SOCIAL PRISM

Volume 3(9), 2026, 166-187
Online ISSN: 3006-8886
Print ISSN: 3006-8878

Regulating Personal Data in the Age of Artificial Intelligence: A Comparative and Critical Analysis of Privacy, Accountability and Digital Governance in the United Kingdom and Australia

Muhammad Shoaib[1], Aamir Khan[2]

[1]LLM Scholar, Brunel University London, United Kingdom Email: shoaibwassan105@gmail.com
[2]PhD Scholar, University Gillani Law College, Bahauddin Zakariya University, Multan, Pakistan
Email: aamirhashimkhan@gmail.com

Abstract

Artificial intelligence (AI) systems now make use of personal data to predict, classify and decide things like access to jobs, credit and public services. This article poses the question of whether the data protection legislation of the United Kingdom (UK) and Australia is open to any real challenge to such decisions. It uses doctrinal and functional legislative and case law comparison, regulatory decisions, official reports and scholarship, and states the law as of October 2026. It creates a contestable accountability mechanism to determine if the law connects lawful data usage, advanced risk assessment, notice at the decision-making level, intelligible reasons, effective human oversight, auditable data records and accessible redress. In the UK, since the Data (Use and Access) Act 2025 came into effect in February 2026, it is possible to make important decisions based solely on automated processing of non-special category data, as long as there are safeguards in place to ensure that information is represented, contested and that humans are involved. Australia's privacy laws are principles based. There is no general right to reasons or human review of a particular decision from 10 December 2026, the privacy policy is required to describe certain automated decisions. The new statutory privacy tort does not fill this gap but provides a remedy. Both systems are incomplete with respect to the framework. The UK does not have a clear right to personalised reasons and has lowered its threshold for automation. Australia has no decision level rights or a general obligation to review high-risk processing. The article proposes targeted reforms which are suitable to each legal tradition.

Keywords: artificial intelligence; data protection; privacy; automated decision-making; accountability; contestability; United Kingdom; Australia

Introduction

Artificial intelligence has changed the role of personal data. Personal data no longer is used just to identify, contact or maintain records of individuals. They also employ it to deduce preferences, forecast behaviour and grade risk, create profiles and make or support decisions. The key question in the law in these areas of employment, lending, insurance, health, policing and public administration, is therefore not only whether data were lawfully collected. It is also if the affected person can understand, contest and have a significant decision reviewed that was made with the assistance of an AI system. Privacy law has been primarily created to govern inputs: collection,

Received 08 October 2026; Revised 19 October 2026; Accepted 07 November 2026; Published (online) 10 November 2026

Attribution 4.0 International (CC BY 4.0)

Corresponding Author Email: shoaibwassan105@gmail.com

DOI: https://doi.org/10.69671/socialprism.3.9.2026.327

Online ISSN: 3006-8886
Print ISSN: 3006-8878

use, disclosure and security. It is not always the decision-making authority that is given to the output of an AI system. As a result, scholars have shifted from opacity to accountability, contestability and institutional control in algorithmic regulation (Kroll et al., 2017; Yeung, 2018).

The UK and Australia provide a helpful comparison. They both have common law systems, independent privacy regulators and similar data protection principles, but have recently taken different decisions regarding automated decision-making. In the UK, section 80 of the Data (Use and Access) Act 2025 (DUAA) introduces new Articles 22A to 22D of the UK General Data Protection Regulation (UK GDPR) which came into effect on 5 February 2026 (ICO, 2026a). These rules eliminate the blanket ban on significant automated decisions based on non-special category information but do not compromise information safeguards, contestation and the human intervention. The Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) continue to be the primary structure in Australia. Automated decision transparency requirements are introduced into APP 1 on 10 December 2026 under the Privacy and Other Legislation Amendment Act 2024 (Cth), but do not include an individual right to human review (OAIC, 2026a, 2026c).

On the surface, the UK is rights-based, and Australia principles-based. The DUAA provides increased flexibility to automate, while maintaining procedural protections. Australia has a broader range of controls, such as regulator guidance, public sector governance guidance, administrative law, the lessons from the Robodebt Royal Commission and a new statutory tort for privacy which commenced on 10 June 2025 (OAIC, 2025; Royal Commission into the Robodebt Scheme, 2023). The actual problem is if the guidelines establish accountability where AI is used to make an important decision based on personal data.

This article begins with introduction in section 1. The research problem, gap and questions are presented in Section 2. The research methodology is explained in section 3. The legal framework is presented in Section 4, and the contestable accountability framework is developed. A comparison of the two jurisdictions is made in Section 5, practical challenges are discussed in Section 6, answers to the research questions are provided in Section 7, recommendations are provided in Section 8 and the final conclusions in Section 9.

Research Problem, Research Gap and Research Questions

The research problem is the disconnect between decision-making rules and the capabilities of AI-assisted decisions. While the principles of lawful collection, purpose limitation, data minimisation, accuracy, security and transparency may all be applied, the affected person may still not be aware that an algorithm contributed to an important decision, what the key factors were, or how to get the algorithm reconsidered. An explanation is of little value if it is not accompanied by a remedy that will alter the outcome, as Edwards and Veale (2017) have pointed out.

This is an issue that is made more urgent by recent reforms. DUAA makes a conscious effort to broaden the scope of substantial automated decisions that can be taken on non-special category data, while safeguarding them (DSIT, 2025; ICO, 2026a). Australia's leap is less. The introduction of privacy policies in new APPs 1.7 to 1.9, which are to outline the categories of personal information that are being used, and the types of decisions being made through automated means

Online ISSN: 3006-8886
Print ISSN: 3006-8878

(Privacy and Other Legislation Amendment Act 2024 (Cth), sch.). 1, pt. 15). Whether these reforms target the point of harm or primarily boost disclosure in general.

Some aspects of this issue have been explored in the existing literature, such as; whether the GDPR provides a right to explanation (Selbst & Powles, 2017; Wachter et al., 2017), whether explanation is an effective remedy (Edwards & Veale, 2017), counterfactual explanations (Wachter et al., 2018), impact assessments (Kaminski & Malgieri, 2021), contestability by design (Alfrink et al., 2023) and the limits of human oversight (Green, 2022). There is a statutory right to explanation proposed for Australia (Gacutan & Selvadurai, 2020) and there are dangers in opaque automated administration, as with Robodebt (Henman, 2025). Two gaps remain. Firstly, much of this work is done prior to the DUAA and the 2024 Australian changes. Second, it typically considers the data collection, decision rights and remedies, and data collection to correct a harmful decision, as separate matters, and few courts subject the data collection to an examination of whether it is related as one chain from the data collection to the decision to correct the harmful decision.

The main research question is: what are the current UK and Australian data protection laws and how contestable is AI-assisted significant decision making based on personal data? and what are the necessary reforms to address current gaps? The first sub-question (RQ1) is designed to assess the effectiveness of each system in controlling the collection, inference and use of personal and sensitive information in AI systems. The second (RQ2) concerns the procedural rights that should accompany the making of a significant decision by an AI, such as the right to be notified, to be given reasons, to contest and to have a human review. The third (RQ3) is whether these rules are effective in practice by means of enforcement, remedies and oversight.

The article is a contribution in three directions. It creates a framework to evaluate data rules, decision rights and remedies as a whole. It offers a comparison post-DUAA and the 2024 Australian changes. It recommends changes that are directly related to the gaps identified. The claims are doctrinal and normative; the article is not a measure of organisational behaviour.

Methodology

Research Approach

The article adopts a doctrinal legal research method and functional comparative analysis method. Doctrinal research identifies, interprets and evaluates legal rules that are contained in legislation and case law (Hutchinson & Duncan, 2012). Functional comparison is not based on the comparison of rules with similar names, but rather it begins with a shared practical problem and asks how the different legal systems deal with it (Van Hoecke, 2015; Zweigert & Kötz, 1998). The common issue is the regulation of major decisions made or supported by AI systems based on personal data, by law.

Selection of Jurisdictions and Sources

The UK and Australia were chosen because they both have independent privacy regulators and similar privacy principles, a common law tradition, and were recently reformed in different

Online ISSN: 3006-8886
Print ISSN: 3006-8878

directions with regard to automated decision-making. This makes them a great, matched pair. The comparison does not necessarily reflect all common law jurisdictions.

Four criteria were used for the selection of the sources. Legislation was included where it was in force and directly applies to the personal data of AI systems, the UK GDPR as amended, the Data Protection Act 2018, the Human Rights Act 1998, the Privacy Act 1988 (Cth) and the Privacy and Other Legislation Amendment Act 2024 (Cth) with Article 17 of the International Covenant on Civil and Political Rights (ICCPR) as context. Second, cases and regulatory decisions were selected where they were issued by a superior court or specialist court or the national regulator and directly concerned with one of the stages of governance: scope of personal information, lawfulness of collecting, impact assessment, transparency, territorial scope, or remedies. Biometric cases were selected as the most clear-cut AI related cases in both countries. Other non-AI cases (e.g., Experian, Australian Clinical Labs, Lloyd and Vidal-Hall) were added because of the general questions that are relevant to AI. Third, interpretative guidance and reform reports were used as tools to help with the interpretation, but not law (Attorney-General's Department, 2023a; AHRC, 2021; ICO, 2023; ICO & The Alan Turing Institute, 2020; OAIC, 2024a). Fourth, academic sources were chosen from those that were peer-reviewed and directly related to the topics of explanation, contestability, accountability or impact assessment.

Comparative Evaluation Criteria

Each jurisdiction is judged on seven criteria based on the framework in Section 4 (Table 1). Where a binding law provides a general legal duty or right, it is categorized as "provided," where a binding law has limited protection, is sector-specific or has protection primarily through guidance, it is categorized as "partly provided" and where a binding law does not provide for general legal protection, it is categorized as "not provided. It is a qualitative method, which has been used here.

Table 1: Comparative Evaluation Criteria Derived from the Contestable Accountability Framework

Code	Criterion	Evaluation question
C1	Lawful and limited data use	Does the law require a lawful or authorised purpose, necessity and extra protection for sensitive data, including inferred data?
C2	Prior risk assessment	Must organisations assess high-risk processing before deployment?
C3	Decision-level notice	Must the individual be told that automation materially affected a particular significant decision?
C4	Intelligible reasons	Must the individual receive the main reasons in a form that allows challenge?
C5	Effective human review	Can the individual obtain review by a person with authority to change the outcome?
C6	Auditability and oversight	Must records allow a regulator to reconstruct and test significant automated decisions?

Online ISSN: 3006-8886
Print ISSN: 3006-8878

C7	Accessible remedies	Are practical regulatory and judicial remedies, including corrective orders, available?

Source: Created by the authors. The criteria are drawn from the three layers of the framework explained in Section 4.4.

Scope and Limitations

This analysis is limited to personal data governance, rather than all AI regulation. Other areas of law are only referenced if they have a bearing on privacy accountability. The design of the new APPs 1.7 to 1.9 is considered, as these are set to begin on 10 December 2026. There is a lack of clarity as to what will be included in future regulations under Article 22D. The study focuses on the law in the books and in decisions, not organisational practice.

Legal and Theoretical Framework

Human Rights Foundations

Informational privacy is not just about secrecy, but a condition for lawful and accountable power over people (Lynskey, 2015). Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life and the necessity of public interference to be lawful, necessary and proportionate. UK public bodies are under a duty to act compatibly with Convention rights under the Human Rights Act 1998. Privacy in Australia is not a general constitutional right; however, the objects of the Privacy Act make reference to Article 17 of the ICCPR and seek to protect privacy whilst also taking into account other competing interests (Privacy Act 1988 (Cth), s. 2A).

The United Kingdom Framework

The principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability are outlined in Article 5 of the UK GDPR. Article 6 requires that it must have a lawful basis and Article 9 explains that a special category data is restricted. Articles 12-15 give details and access rights including meaningful information regarding the logic of only automated decision making. Articles 16 and 17 - Rectification and Erasure. There is a right of objection in Article 21. Data protection by design and by default is required under article 25. Data protection impact assessment (DPIA) for likely high-risk processing required under Article 35. These provisions are relevant as AI can propagate errors, can draw inferences of sensitive characteristics and can give rise to systemic risks (ICO, 2023; Lynskey, 2015).

Article 22A defines a decision made on the basis of solely automated processing as a decision made without any meaningful human intervention and a significant decision as one which has a legal or otherwise significant effect. Article 22B limits ‘significant’ automated decisions that are made on the basis of special category data. These can only be used with explicit consent, or if they are required or authorised by law and a substantial public interest condition is met. The new lawful basis of recognised legitimate interests in Article 6(1)(ea) is also not an option for any ‘significant solely automated decision’ in accordance with Article 22B (4). Article 22C mandates safeguards

Online ISSN: 3006-8886
Print ISSN: 3006-8878

for each and every decision allowed: information about the decision and ability to make representations, obtain human intervention and challenge the decision. Regulations on meaningful human involvement, significant effects and safeguards (Data (Use and Access) Act 2025, s. 80). The shift from a general prohibition, subject to exceptions, to a general permission, subject to safeguards for ordinary personal data.

The Australian Framework

Australian law is not as concerned with making individual decisions. APP 1 mandates open and transparent governance of personal information and reasonable governance practices. APP 3 states that the collection of personal information must be reasonably necessary for the functions or activities of the organisation and in general, consent is required for the collection of sensitive information. APP 5 deals with notice of collection, APP 6 with use and disclosure for secondary purposes, APP 8 with cross-border disclosure, APP 10 with data quality and APP 11 with security and the destruction or de-identification of information. There are rights of access and correction provided in APPs 12 and 13. The rules apply to a wide range of inputs and outputs from AI, such as inferred personal information. At present, there is no general right at the decision level like Article 22C (OAIC, 2024a, 2026b).

APPs 1.7 to 1.9 will apply where an entity has organised for a computer program to make a decision or to do a thing which is substantially and directly related to making the decision, the decision could reasonably be expected to have a significant effect on the rights or interests of an individual and personal information is used. The privacy policy is then to specify the type of personal information used, the type of decisions made solely by the program and the type of decisions to which the program makes a substantial and direct contribution (Privacy and Other Legislation Amendment Act 2024 (Cth), sch.). 1, pt. 15; OAIC, 2026c). It need not notify an individual about a particular decision, give reasons or offer human reconsideration.

Developing the Contestable Accountability Framework

The framework draws on three sources: the data protection principles above, scholarship on explanation, contestability and accountability, and the record of institutional failure in automated public decision-making, especially Robodebt (Royal Commission into the Robodebt Scheme, 2023). It has three layers, all of which are connected. Ex ante legality includes lawful purpose, minimisation, security and data quality, and sensitive data safeguards, and prior risk assessment. Decisional due process involves providing prompt notice that a decision was made by automation, providing intelligible information on the principal considerations, an opportunity for representation and review by a person in real control. Ex post accountability involves auditable records, regulator access, independent assessment and effective orders and realistic remedies. These layers result in the seven criteria given in Table 1.

The framework is different from what has been done so far. Accountability is, according to Bovens (2007) a general forum-centred theory of accountability in which an actor has to explain itself to a forum that has the ability to question and impose consequences. The attention of Kroll et al. (2017) is on technical verifiability, Kaminski and Malgieri (2021) on multi-layered explanations

Online ISSN: 3006-8886
Print ISSN: 3006-8878

given by impact assessments, and Alfrink et al. (2023) on contestability as a design goal. There are three differences in the present framework. A legal test used with statutes when they are compared. It sees the seven elements as a chain, meaning that if there is a weak link at one point, it affects the rest of the chain, e.g. if an individual does not know that automation was used, a right to human review is not very useful. It also focuses on the possibility of the person affected to actually change an outcome. It does not require the sharing of source code, which is not always necessary or sufficient (Selbst & Powles, 2017; Wachter et al., 2018). It considers AI as a sociotechnical system (Selbst et al., 2019) and ties explanation to action (Gacutan & Selvadurai, 2020).

Critical Comparative Analysis

Scope of Personal Information and Lawful AI Processing

The UK GDPR has a wide definition of personal data and specifically includes profiling, so an inference can be personal data if it relates to an identifiable person. Information or opinion about an identified or reasonably identifiable person. In Privacy Commissioner v Telstra Corporation Ltd (2017), the Full Federal Court reiterated that the information must be ‘about' the individual, which can lead to disagreement on whether metadata and derived attributes constitute information about the individual (OAIC, 2017).

A functional approach is better when it comes to AI. A risk score is about a person determining their eligibility. The creation of inferred personal information is considered a collection by the OAIC, and thus is covered by APP 3 (OAIC, 2024a). A similar conclusion is reached in the UK, by means of the notions of processing and profiling. Developers should not put off privacy obligations by invoking the assessment machine output of a model.

There are varying rules on lawful processing. Controllers in the UK must have a lawful basis under Article 6 and for special category data a condition under Article 9. The DUAA adds recognised legitimate interests for certain purposes but, as said above, Article 22B (4) does not allow for the use of this basis for a serious automated decision made by a controller. Australia's reasonable necessity test is provided in APP 3 and limits on secondary use and disclosure in APP 6. Consent is a key issue for sensitive information, as outlined in APP 3.3, subject to statutory exceptions.

These principles are demonstrated in the Australian Clearview determination. The Commissioner determined in Commissioner Initiated Investigation into Clearview AI, Inc. (Privacy) (2021) that the practice of scraping images of faces from the Internet and creating templates of them violated APPs 1.2, 3.3, 3.5, 5 and 10.2. Even though the images were publicly accessible, this did not absolve them of the obligation to obtain consent and act fairly in collecting them. Also, in the guidance on generative AI the OAIC has confirmed that web scraping continues to be covered by the collection rules in the APP (OAIC, 2024b).

Proportionality is a dimension added to the UK. In R (Bridges) v Chief Constable of South Wales Police (2020), the Court of Appeal determined that the police use of live facial recognition was not lawful under Article 8, due to the rules allowing for too much discretion on who should be

Online ISSN: 3006-8886
Print ISSN: 3006-8878

added to a watchlist and the use of the technology. The court also ruled that the DPIA lacked and that the police failed to fulfil its obligations under the public sector equality duty. Bridges does not outlaw the practice of facial recognition per se. It demonstrates that the proper application of AI by public entities must be based on foreseeable rules, restricted discretion and proper risk assessment.

The actual impact of the differences is moderate. Either system can prevent blatantly illegal AI data collection. But the Australian "about" test is less clear-cut when it comes to data which is derived from other sources, which could hamper enforcement in close cases. A simpler rule for organisations to follow is provided by the UK bar preventing organisations from relying on recognised legitimate interests for solely automated significant decisions.

Automated Decisions, Explanation and Human Review

Prior to the DUAA, Article 22 was interpreted as a qualified right not to be subject to “purely automated important decisions”. Wachter et al. (2017) did not accept a broad right to explanation and Selbst and Powles (2017) suggested that the duty to provide meaningful information should be interpreted in the context of its purpose. Edwards and Veale (2017) continued that explanation must be accompanied by an effective remedy.

The DUAA modifies the starting point but maintains contestability. Article 22A poses the question of meaningful human involvement, rather than just human involvement. A person who routinely approves a machine's output without authority, time or information should not count. Where a significant decision is made purely automatically, Article 22C introduces safeguards to the decision made by the machine (Data (Use and Access) Act 2025, s. 80).

The weakness is that the UK liberalised the rules at the same time. For data that is not included in the special categories, the same stringent conditions are no longer in place, and the focus is shifted from prevention prior to deployment to challenge after deployment. That change can only be justified if the information provides for real challenge and the reviewer has the ability to alter the result. According to the ICO and Alan Turing Institute guidance, there are 6 different types of explanations: Rationale, Responsibility, Data, Fairness, Safety and performance and Impact (ICO & The Alan Turing Institute, 2020). Not required and being reviewed after the DUAA (ICO, 2026b).

APPs 1.7-1.9 are weaker in terms of the individual decision in Australia. They have a wide trigger, one way. It includes decision-support systems in which a program performs a task that is closely and directly linked to a decision, and without which a human decision would not otherwise be made (OAIC, 2026c). However, the duty is met through the privacy policy. The policy should outline the type of personal information and the type of decisions being made, but not provide details of any individual decision; the rule does not require any human reconsideration (OAIC, 2026a). The person will thus be aware that an organisation uses automation, but not necessarily whether or how this impacted their case.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

The practical impact is illustrated with a simple example. Imagine that a bank turns down a loan based on an automated credit model. In the UK the applicant is informed of the automated decision if it is a significant decision, the applicant can make representations and challenge the decision and the applicant may seek human intervention. The Privacy Act does not provide for a right to reasons or human review in Australia; the applicant may read the privacy policy and may make an APPs 12/13 access/correction request and complain to the OAIC. However, the safeguards in the UK do not apply where a human is meaningfully involved and Article 22C applies only to solely automated decisions. Such hybrid decisions are included in the Australian trigger, but only policy level information is provided. The UK thus affords more protection to a smaller range of decisions and vice-versa for Australia.

The Robodebt Royal Commission made a series of recommendations regarding a clear pathway to review, plain language information on automation, access to business rules and algorithms for independent expert review and audit, and a body to review and audit automated decision-making (Royal Commission into the Robodebt Scheme, 2023). These recommendations relate to the government but are applicable to high impact private decisions. The Privacy Act Review recommended the right to request meaningful information about the process of making substantially automated decisions and the Government accepted this (Attorney-General's Department, 2023a, 2023b). The Act 2024 introduced just the privacy policy aspect.

Other Australian controls do not close the gap but reduce it. In public settings, there may be a requirement for administrative law to provide reasons and for a privacy impact assessment (PIA) under the Privacy (Australian Government Agencies – Governance) APP Code 2017 for projects that have a high privacy risk. The Australian Federal Police (AFP) failed to conduct a PIA before using the Clearview tool and breached APP 1.2 and the Code in Commissioner Initiated Investigation into the Australian Federal Police (Privacy) (2021). This does not represent a general right to contest decisions but is enforceable risk assessment.

Both systems also have to determine the contents of an adequate explanation. No explanation is not the answer for a complex model. A person who wants to challenge a decision must have the key factors that influenced the decision, the data that the decision was based on which may be inaccurate, the rule or threshold that was used and the pathway for review. Counterfactual explanations can reveal what has to change to get a different result, without revealing all the parameters of the model (Wachter et al., 2018). However, they are not required to disclose illegal criteria, improper uses or even biased information. Individual reasons and auditability should thus complement each other.

Impact Assessment and Data Governance

Accountability is most effective when it prevents harm from happening. UK controllers should ensure compliance (Article 5(2)), implement data protection by design and by default (Article 25) and carry out a DPIA for likely high-risk processing (Article 35). ICO guidance takes a risk-based approach to AI (ICO, 2023). Data sources, necessity, sensitive inferences, accuracy, security, representativeness, human oversight, explainability and routes for challenge are all factors to consider in an AI DPIA. An impact assessment can also help to explain (Kaminski & Malgieri,

Online ISSN: 3006-8886
Print ISSN: 3006-8878

2021). Bridges demonstrates that a DPIA cannot and should not be used to justify a decision that has already been made; rather, a DPIA should inform the deployment decision.

Governance is more based on general obligations and directions in Australia. APP 1.2 calls for reasonable practices, procedures and systems to ensure compliance. Agencies are required to undertake PIAs for projects with a high level of privacy under the Code and PIAs and privacy by design are encouraged for AI (OAIC 2024a, 2024b). There is no general obligation for all APP entities, however, to make an assessment prior to processing if the processing is considered to be high risk. The Privacy Act Review recommended that a duty be put in place for high privacy risk activities to ensure that a Privacy Impact Assessment (PIA) is completed (Attorney-General's Department, 2023a). This was agreed in principle by the Government (Attorney-General's Department, 2023b) but has yet to be legislated.

An express assessment duty provides a trigger, a record and a point for regulatory intervention prior to deployment, while a general "reasonable steps" duty may only be specified by a complaint or breach. The Federal Court imposed civil penalties of $5.8 million in Australian Information Commissioner v Australian Clinical Labs Ltd (No 2) (2025) for security failures and failure to handle and notify a data breach. These were the first civil penalties imposed under the Privacy Act. Although this case is not about AI, it demonstrates that there are operational privacy responsibilities that can be daunting.

The UK continues to rely heavily on the judgement of the controllers and interpretation of the regulators. The ICO had issued notice predates the 2023 Tribunal decision regarding Experian's processing of information for marketing purposes, and the level of transparency. In 2023 the First-tier Tribunal upheld Experian's appeal and issued a more limited notice. In April 2024 the ICO's appeal was unsuccessful and the Upper Tribunal provided guidance on Article 5(1)(a) and Article 14. The case illustrates how general transparency requirements are interpreted and applied on a case-by-case basis and are in some cases unpredictable, which is a clear indication of the need for clear minimum standards in the case of significant automated decisions.

A UK DPIA provides a document for the regulator to analyse before it can cause harm, and an Australian private organisation can use high-risk AI without any formal assessments. The introduction of a new duty should be limited to high risk processing to manage compliance costs.

Biometric Surveillance, Scraping and Territorial Reach

Biometric AI is a test on the safeguard of sensitive data and the territorial scope of the law. As mentioned, it is the Clearview determination in Australia, which concluded that facial scraping and biometric templates violated a number of APPs. The Commissioner ordered Clearview to stop collecting the images and templates and to destroy those already collected. Consent and fairness were paramount in the decision as biometric information used for automated identification is sensitive information.

Jurisdiction has been the issue in the UK with the Clearview litigation. In 2022, the ICO issued an enforcement notice and a fine against Clearview, which challenged the ICO's jurisdiction on the

Online ISSN: 3006-8886
Print ISSN: 3006-8878

grounds that its clients were foreign law enforcement agencies. The Upper Tribunal agreed with the ICO's appeal in Information Commissioner's Office v Clearview AI Inc (Privacy International intervening) (2025). It concluded that it was processing the behaviour of those in the UK and that the exclusion of processing by foreign states did not extend to Clearview's own commercial processing and it remanded the case (ICO, 2025). Clearview was granted permission to file an appeal. The ICO had issued a Statement stating that the appeal was 'under consideration' in February 2026 (ICO, 2026c) and the Court of Appeal heard the appeal in October 2026 (Howse, 2026). The result is still pending.

Australia has been testing out the section 5B of the Privacy Act. In Facebook Inc v Australian Information Commissioner (2022), the Full Federal Court determined a prima facie case had been established that Facebook Inc conducted business in Australia, for which service was permitted outside of Australia. The High Court granted special leave but withdrew its special leave in March 2023 because of changes in the Federal Court Rules which no longer left the appeal as one of public importance (OAIC, 2023). The common thread is that an organisation's data practices need to have a sufficient tie with residents to not put it out of reach of privacy law because of its foreign location.

However, slow enforcement and technical opacity can't be addressed by territorial rules. AI systems evolve rapidly and the UK Clearview proceedings were ongoing as of late 2026 without any resolution. Thus, alongside the jurisdictional rules, cross-border cooperation, procurement control, corrective orders and the regulator's access to technical records are also key.

Remedies, Enforcement and Practical Effectiveness

In the UK, there are enforcement notices and monetary penalties issued by ICO and court remedies and compensation under the Data Protection Act 2018. There are limits to private enforcement. The Supreme Court in Lloyd v Google LLC (2021), a claim under the Data Protection Act 1998 held that compensation could not be awarded under section 13 unless there was material damage or distress from the breach, that a lack of control was insufficient to establish compensation and that the claim could not be brought as a representative action for uniform damages without particular assessment. Lloyd's relevance to the economics of mass privacy claims are still on point.

In Vidal-Hall v Google Inc (2015) the Court of Appeal found that misuse of private information could be a tort and that distress could be a basis for a claim for compensation under section 13 of the 1998 Act, even if there were no financial loss. In the UK, there are consequently a number of remedial pathways which have thresholds. Regulator action is particularly significant as AI harms tend to be small and ubiquitous.

Schedule 2 of the Privacy Act which came into force on 10 June 2025 establishes a cause of action for serious invasion of privacy by intrusion upon seclusion or misuse of information. There must be a reasonable expectation of privacy, intentional or reckless invasion and seriousness, and a public interest in privacy must prevail. The tort is actionable without proof of damage, it gives rise to defences/exemptions and is subject to damages and injunctions (OAIC, 2025; Privacy Act 1988 (Cth), sch. 2).

Online ISSN: 3006-8886
Print ISSN: 3006-8878

The tort only partially tackles harmful automated decisions, which can be caused by negligence, wrong inferences or simply by automated processing which is opaque but is nonetheless authorised by law. Many of these cases will fall short of the intention and seriousness thresholds, and the tort is not administered by the OAIC (OAIC, 2025). The need for direct statutory rights of challenge to decisions remains.

Controlling ability is at the core. Australian courts will now be able to impose significant penalties, while the ICO has significant enforcement powers. However, deterrence is about speed and corrective ability, not about maximum penalties. Orders to halt processing, to delete illegally acquired data, to enhance governance and to be subject to audit are often the most helpful for AI. Table 2 summarises the legal architecture.

Table 2: Comparative Architecture of AI-Related Data Protection in the United Kingdom and Australia

Issue	United Kingdom	Australia	Comparative implication
Core framework	UK GDPR; Data Protection Act 2018; DUAA 2025	Privacy Act 1988 (Cth); APPs; Privacy and Other Legislation Amendment Act 2024 (Cth)	Both are general privacy regimes, but their rules on automated decisions differ.
AI data collection	Article 5 principles; Article 6 lawful basis; Article 9 special category data	APP 3 necessity; consent usually required for sensitive information; APP 6 secondary use	Both can limit data collection and inference.
Automated decisions	Articles 22A–22D (from 5 February 2026): general permission with Article 22C safeguards; Article 22B limits for special category data and recognised legitimate interests	APPs 1.7–1.9 (from 10 December 2026): privacy policy must describe kinds of personal information and kinds of decisions	UK safeguards attach to individual decisions; Australian duty operates at policy level.
Human review	Article 22C right to obtain human intervention for solely automated significant decisions	No general equivalent in the Privacy Act	Australia has a core contestability gap.
Impact assessment	Article 35 DPIA for likely high-risk processing	PIA duty for agencies under the 2017 APP Code; no general private sector duty	UK has stronger rules before deployment.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Biometrics	Special category data; Bridges and Clearview litigation	Sensitive information; Clearview and AFP determinations	Both treat biometric AI as high risk.
Private remedies	DPA 2018 compensation; misuse of private information tort	Statutory tort in Schedule 2 (from 10 June 2025)	Australian remedies have expanded but have high thresholds.
Regulatory enforcement	ICO enforcement notices and monetary penalties	OAIC determinations; civil penalties ordered by the Federal Court	Effectiveness depends on speed, auditability and resources.

Source: Created by the authors from the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, Privacy Act 1988 (Cth), Privacy and Other Legislation Amendment Act 2024 (Cth) and the cited regulatory materials.

Table 3: Qualitative Accountability Profile of the United Kingdom and Australia

Criterion	United Kingdom	Australia
C1 Lawful and limited data use	Provided. Articles 5, 6 and 9 apply; Article 22B adds limits for special category data and recognised legitimate interests.	Provided. APPs 3 and 6 apply, with consent for sensitive information; the "about" test creates some uncertainty for derived data.
C2 Prior risk assessment	Provided. Article 35 requires a DPIA for likely high-risk processing.	Partly provided. Agencies must conduct PIAs under the APP Code; private entities rely on APP 1.2 and guidance.
C3 Decision-level notice	Partly provided. Article 22C applies only to solely automated significant decisions.	Not provided. APPs 1.7–1.9 require only a general privacy policy description.
C4 Intelligible reasons	Partly provided. Information duties exist, but there is no clear general right to personalised main reasons.	Not provided. The agreed right to request meaningful information has not been enacted.
C5 Effective human review	Partly provided. A right to human intervention exists for solely automated decisions; the meaning of meaningful involvement awaits regulations.	Not provided in the Privacy Act. Administrative review may apply in some public settings.
C6 Auditability and oversight	Partly provided. Accountability and DPIA records exist; there is no specific duty to log automated decisions.	Partly provided. APP 1.2 governance duties and OAIC powers exist; there is no specific decision record duty.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

C7 Accessible remedies	Partly provided. ICO powers and compensation exist, but thresholds and slow litigation limit them.	Partly provided. Civil penalties and the statutory tort exist, but the tort has high thresholds.

Source: Created by the authors from the analysis in Section 5, applying the categories defined in Section 3.3. The assessments are qualitative legal judgements, not measurements.

Digital Governance and Institutional Coherence

In the UK, there is no specific cross-sector AI law; sector-specific laws and regulators still have a prominent role to play, and data protection is still horizontal (Rough, 2026). In December 2025, Australia's National AI Plan (Department of Industry, Science and Resources, 2025) was also launched, which is built on existing laws and regulators with the new AI Safety Institute. In 2024, the Government proposed implementing mandatory guardrails for high-risk AI but did not take action on this proposal (Department of Industry, Science and Resources, 2024).

This adds weight to the privacy law, as one of the few cross-sector laws, which can follow the personal data from its collection to the decision. Bias can be considered an issue under equality law, misleading conduct under consumer law, unlawful public decision under administrative law and failure to take safety precautions under sector regulators. Coordinating itself is the task.

That coordination is facilitated by Contestable Accountability. Privacy law should result in a minimum set of facts that can be used by other regimes: what was the material information that was personal; what was the role of automation; what reasons can be offered; what human review took place; what records exist. This isn't a complete AI code for data protection. It provides data protection as a gateway for specialised legal controls.

Guidance provided by the regulators should not be seen as law. Its strength is based on the statute which it interprets, and on being accepted by courts and tribunals. The most effective is the one that allows flexibility and yet has minimum standards of law to guide decisions of high impact.

Practical Challenges

Four practical issues have to be addressed in the reform. The first one is regulatory capacity. AI audits are a technical process that takes time and money, and the lengthy Clearview and Experian litigation demonstrates that contested enforcement can be a lengthy process that takes years. Stronger rights on paper without resources are ineffective in changing very much.

The second is the cost of compliance. Evaluations, documentation, explanations and trained evaluators are appropriate for high impact decisions but may be overkill for small organisations and low impact systems. The responsibilities should thus reflect the impact of the decision, the impact of automation and the sensitivity of the data.

The third is transparency's end. Explanation of some models is complex, simplified explanations can be misleading, and organisations are concerned about trade secrets and gaming. This can be done by providing layered explanations: general for the public, specifically for individuals and technical for regulators (Kaminski & Malgieri, 2021).

Online ISSN: 3006-8886
Print ISSN: 3006-8878

The fourth is a meaningful human supervision. Reviewers may go with the automated outputs due to automation bias, workload and pressure. Green (2022) suggests that the need for human oversight can lead to a false sense of security and Robodebt demonstrates how human involvement can break down when officials are unable to change the automated outcome (Royal Commission into the Robodebt Scheme, 2023). Review should be assessed based on if the reviewers have authority, information, time, competence and if they make a difference.

Findings and Original Contribution

Each of the research questions is addressed in this section.

RQ1: Both systems offer a relatively good overall framework for the collection, inference and usage of personal data in AI systems. The UK have more specific guidance on lawful basis – including a restriction on using recognised legitimate interests for important decisions made by automated processes – and a general DPIA obligation. The necessity test in APP 3 and the consent for sensitive information, however, leave less scope for uncertainty than does the 'about' test and the lack of a general PIA duty. As evidenced in the Clearview, AFP and Bridges cases, both systems are high-risk biometric AI.

As for RQ2, the central difference is not between a strict UK and a flexible Australia. It is a contrast between protected permission and fragmentation with a focus on transparency. The UK allows for more decisions to be made using ordinary personal data that are ‘solely automated' than the previous Article 22, but Article 22C applies safeguards to each of these decisions. But there is no clear general right to personalised main reasons in the UK and the issue of a right to explanation is still pertinent (Gacutan & Selvadurai, 2020; Wachter et al., 2017). Australia is more general, in that they have a much wider definition of what constitutes a trigger, and thus a broader obligation to report on the privacy policy. It doesn't provide any individual with the notice, reasons or human review.

In response to RQ3, the enforcement has been strengthened in both countries. Australia has civil penalties for the first time under the Privacy Act and a new statutory tort, and the UK has wide enforcement powers and a number of remedial options. But slow litigation, limits on compensation and the tort, and limited regulatory resources limit the effectiveness of this approach. It is not the highest possible penalty that is the most important factor in effectiveness; it is the speed of action, and the availability of technical records and means to require corrective action.

As for the main research question, neither of the systems make significant decisions contestable using AI. Both offer a portion of the accountability chain, with the missing pieces varying. The UK has a strong focus on processes at decision level, and prior assessment, but has cut back on the scope of automation and its safeguards only cover decisions that are made entirely by automated means. Australia has strong institutional lessons, but no decision level rights and a broad transparency trigger, and a growing number of remedies. There is much to be learnt from each other, but neither should the two jurisdictions attempt to copy the other regime in its entirety.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

The contestable accountability framework is summarised in Table 4. Table 4 shows how each element can be related to its legal basis, how it is missing in each jurisdiction and a practical way to implement it. The framework clarifies the importance of not relying on transparency alone – a privacy policy that tells them that the AI is being used does not give a person the ability to alter the outcome; human involvement is ineffective if the human has no authority or information. It also does not involve two extremes. It does not have to be technically explained in detail for every system, and it does not only apply when no human is involved, otherwise nominal sign-offs would not have to be explained. The level of duties should be commensurate with risk.

Table 4: The Contestable Accountability Framework: Legal Basis, Gaps and Implementation

Element	Main legal basis (UK; Australia)	Main gap identified	Practical implementation
C1 Lawful data use	Articles 5, 6, 9, 22B; APPs 3 and 6	Australia: uncertainty over derived data	Treat inferences used in decisions as personal information.
C2 Risk assessment	Article 35; APP 1.2 and the 2017 APP Code	Australia: no general private sector duty	Require assessment of high-risk processing before deployment and after material change.
C3 Notice	Article 22C; APPs 1.7–1.9	UK: solely automated decisions only. Australia: policy level only	Give individual notice when automation materially affects a significant decision.
C4 Reasons	Articles 13–15 and 22C; no general Australian equivalent	Both: no clear right to personalised main reasons	Set minimum content: main factors, data relied on, how to correct errors, how to contest.
C5 Human review	Articles 22A and 22C; no general Australian equivalent	UK: scope of meaningful involvement unclear. Australia: no right	Require reviewer authority, information, time and competence; record overrides.
C6 Auditability	Articles 5(2), 30 and 35; APP 1.2	Both: no specific decision records	Keep proportionate decision records; allow regulators to order independent evaluation.
C7 Remedies	ICO powers and DPA 2018 compensation; civil penalties and Schedule 2 tort	Both: slow enforcement and high thresholds	Use corrective orders, fund regulator expertise and support regulator cooperation.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Source: Created by the authors. The framework synthesises UK GDPR Articles 5, 13–15, 22A–22D, 25, 30 and 35; APPs 1, 3, 5, 6 and 10–13; the 2024 Australian automated decision reforms; and the cited case law and regulatory materials.

The framework also offers a test for reform: a reform should strengthen at least one link in the accountability chain without weakening another. Because this test does not depend on a particular technology, it can remain useful as AI changes.

Recommendations

Each recommendation responds to a specific finding. First, in response to the UK gap under RQ2, regulations under Article 22D should establish the minimum content of the information to be provided in a decision: the main factors, the categories of personal data used for the decision, information which would enable the person to identify and correct significant errors and a clear path to contest. This does not mean that the source code needs to be disclosed. ICO guidance should differentiate between public explanations and individual reasons and regulators technical documentation.

Secondly, under RQ2, there should be a possibility for human reviewers to alter the decision, they have to be provided with relevant information and competence, and they should not be directed to accept the automated result. Controllers should keep track of any override to enable ICO to test if it is review or not.

Third, in response to the Australian gap under RQ2, and on the basis of the agreed Privacy Act Review proposal (Attorney-General's Department, 2023a, 2023b), Australia should provide individuals with the right to be notified when an automated processing activity is likely to have a significant impact on them and is used to make a decision about them. On the right side should be included the main reasons, representations, correction of relevant data and meaningful human reconsideration. The “substantially and directly related” trigger should remain, as automated means can influence the decisions even if a human is ultimately responsible for signing it (OAIC, 2026a).

Fourth, in response to the Australian gap under RQ1, Australia should implement a general obligation to assess high privacy risk processing, but to exempt low privacy risk processing. Evaluation should happen pre-deployment, must be updated as models, uses or data change, and should cover data sources, need, sensitive inference, accuracy, security, explainability, human oversight and unequal impacts. The AFP determination shows such duties can be enforced.

Fifth, both jurisdictions should mandate proportionate documentation to enable the reconstruction of significant automated decisions, such as system versions, data categories, key factors, human intervention and corrections, in response to the enforcement gap under RQ3. Regulators need to be able to mandate independent technical assessment if there is systemic risk. Auditability provides the expert review, ensuring legitimate confidentiality.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Sixth, both jurisdictions need to invest in regulators' capacity and enhance collaboration between the privacy, equality, consumer and sector regulators, to address the capacity and coordination challenges identified in Sections 5.6 and 6. Data protection does not necessarily need to be the magic bullet for all AI unfairness but can serve as the procedural backbone for other legal claims.

Conclusion

The governance of personal data can no longer be separated from the governance of decisions with the help of AI. The DUAA allows for significant automated decisions to be taken on ordinary personal data, but maintains protections of information, representations, contestation and human intervention. From December 2026, the Australia privacy policies will need to explain some automated decisions but there is no general right to explanation or human intervention. The additions of a remedy with the statutory tort in 2025 are welcome but insufficient on their own to give people the right to reasons or to be heard.

Transparency and simply formal human involvement are not sufficient. The chain of accountability must include lawful data gathering, a risk assessment, an explanation of the decision, an empowered review, audit and remedy. The contestable accountability framework as outlined in the chain gives a framework for the UK's regulations under Article 22D and the next steps in the Australian reform process. It is not about prohibiting automated decision making but to make sure that where it is used, those concerned can understand, challenge and rectify the use of their personal data for major decisions. This study is doctrinal and does not measure compliance in practice. It reflects the law as it stands ahead of the coming into force of APPs 1.7 to 1.9 and as it is prior to a potential decision in the UK Clearview appeal. Future research should focus on the use of these rules by the regulators and organisations in particular with regard to the quality of the explanations and human review.

References

1. Alfrink, K., Keller, I., Kortuem, G., & Doorn, N. (2023). Contestable AI by design: Towards a framework. Minds and Machines, 33(4), 613–639. https://doi.org/10.1007/s11023-022-09611-z
2. Attorney-General's Department. (2023a). Privacy Act review report. Australian Government. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
3. Attorney-General's Department. (2023b). Government response to the Privacy Act review report. Australian Government. https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report
4. Australian Human Rights Commission. (2021). Human rights and technology: Final report. https://humanrights.gov.au/resource-hub/technology-and-human-rights/final-report-human-rights-and-technology
5. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Online ISSN: 3006-8886
Print ISSN: 3006-8878

6. Department for Science, Innovation and Technology. (2025). Data (Use and Access) Act 2025: Explanatory notes. UK Government. https://www.legislation.gov.uk/ukpga/2025/18/notes/contents
7. Department of Industry, Science and Resources. (2024). Introducing mandatory guardrails for AI in high-risk settings: Proposals paper. Australian Government. https://consult.industry.gov.au/ai-mandatory-guardrails
8. Department of Industry, Science and Resources. (2025). National AI plan. Australian Government. https://www.industry.gov.au/publications/national-ai-plan
9. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16(1), 18–84.
10. Gacutan, J., & Selvadurai, N. (2020). A statutory right to explanation for decisions generated using artificial intelligence. International Journal of Law and Information Technology, 28(3), 193–216. https://doi.org/10.1093/ijlit/eaaa016
11. Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. Computer Law & Security Review, 45, Article 105681. https://doi.org/10.1016/j.clsr.2022.105681
12. Henman, P. W. F. (2025). Robodebt cultures and useful idiots: Why Robodebt was not a techno-failure. Australian Journal of Social Issues, 60(1), 4–20. https://doi.org/10.1002/ajs4.383
13. Howse, I. (2026, October 19). Clearview AI denies behavioral monitoring in UK privacy fine appeal. MLex. https://www.mlex.com/mlex/articles/2539639/clearview-ai-denies-behavioral-monitoring-in-uk-privacy-fine-appeal
14. Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70
15. Information Commissioner's Office. (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
16. Information Commissioner's Office. (2025). UK Upper Tribunal hands down judgment on Clearview AI Inc. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/10/uk-upper-tribunal-hands-down-judgment-on-clearview-ai-inc/
17. Information Commissioner's Office. (2026a). The Data (Use and Access) Act 2025: What does it mean for organisations? https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/
18. Information Commissioner's Office. (2026b). Explaining decisions made with AI. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/
19. Information Commissioner's Office. (2026c). John Edwards speaks at IAPP UK Intensive 2026. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/john-edwards-speaks-at-iapp-uk-intensive-2026/
20. Information Commissioner's Office, & The Alan Turing Institute. (2020). Explaining decisions made with AI. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/

Online ISSN: 3006-8886
Print ISSN: 3006-8878

21. Kaminski, M. E., & Malgieri, G. (2021). Algorithmic impact assessments under the GDPR: Producing multi-layered explanations. International Data Privacy Law, 11(2), 125–144. https://doi.org/10.1093/idpl/ipaa020
22. Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705. https://www.jstor.org/stable/26600576
23. Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198718239.001.0001
24. Office of the Australian Information Commissioner. (2017). What is personal information? https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information
25. Office of the Australian Information Commissioner. (2023, March 7). High Court clears way for OAIC case against Facebook to proceed [Media release]. https://www.oaic.gov.au/news/media-centre/high-court-clears-way-for-oaic-case-against-facebook-to-proceed
26. Office of the Australian Information Commissioner. (2024a). Guidance on privacy and the use of commercially available AI products. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products
27. Office of the Australian Information Commissioner. (2024b). Guidance on privacy and developing and training generative AI models. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models
28. Office of the Australian Information Commissioner. (2025). Statutory tort for serious invasions of privacy. https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy
29. Office of the Australian Information Commissioner. (2026a). Consultation on guidance for transparency in automated decision making. https://www.oaic.gov.au/engage-with-us/consultations/consultation-on-guidance-for-transparency-in-automated-decision-making
30. Office of the Australian Information Commissioner. (2026b). Australian Privacy Principles guidelines. https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines
31. Office of the Australian Information Commissioner. (2026c). New resources on transparency for use of AI and automated decision making [Media release]. https://www.oaic.gov.au/news/media-centre/new-resources-on-transparency-for-use-of-ai-and-automated-decision-making
32. Rough, E. (2026). AI regulation in the UK. House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cbp-10003/
33. Royal Commission into the Robodebt Scheme. (2023). Report of the Royal Commission into the Robodebt Scheme. https://robodebt.royalcommission.gov.au/publications/report
34. Selbst, A. D., boyd, d., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 59–68). Association for Computing Machinery. https://doi.org/10.1145/3287560.3287598

Online ISSN: 3006-8886
Print ISSN: 3006-8878

35. Selbst, A. D., & Powles, J. (2017). Meaningful information and the right to explanation. International Data Privacy Law, 7(4), 233–242. https://doi.org/10.1093/idpl/ipx022
36. Van Hoecke, M. (2015). Methodology of comparative legal research. Law and Method. https://doi.org/10.5553/REM/.000010
37. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
38. Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841–887.
39. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505–523. https://doi.org/10.1111/rego.12158
40. Zweigert, K., & Kötz, H. (1998). An introduction to comparative law (T. Weir, Trans.; 3rd ed.). Oxford University Press.
41. **Cases**
42. Australian Information Commissioner v Australian Clinical Labs Ltd (No 2) [2025] FCA 1224.
43. Commissioner Initiated Investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54.
44. Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74.
45. Facebook Inc v Australian Information Commissioner [2022] FCAFC 9; (2022) 289 FCR 217.
46. Information Commissioner v Experian Ltd [2024] UKUT 105 (AAC).
47. Information Commissioner's Office v Clearview AI Inc (Privacy International intervening) [2025] UKUT 319 (AAC).
48. Lloyd v Google LLC [2021] UKSC 50; [2022] AC 1217.
49. Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4; (2017) 249 FCR 24.
50. R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058; [2020] 1 WLR 5037.
51. Vidal-Hall v Google Inc [2015] EWCA Civ 311; [2016] QB 1003.
52. **Legislation and Treaties**
53. Data (Use and Access) Act 2025, c. 18 (UK). https://www.legislation.gov.uk/ukpga/2025/18/contents
54. Data Protection Act 1998, c. 29 (UK).
55. Data Protection Act 2018, c. 12 (UK). https://www.legislation.gov.uk/ukpga/2018/12/contents
56. European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, November 4, 1950, ETS No. 5.
57. Human Rights Act 1998, c. 42 (UK).
58. International Covenant on Civil and Political Rights, art. 17, December 16, 1966, 999 U.N.T.S. 171.
59. Privacy Act 1988 (Cth) (Austl.). https://www.legislation.gov.au/C2004A03712/latest/text
60. Privacy and Other Legislation Amendment Act 2024 (Cth) No. 128, 2024 (Austl.). https://www.legislation.gov.au/C2024A00128/latest/text
61. Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth) (Austl.).

Online ISSN: 3006-8886
Print ISSN: 3006-8878

62. UK General Data Protection Regulation, Regulation (EU) 2016/679 as retained and amended in United Kingdom law.