these digital bordering systems, which, along with other objectives, seek to render the systems transparent in ways that align to the promotion of democratic principles in border governance and the upholding of natural justice (Regulation 767/2008; Regulation 2017/2226; European Commission, 2016; Regulation 2018/1240). This includes by explicitly defining the architecture and components of digital bordering systems and thus exposing them to public scrutiny. For example, the VIS Regulation (767/2008) defines who can access the VIS database (article 6), the types of data that can be entered into the database (article 9), the location of the system's servers (article 27), and other system features.

Nevertheless, the VIS Regulation is not itself evidence of the material nature or reality of bordering actants. All that can be understood from the VIS regulation is its own form, which provides hints as to how it might influence other actants. To confirm this influence and how it is mediated, resisted and co-constituted by other actants, those other actants and the relationships they have with the VIS Regulation need to be brought into the analytical picture. In doing so we can see that sections of the VIS Regulation do accurately describe features of VIS actants, which indicates that the Regulation was either produced in a fashion that described the reality of actants, or actants were enacted in line with VIS Regulation descriptions. This is the case for VIS system servers which exist as described in article 27, namely within eu-LISA's central data centre in Strasbourg (France) and backed up by its continuity site in a mountain bunker in Austria's Pongau region (Trauttmansdorff, 2024, p. 15).

However, other aspects of VIS described in the Regulation are individually interpreted and implemented at Member State level. This was shown for instance in a 2016 report by the VIS Supervision Coordination Group (VIS SCG) – a body that comprised representatives from national data protection authorities (DPAs) and the European Data Protection Supervisor that coordinated supervision of VIS in accordance with relevant EU Regulations (now replaced by the Coordinated Supervision Committee that covers all EU Digital Border Systems) – which examined how access to VIS and the protection of data subjects' rights were being managed at a Member State level (VIS Supervision Coordination Group, 2016). For example, there was a wide variety of accounts from DPAs as to the number of law enforcement authorities and personnel with access to VIS data, and the level of information provided to national DPAs about this access (VIS Supervision Coordination Group, 2016, pp. 6–7). Likewise, a 2016 European Commission (2016) report on the establishment of VIS indicates that the extent to which Member State authorities enter full data sets into VIS is highly variable, something that has led to redesigns of the regulation of infrastructure-state actor relationships in order to promote complete data entry.

Another way that border transparency is promoted in the EU is through the establishment of transparency obligations towards subjects of bordering decisions, which upholds the rights of those subjects to natural justice (e.g. SIS Regulation [EU] 2018/1862, art 67; ETIAS Regulation 2017/2226, art. 52). For instance, Article 37 of the VIS Regulation establishes that people whose data is recorded in VIS are to be provided certain information about how their data is used and what rights of access they have. Additionally, Article 38 provides people with 'the right to obtain communication of the data relating to him or her recorded in the VIS and of the Member State which entered them in the VIS.' There are exceptions, allowing states to refuse to provide such data including for general public security and national security

grounds (Regulation 767/2008, art. 38[7]), but nonetheless, the regulation seeks to embed transparency mechanisms into VIS. While the VIS Regulation promotes the right to access information, the performance of that right requires people to be aware of it and know how to request information. In their 2016 report, VIS SCG (2016, p. 15) found that there had been very few requests, which was potentially 'explained by data subjects' unawareness of the very existence of their data protection rights but also by the lack of information about the way to exercise them (e.g. to whom data subjects should address their requests?).' This indicates that the VIS regulation is perhaps not influencing system actants to a significant extent when it comes to promoting the transparency rights of data subjects.

An in-depth analysis of the operation of rights of access towards digital border data was undertaken by Plixavra Vogiatzoglou et al. (2020), who examined the process for people to request access to their PNR data under national laws transposing the PNR Directive (2016/681). Vogiatzoglou et al.'s (2020) research is significant because it studied the relationship between legal instruments and other assemblage actants, including by engaging the assemblages through PNR information requests. This is important because the European Commission's own review of the PNR Directive focussed almost purely on whether legal mechanisms and administrative processes had been set up to protect data rights, but '[n]o mention is made of the practical exercise of data subjects' rights', or in other words, the actual operation of the relevant socio-legal assemblage (Vogiatzoglou et al., 2020, p. 278).

The way that the PNR Directive (EU2016/681) attempts to promote system transparency for data subjects is by applying the Council Framework Decision (2008/977/JHA) (which has subsequently been replaced by the Law Enforcement Directive 2016/680, arts 14–15), that grants people the right to know 'whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data' along with other information such as 'the categories of personal data concerned', 'the recipients or categories of recipients to whom the personal data have been disclosed', 'the existence of the right to request from the controller rectification or erasure of personal data'; although this right is limited by wide ranging national, public security and other grounds. However, being Directives, the PNR and Law Enforcement Directives need to be transposed into national level legislation to be legally enforceable, which has not uniformly occurred (Vogiatzoglou et al., 2020, pp. 291–292).

Furthermore, Vogiatzoglou et al.'s (2020, p. 293) research demonstrates that there is a vast difference in how easy Member State authorities make it to 'find meaningful information detailing the modalities and procedure for submitting access requests … with some websites providing very easily accessible information (like Cyprus's or Luxembourg's National Polices) and others a more complex presentation (for instance, Belgium's or the Netherland's authorities).' They also found differences in the difficulty of the submission process with most Member States allowing electronic communication, but a few requiring regular mail, some Member States required greater proof of address, and 'no official online presence of the Cypriot nor Portuguese PIUs was detected, while the Greek PIU did not appear to be operational at the time we sent our SARs' (Vogiatzoglou et al., 2020, p. 295). Such differences between Member States continued to characterise every step of the PIU request process, which produced differing request outcomes from the declaration that no data about the applicant was being processed, to the disclosure of data undergoing processing, and in

France and Italy, the provision of specific flight information held in the PNR system (Vogiatzoglou et al., 2020, p. 296). This research illustrates how the same legal instrument, namely the PNR Directive, is enacted in differing ways as it is embedded into different socio-material assemblages that shape an important part of border transparency, namely what people know about the processing of their data at the border.

2 AUSTRALIA

Like the EU, Australia utilises digital systems to manage and perform many of its bordering functions. These include the Integrated Client Services Environment (ICSE), Australia's main visa processing and case management system; the Immigration Records Information System (IRIS) which runs alongside ICSE and is used in the processing of some visa types (Australian National Audit Office, 2023, p. 63; Parliament of Australia, 2024, p. 83); Passenger Analysis Clearance and Evaluation (PACE), a system used to assess plane arrivals that matches passengers against alert lists (Australian National Audit Office, 2012, p. 87); and TRIPS, a computer system that records visa and passport details, and creates expected movement records (EMRs) for international travellers. In addition to these core programs, there are a range of other digital systems and databases that are utilised alongside ICSE, PACE and TRIPS. These include the Central Movement Alert List (CALM), an electronic watch list containing information about individuals deemed to pose an immigration or national security concern; and Safeguards, an automated risk management system used to identify visa applicants and travellers who match pre-determined profiles generated from confidential department information sources (Commonwealth Ombudsman, 2008).

This list of digital bordering systems is certainly not exhaustive and may not accurately reflect those currently in use. There is no publicly available register of Australia's digital boarding programs, so we have identified them from an assortment of government documents requested through freedom of information, partially redacted workplace manuals and Australian National Audit Office (ANAO) and Commonwealth Ombudsman reports. Additionally, and unlike in the EU, specific legislation is not established in relation to Australia's digital bordering systems. Instead, general legal instruments are used to define the powers of all digital bordering systems, as well as the transparency obligations associated with them. The most important piece of legislation in this respect is the *Migration Act 1958* (Cth), which defines the powers and scope of Australia's digital bordering systems in relation to the powers of the immigration minister. Section 495A(1) of the *Migration Act 1958* states:

> The Minister may arrange for the use, under the Minister's control, of computer programs for any purposes for which the Minister may, or must, under the designated migration law: (a) make a decision; or (b) exercise any power, or comply with any obligation; or (c) do anything else related to making a decision, exercising a power, or complying with an obligation.

The authority that can be assigned to computer systems is incredibly wide-ranging as the immigration minister, and now any computer system they elect, has almost absolute discretion over whether to grant or cancel certain visas and determine other border matters (Ghezelbash & Kinchin, 2025). Indeed, section 495A(2) explicitly states

that a decision made by a computer system designated by the minister, is taken to have been made by the minister themself. This law is a very different legal actant than a system-specific EU Regulation. The *Migration Act* contributes to the production of digital bordering systems by giving them authority, but without influencing in any meaningful fashion their structure or operations. It is thus a source of little border transparency, not because laws directly determine and are thus evidence of bordering outcomes, but because laws are actants so their details provide insights into how they may influence other actants.

The Australian legal instruments that do contain designs and outlines for how specific bordering systems should operate are largely forms of secondary law, like administrative instruments granting computer systems migration and border authorities under the Mi*gration Act*. Legislative and administrative instruments provide details about digital migration systems, such as what visa applicant characteristics are supposed to be assessed by ICSE in its automated visa determination (autogrant) of specific visa types (Department of Home Affairs, 2022a). However, administrative instruments are not a good source of transparency, because much of their description about how border actants are intended to operate are vague, and many instruments made in relation to bordering systems are not publicly available. Even when requested by FOI, they are significantly redacted. For instance, while some of the characteristics assessed for autogrant are described in a relevant instrument attained under FOI – including the nationality, age range and educational attainment of applicants – it is stated that 'a full list of key criteria is listed in attachment B', but attachment B is redacted (Department of Home Affairs, 2022a).

A form of legal instrument that does appear to hold a more influential position within bordering assemblages is the Department of Home Affairs and Australian Border Force's policy framework: the Policy and Procedure Control Framework (PPCF). This type of document, which is sometimes described as soft law, is potentially more powerful than generalist laws because it describes the specific procedures and steps that department staff are intended to follow in undertaking their duties. For example, the 'Use of Digital Device Examination to examine electronic devices' Standard Operating Procedure guides how Australian Border Force personnel should use their digital tools to examine and record the data from the mobile phones, laptops and other digital devices held by travellers (Department of Home Affairs, 2022b). This instruction includes the specific steps to be taken as part of the 'digital device examination procedure', almost all of which are redacted. Such instructions are included in training programs and made available to staff, further adding weight to the designs inscribed into them.

However, something that weakens the ability of the PPCF to structure other actants – whether it be by humans following its instructions or systems being designed in line with descriptions of them – is the diminished legal authority of the PPCF in comparison to ordinary law. The authority of the PPCF actually comes from its relationship with the Australian Public Service (APS) Code of Conduct, which states that 'an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction' (*Public Service Act 1999* [Cth], s. 13), which includes some sections of the PPCF. Subsequently, failure by Department personnel to comply with these sections could result in sanctions including employment termination. And the *Australian Border Force Act 2015* (Cth, s. 55[1]) extends this obligation to workers who are not APS employees

(such as contractors or consultants). However, other sections of the PPCF are considered guidelines or recommendations, and they do not have to be followed if a worker considers a departure 'reasonable and justified in the circumstances' along with several other considerations (Department of Home Affairs, 2022b).

While it is impossible to know the extent to which the PPCF influences other actants without detailed analysis of the relationships between these actants – something that is virtually impossible in the highly secretive environment of Australian border management – it can be suggested based on the detailed and instructional nature of the document, and its integration into training and availability to staff, that it is likely deeply embedded in bordering assemblages and thus influences other actants.

Nevertheless, like with the instruments described above, the ability of PPCF to promote public transparency into digital bordering systems is hindered by restrictions on its public availability and redactions for anyone other than Australian Department of Home Affairs (Department) staff. For instance, the *Arrival, immigration clearance and entry – Immigration clearance at airports and seaports* Procedural Instruction (2018, s 4.12) states that airport clearance through a SmartGate involves 'verifying the person is an eligible ePassport holder and, if applicable, that the person holds a visa that is in effect', checking 'biographical details on the Machine Readable Zone of the ePassport match the biographical details contained on the microchip of the ePassport', verifying 'whether the person is of health or character concern by asking health and character related questions to be answered via a touch-screen', verifying 'the person's identity using facial recognition technology', and something else which is redacted from the document. This is one of the most comprehensive statements about how airport SmartGates operate, which clearly indicates the role of an actant (likely an automated risk assessment, potentially the Safeguards program based on an administrative instrument by FOI (Department of Home Affairs, 2022a) that is not publicly disclosed.

There also appear to be examples in Australia of digital border systems having operated in the absence of significant guiding legal instruments. In examining the use of the Automated Profiling Tool (APT) during a 2011–2012 audit – a program that generated profiles that were matched against passengers for risk assessment – the ANAO (2012, p. 95) stated that:

> there is no national guidance document or plan applying to APT profile creation and management, and no national governance framework. This leaves considerable room for variation in the way that APT is used at airports, particularly in profile governance, creation and review, and match evaluation.

Essentially, while it was a powerful profiling tool, APT's usage was likely inconsistent between airports because official national plans and designs were not inscribed into legal or organisational instruments that could influence actants across Australia.

In relation to the second form of border transparency examined in this article, the transparency of bordering decisions to the people subject to those decisions, Australia lacks specific legislative instruments designed about its digital bordering systems. Instead, the transparency of digital border systems is treated as part of the Department of Home Affairs general transparency obligations under the Australian *Privacy Act 1988* (*Privacy Act*) and *Freedom of Information Act 1982* (*FOI Act*). This means that instead of specific privacy rules and obligations being imposed on digital bordering

systems, they are influenced by the general and technology-neutral Australian Privacy Principles that need to be interpreted in the digital border context, and which scholars argue are severely tested by biometrics and other relevant technology (Vasudevan et al., 2021). This is described by the Department (2025a) in very general terms that provide little insight into specific data collection and use practices.

More details are likely contained in Privacy Impact Assessments developed in relation to digital border systems and processes, such as the Electronic Travel Authority Mobile Application (ETA Mobile App) and the Baggage and Person Search System, but the details of privacy assessments are not publicly disclosed (Department of Home Affairs, 2025b). And like transparency obligations, the processes for data disclosure are managed by the *Privacy Act* and *FOI Act*. While the Department of Home Affairs website contains a specific online form for requests, there is no specialised process for people to apply to access data stored about them, or to amend that data if it is incorrect, which instead occurs as a general FOI request.

Potentials for border transparency in the EU and Australia

What is evident from the above analysis is that while there are striking similarities in terms of the border processes being digitised in the EU and Australia and the types of technologies involved, there are significant divergence in the forms of legal instruments created in relation to digital border systems. In the following section we examine how this different regulatory approach has the potential to create differing levels of border transparency between the two contexts.

As conceptualised in STS-influenced accounts of the law, legal instruments alone do not accurately represent or determine the complex systems that they form part of (Cole & Bertenthal, 2017; Pottage, 2012). Legal instruments are only actants which, like all other actants including humans, infrastructure and concepts, can co-produce one another and assemblage outcomes (Bellanova de Goede, 2020; Sullivan, 2025). Nevertheless, legal instruments are often significant actants because they are inscribed with official political plans and interests, and they normally carry the weight of assemblages designed to render them influential, such as administrative systems intended to promote legal compliance, judicial systems that attempt to enforce the law, and cultural discourses that promote respect for the law. Subsequently, the transparency of legal instruments can significantly influence the transparency of the larger assemblages in which they operate. However, the legal instruments developed in the EU and Australia in relation to bordering systems influence transparency in inverse ways.

In the EU the specific pieces of legislation or directives that operate in relation to digital bordering systems enhance the transparency of those systems. These legal instruments outline the official plans for system architecture, powers and operating principles. They go into detail about what data sets should be recorded and analysed, as well as what forms of data should be excluded from system analysis. And all of these EU-level instruments are publicly available. In contrast, in Australia official system designs are articulated in secondary administrative instruments and procedural documents that are only partially available to the public or not available at all.

The difference between these two approaches in terms of their potentials to enable digital border transparency is exacerbated by differing mechanisms for instrument

compliance. In the EU, there are monitoring bodies like the Coordinated Supervision Committee that are charged with supervising large scale IT systems and the EU bodies, offices and agencies that use them, in accordance with both the EU Data Protection Regulation (EU DPR) and the EU legal acts establishing specific IT systems, such as the VIS Regulation. Furthermore, the position of EU Regulations and Directives within the EU's larger socio-legal assemblages, as well as their public visibility, enables EU citizens and advocacy groups to attempt to enforce compliance through court action (Korff, 2023).

These avenues for border transparency largely do not exist in Australia. Legislation like the *Migration Act*, only contains vague and sweeping descriptions of digital border system authority, and it enshrines authority in the prerogative power of the executive. The hidden nature of administrative arrangements for the minister to confer powers onto computer programs makes it almost impossible to determine whether digital border systems are operating in alignment with the *Migration Act* and other legislation. Indeed, in another area of border performance – the exercise of statutory search and seizure powers – the ANAO found a lack of legislative instruments resulting in 'instances of potentially unlawful searches and failure to comply with instructions under both the *Customs Act* and *Migration Act,* which indicate current internal controls for mitigating the risk of unlawful or inappropriate use of coercive powers are inadequate.' And the soft law that does exist and describes digital system plans, like Australia's Procedure Control Framework (PPCF), is not all publicly available with key sections, especially those relating to digital border systems, kept confidential. Thus, failures by system actants to comply with, or more accurately, to be influenced by, Australia's legal instruments are not publicly revealed. Even if such breaches were known, compliance could not easily be enforced through judicial proceedings in the fashion of challenges related to breaches of legislation. And when a digital system has made an automated decision, there is the extra hurdle of Australian administrative law being 'focused upon human decision-makers', which means that 'the automation of decisions is likely to preclude judicial review' (Ng, 2021, p. 921).

Australia also lacks border system specific monitoring bodies, with public sector wide organisations such as the Commonwealth Ombudsman and ANAO instead tasked with assessing government compliance with border laws and investigating complaints (Ng, 2021). While both organisations have conducted insightful investigations into digital bordering systems, they do not systematically track the dynamic changes that are occurring to Australia's digital bordering systems or uncover many of the aspects of system architecture and design that are articulated in EU legislation about the EU's border systems. The inability of the Commonwealth Ombudsman to properly describe and thus provide transparency about Australia's digital bordering systems was captured in its report of the highly secretive Safeguards system, which automatically assesses visa applicants and travellers against risk profiles. The very name, 'Safeguards', is normally redacted from department manuals and other FOI requested documents (Department of Home Affairs, 2022a), and prior to its 2008 investigation, the Commonwealth Ombudsman appears to have been unaware of the system. In the introduction to their report, it is stated:

> This investigation arose out of a number of complaints to the Ombudsman about visa refusal decisions based on the Risk Factor List (RFL). In investigating DIAC's use of the RFL, we became aware of the Safeguards System and its use as a distributed system of intelligence gathering and analysis to support the visa

> decision-making process. While we have not received any complaints specifically about the Safeguards System, we are aware of complaints about visa refusal decisions that are likely to have involved the use of Safeguards information, even though the complainants were not made aware of this information (Commonwealth Ombudsman, 2008, p. 1).

This statement indicates that individuals subject to Safeguards' assessments, the general public, and a primary investigative agency of government decisions, all have little knowledge about Safeguards, a system that directly impacts Australia's visa decisions and other border operations. It is the equivalent of the EU's proposed ETIAS automated risk assessments not being articulated in legislation or indeed disclosed to the public in any fashion. The planned automated profiling of ETIAS applicants is currently the subject of much debate and controversy in Europe, including in relation to whether advanced algorithmic processes embed opacity into border decisions (Derave et al., 2022). Nevertheless, the existence of this debate is evidence of a level of border transparency that does not exist in relation to similar digital border systems in Australia.

Conclusion

This article has examined the digitisation of bordering in the EU and Australia. Our focus has been on the legal and political frameworks that influence the opacity of digital bordering technologies. It has been shown that there are significant overlaps in how border digitisation is occurring in the EU and Australia with digital systems being used for the same purposes, including visa processing, the advanced assessment of passenger information and the examination of travellers at customs clearance points. Additionally, the same technology companies are involved in both contexts, such as multinational IT companies Unisys and IDEMIA that have been contracted by the Australian government and The European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) to develop digital bordering systems including EES (eu-LISA, 2020; Wilson et al., 2021). Nevertheless, we have argued that the EU's approach to regulating digital bordering systems offers far greater potential for border transparency than the approach being taken in Australia.

This comparative conclusion is a departure from much of the literature on digitised bordering systems, which often focuses on inherent system opacity. As has become an almost cliché debate of research on advanced algorithmic processes, transparency in a complete sense may not be technically possible (Amoore, 2020; Ananny & Crawford, 2018; Burrell, 2016). Indeed, the unknowability of assemblages is a fundamental principle of the materialist theory that has influenced the STS-influenced accounts of law drawn upon in this article because it frames actants as being brought into existence through ongoing and dynamic processes of enactment. From this perspective, Sullivan (2022) argues that traditional approaches to legislating algorithmic systems, which treat them as predictable and discrete tools, fail. Sullivan (2022, p. 35) states that '[a]lgorithms perform security governance not as discrete tools but as heterogeneous socio-technical infrastructures or assemblages that are constantly unfolding in practice.' Additionally, recent research has suggested that aspects of the EU's regulations, like the prohibition on algorithms assessing certain prohibited traveller characteristics, are undermined by advanced algorithmic systems being able to engage in proxy coding whereby they assess prohibited characteristics via profiles constructed from available characteristics (Derave et al., 2022; Dumbrava, 2021). This

diminishment of the influence of regulation in the face of algorithmic agency is likely being exacerbated by the current push for EU database interoperability, which will expand the data available within digital bordering systems and make it more difficult to determine what data algorithmic systems are drawing upon (Vavoula, 2020).

These are important illustrations of forms of opacity embedded into the EU's bordering systems, which are being intensified by advanced digitalisation processes. However, such instances of opacity do not preclude the comparison made in this article between the transparency of border systems in the EU and Australia nor the conclusion that the EU's approach offers far greater transparency potentials. It would be a mistake to allow the inability to precisely know an algorithmic system to be used as a principle to flatten the different levels of transparency that exist between algorithmic systems. This paper has clearly demonstrated that a greater proportion of the EU's digitised bordering systems are brought into public view, which is, in a large part, driven by the types and public transparency of the legal instruments that are embedded within them. In contrast, very little of Australia's digital border systems are exposed to public scrutiny, something that is supported by the types of border-based legal instruments created in the Australian context.

Acknowledgements

This research was supported by the UniSA Jean Monnet Centre of Excellence, cofounded by the Erasmus+ Programme of the European Union.

References

Agamben, G. (1998). *Homo Sacer: Sovereign Power and Bare Life*. Stanford University Press.

Amoore, L. (2020). *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Duke University Press.

Amoore, L. Marmura, S. & Salter, M. (2008). Smart Borders and Mobilities: Spaces, Zones, Enclosures. *Surveillance & Society*, *5*(2), 96–101. https://doi.org/10.24908/ss.v5i2.3429

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New media & society*, *20*(3), 973–989. https://doi.org/10.1177/1461444816676645

Australian Border Force Act 2015 (Cth). https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/abfa2015225/

Australian National Audit Office. (2012). *Processing and Risk Assessing Incoming International Air Passengers*. Audit Report No. 50 2011–12. https://www.anao.gov.au/sites/default/files/201112%20Audit%20Report%20No%2050.pdf

Australian National Audit Office. (2017). *The Australian Border Force's Use of Statutory Powers*. ANAO Report No. 39 2016–17. https://www.anao.gov.au/sites/default/files/ANAO_Report_2016-2017_39.pdf

Australian National Audit Office. (2023). *Management of Migration to Australia – Family Migration Program*. Auditor-General Report No. 16 2022–23.

https://www.anao.gov.au/sites/default/files/2023-03/Auditor-General_Report_2022-23_16.pdf

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*. *16*(1), 102–118. https://doi.org/10.1111/rego.12338

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Cole, S. A., & Bertenthal, A. (2017). Science, Technology, Society, and Law. *Annual Review of Law and Social Science*, *13*, 351–371. https://doi.org/10.1146/annurev-lawsocsci-110316-113550

Commonwealth Ombudsman. (2008). *Department of Immigration and Citizenship: The Safeguards System*. Report No. 07/2008 https://www.ombudsman.gov.au/__data/assets/pdf_file/0023/26186/investigation_2008_07.pdf.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350, 60–71.

Department of Home Affairs. (2018). *Arrival, immigration clearance and entry – Immigration clearance at airports and seaports*. Procedural Instruction BC-536.

Department of Home Affairs. (2022a). FOI Request – FA 22/02/00278. https://www.homeaffairs.gov.au/access-and-accountability/freedom-of-information/disclosure-logs/2022

Department of Home Affairs. 2022b. FOI Request – FA 22/01/00786, Canberra, Australia. https://www.homeaffairs.gov.au/foi/files/2022/fa-220100786-document-released.PDF

Department of Home Affairs. 2022c. FOI Request – FA 19/05/01096. https://www.homeaffairs.gov.au/foi/files/2019/fa-190501096-document-released.PDF

Department of Home Affairs. (2025a). *Privacy policy*. https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/plans-and-charters/privacy-policy.

Department of Home Affairs. (2025b). *Privacy Impact Assessment Register*. https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/privacy/privacy-impact-assessment-register

Derave C., Genicot N., & Hetmanska N. (2022). The Risks of Trustworthy Artificial Intelligence. *European Journal of Risk Regulation*. *13*(3), 389–420. https://doi.org/10.1017/err.2022.5

Directive 2016/680. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision. 2008/977/JHA*. https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

Directive 2016/681. *Directive (EU) 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*. https://eur-lex.europa.eu/eli/dir/2016/681/oj/eng

Dumbrava, C. (2021). Artificial intelligence at EU borders: Overview of applications and key issues. PE 690.706. European Parliamentary Research Service. https://doi.org/10.2861/91831

eu-Lisa. (2020). *Ex-Post Publication, Annual List of Contracts Signed in 2020, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*. https://www.eulisa.europa.eu/sites/default/files/documents/contracts-awarded-2020.pdf.

European Commission. (2008). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Preparing the next steps in border management in the European Union*. COM/2008/69 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008DC0069

European Commission. (2016). *Communication from the Commission to the European Parliament, the European Council and the Council, Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*. COM/2016/0602. https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:52016DC0602

European Commission. (2016). *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*. COM/2016/655 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0655&qid=1755298382197

Freedom of Information Act 1982 (Cth). https://www.legislation.gov.au/C2004A02562/2018-12-29/text

Everuss, L. (2020a). Mobile sovereignty: The case of 'boat people' in Australia. *Political Geography*, *79*, 102162. https://doi.org/10.1016/j.polgeo.2020.102162

Everuss, L. (2020b). Westphalian sovereignty as a zombie category in Australia. *Borderlands*, *19*(1), 115–146. https://doi.org/10.21307/borderlands-2020-006

Everuss, L. (2021). AI, smart borders and migration. In A. Elliott (Ed.), *The Routledge Social Science Handbook of AI* (pp. 339-356). Routledge.

Everuss, L. (2024). *Digital Mobilities and Smart Borders: How Digital Technologies Transform Migration and Sovereign Borders*. De Gruyter.

Ghezelbash, D., & Kinchin, N. (2025). Automated Decision-Making in Australia's Migration System: Risks and Opportunities. *UNSW Law Research*, 25-19. https://dx.doi.org/10.2139/ssrn.5286438

Korff, D. (2023). Did the PNR judgment address the core issues raised by mass surveillance? *European Law Journal*, 29(1–2), 223–236. https://doi.org/10.1111/eulj.12480

Latour, B. (1984). The powers of association. *The Sociological Review*, *32*(S1), 264–280. https://doi.org/10.1111/j.1467-954X.1984.tb00115.x

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

Law, J. (2008). On sociology and STS. *The Sociological Review*, *56*(4), 623–649. https://doi.org/10.1111/j.1467-954X.2008.00808.x

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*(5), 494–511. https://doi.org/10.1177/0967010614544204

Lisle, D. & Bourne, M. (2019). The many lives of border automation: Turbulence, coordination and care. *Social Studies of Science*, *49*(5), 682–706. https://doi.org/10.1177/0306312719870868

Migration Act 1958 (Cth). https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/ma1958118/

Lodge, J. (2003). Transparency and EU Governance: Balancing Openness with Security. *Journal of Contemporary European Studies*. *11*(1), 95–117. https://doi.org/10.1080/14782800305483

Marenin, O. (2006). Democratic oversight and border management. In M. Caparini & O. Marenin (Eds.), *Borders and Security Governance: Managing Borders in a Globalised World*. DCAF.

Martins, B. O., Lidén, K. & Jumbert, M. (2022). Border security and the digitalisation of sovereignty: insights from EU borderwork. *European Security*, *31*(3), 475–494. https://doi.org/10.1080/09662839.2022.2101884

Milaj, J., & Bonnici, J. P. M. (2025). Transparency as the defining feature for developing risk assessment AI technology for border control. *International Review of Law, Computers & Technology*, *39*(2), 140–151. https://doi.org/10.1080/13600869.2024.2364996

Moses, L., & De Koker, L. (2018). Open secrets: Balancing operational secrecy and transparency in the collection and use of data by national security and law enforcement agencies. *Melbourne University Law Review*, *41*(2), 530–570. https://law.unimelb.edu.au/__data/assets/pdf_file/0006/2771439/03-Bennett-Moses-and-de-Koker.pdf

Musco Eklund, A. (2024). Limits to discretion and automated risk assessments in EU border control: Recognising the political in the technical. *European Law Journal*, *30*(1)-2, 103–121. https://doi.org/10.1111/eulj.12513

Ng, Y.-F. (2021). Institutional adaptation and the administrative state. *Melbourne University Law Review*, *44*(3), 889–927. https://law.unimelb.edu.au/__data/assets/pdf_file/0008/3898601/04-Ng-889.pdf

Parliament of Australia. (2024). *Joint Standing Committee on Migration – Migration, Pathway to Nation Building*. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000214/toc_pdf/Migration,PathwaytoNationBuilding.pdf

Pottage, A. (2012). The Materiality of What? *Journal of Law and Society*, *39*(1) 167–183. https://doi.org/10.1111/j.1467-6478.2012.00576.x

Pötzsch, H. (2015). The Emergence of iBorder: Bordering Bodies, Networks, and Machines. *Environment and Planning D: Society and Space*, *33*(1), 101–118. https://doi.org/10.1068/d14050p

Privacy Act 1988 (Cth). https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/pa1988108/

Public Service Act 1999 (Cth). https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/psa1999152/

Salter, M. (2008). When the exception becomes the rule: borders, sovereignty, and citizenship. *Citizenship Studies*, *12*(4), 365–380. https://doi.org/10.1080/13621020802184234

Scheel, S. (2019. *Autonomy of migration? Appropriating mobility within biometric border regimes*. Routledge.

Regulation 767/2008. *Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)*. https://eur-lex.europa.eu/eli/reg/2008/767/oj/eng

Regulation (2018/1240. *Regulation (EU) 2018/1240 of the European Parliament And Of The Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226*. https://eur-lex.europa.eu/eli/reg/2018/1240/oj/eng

Regulation 2017/2226. *Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011*. https://eur-lex.europa.eu/eli/reg/2017/2226/oj/eng

Sullivan, G. (2022). Law, technology, and data-driven security: infra-legalities as method assemblage. *Journal of Law and Society*, *49*(S1), S31–S50. https://doi.org/10.1111/jols.12352

Sullivan, G. (2025). Algorithmic governance of 'terrorism' and 'violent extremism' online. *London Review of International Law*, *13*(1), 47–75. https://doi.org/10.1093/lril/lraf005

Trauttmansdorff, P. (2024). *The Digital Transformation of the European Border Regime*. Policy Press.

Vasudevan M., Wood E. & Cross K. (2021). Identity at Risk: Are Australia's Privacy Laws Prepared for Growth in the Use of Biometric Data?. *Privacy Law Bulletin*, *18*(8), 168–171. https://search.informit.org/doi/10.3316/agispt.20220131061231

Vavoula, N. (2020). Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?. *European Public Law*, *26*(1), 131–156. https://doi.org/10.54648/euro2020008

VIS Supervision Coordination Group. (2016). *Report on access to the VIS and the exercise of data subjects' rights*. https://www.edps.europa.eu/sites/default/files/publication/16_02_report_on_access_vis_exercise_data_subjects_rights_en.pdf

Vogiatzoglou, P., Tavárez, K. Q., Fantin, S., & Dewitte, P. (2020). From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives.

Journal of Intellectual Property, Information Technology and Electronic Commerce Law. *11*(3), 274–302. https://www.jipitec.eu/jipitec/article/view/287

Wilson, D. and Weber, L. (2008). Surveillance, Risk and Preemption on the Australian Border. *Surveillance & Society*, *5*(2), 121–141. https://doi.org/10.24908/ss.v5i2.3431

Wilson, L. E., Wright, K., Lennard, C. & Robertson, J. (2021). Australian biometric system to meet national security objectives – part I technical capabilities. *Australian Journal of Forensic Sciences*, *53*(6), 640–651. https://doi.org/10.1080/00450618.2020.1766112

Yuval-Davis, N., Wemyss, G. & Cassidy, K. (2018). Everyday Bordering, Belonging and the Reorientation of British Immigration Legislation. *Sociology*, *52*(2), 228–244. https://doi.org/10.1177/0038038517702599