Information, Communication & Society

ISSN: 1369-118X (Print) 1468-4462 (Online) Journal homepage: www.tandfonline.com/journals/rics20

Typology of transparency as best practice: evidence from facial recognition technologies in Australia

Ausma Bernot, Rakibul Hasan, Milind Tiwari, Peita L. Richards & Brendan Walker-Munro

To cite this article: Ausma Bernot, Rakibul Hasan, Milind Tiwari, Peita L. Richards & Brendan Walker-Munro (08 Jul 2026): Typology of transparency as best practice: evidence from facial recognition technologies in Australia, Information, Communication & Society, DOI: 10.1080/1369118X.2026.2699253

To link to this article: https://doi.org/10.1080/1369118X.2026.2699253

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 08 Jul 2026.

Submit your article to this journal

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at https://www.tandfonline.com/action/journalInformation?journalCode=rics20

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2026.2699253

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Typology of transparency as best practice: evidence from facial recognition technologies in Australia

Ausma Bernot[a], Rakibul Hasan[b], Milind Tiwari[c,d], Peita L. Richards[e] and Brendan Walker-Munro[f]

[a]School of Criminology and Criminal Justice, Griffith University, Gold Coast, Australia; [b]International Business, University of Vaasa, Vaasa, Finland; [c]Australian Graduate School of Policing and Security Studies, Charles Sturt University, Canberra, Australia; [d]Centre for Banking Law, Faculty of Law, University of Johannesburg, Johannesburg, South Africa; [e]Centre for Law and Justice, Charles Sturt University, Canberra, Australia; [f]Faculty of Business, Law & the Arts, Southern Cross University, Gold Coast, Australia

ABSTRACT

Facial recognition technologies (FRTs) are commonly used in Australia in an under-regulated environment. Only two regulatory mechanisms currently direct FRT use – industry self-regulation and Australia's privacy laws. Currently, best practices for FRT development and adoption are a key governance mechanism, including the recent guide to FRT privacy risks evaluation published by the Office of the Australian Information Commissioner in 2024. Transparency is lauded as one of the key principles for implementation, yet it can be an elusive best practice to operationalize. Transparency spans everything from technical design decisions and data governance to real-world applications, user communication, and regulatory compliance. Thus, our research critically considers the concept of transparency in FRT governance by asking: *What does transparency as best practice mean in the development and implementation of facial recognition systems?* This study sought to map multi-stakeholder viewpoints through problem-centered interviews ($n = 30$) with expert technical, policy, and academic stakeholders making and informing FRT policy in Australia. Based on their responses, we develop a typology of what transparency means in the context of operationalizing algorithmic surveillance technology governance, specifically FRTs. Our findings adopt a socio-technical perspective and identify five distinct modes of transparency in FRTs, including *technical*, *functional*, *procedural*, *public* and *contextual transparency*.

ARTICLE HISTORY
Received 7 November 2024
Accepted 30 June 2026

KEYWORDS
facial recognition technologies; best practice; transparency; technology governance; industry self-regulation; public deliberation

1. Introduction

Facial Recognition Technologies (FRTs) are increasingly used across Australia's private and government sectors, including in security, retail, entertainment, healthcare, and public-private service partnerships. Despite widespread adoption, regulation remains

CONTACT Ausma Bernot a.bernot@griffith.edu.au School of Criminology and Criminal Justice Griffith University, Gold Coast Campus Building G6, Room 3.12 Parklands Drive Southport QLD 4215 Australia

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

limited. In 2021, the Australian Human Rights Commission, led by Edward Santow, recommended a legal moratorium on FRTs until appropriate regulatory frameworks were in place (Farthing et al., 2021). A Model Law was proposed in 2022 to govern high-risk FRT uses (Davis et al., 2022), but it has not been implemented. Currently, FRT applications fall under Australia's narrow privacy legislation and voluntary best practice codes. High-level principles alone cannot guarantee the ethical use of algorithmic technologies and may obscure deeper political and normative disagreements, making it essential to critically evaluate both their strengths and limitations (Mittelstadt, 2019).

FRT applications can be categorized into two main types (Matulionyte, 2024): *authentication* (or *verification*) using one-to-one (1-1) matching that involves recognizing an individual's face for tasks such as phone lock verification and *identification* using one-to-many (1-N) matching that searches a facial image against a database. Identification can be done in two ways: *ex-post* and in *real-time*. Ex-post identification occurs when a person's picture, taken from a CCTV camera or a photograph, is matched post-factum against the database. Real-time identification occurs when the identity of a natural person is determined immediately after being captured by the camera, typically installed in public spaces. Categorization is used to generate insights into the particularities of an individual, such as race, sex, and ethnicity, and segmentations by recognizing human emotions like anger, fear, and pain. While one-to-one authentication poses a relatively lower risk, deploying FRTs in public spaces for live identification is considered an unacceptable risk and banned in many jurisdictions globally (European Commission, 2024).

Under-regulation of FRTs, especially in one-to-many applications where a person's face is compared against a database, creates the potential for serious social harms. These harms can range from relatively minor incidents, such as incorrect denial of entry to a casino, to more severe consequences, including identity theft (Salko et al., 2024), wrongful stop-and-frisk incidents (Carlo, 2020), wrongful arrests (Hill, 2023), and even wrongful criminal convictions (Moy, 2021), disproportionately impacting people of color (Man, 2021; Raposo, 2024). With the growing adoption of AI technologies, secondary harms can also emerge through the misuse of facial data, such as the production of deepfakes (Firc et al., 2023), stalking (Harwell, 2021), and other forms of harassment and exploitation (Vladimirova, 2024). Once facial data is widely shared, it is nearly impossible to contain it again.

To prevent harmful applications, transparency and accountability have been identified as key principles by both the UN Special Rapporteur on Freedom of Opinion and Expression in 2014 and Australia's Parliamentary Joint Committee on Intelligence and Security in 2019 (Fletcher, 2023). Since 2024 and in response to privacy complaints, the Office of the Australian Information Commissioner has promoted best practice principles including necessity and proportionality, consent and transparency, accuracy and bias mitigation, and governance with ongoing assurance. FRT providers have since adopted the language of transparency in their public-facing materials (see, for example, Nirovision, n.d.).

Transparency, however, can be an elusive best practice to operationalize, as it spans everything from technical design decisions and data governance to real-world applications, user communication, and regulatory compliance. Intentional vagueness about what transparency means in algorithmic decision-making can allow for it to slip into becoming an 'ambiguous normative concept' (Koivisto, 2021). Thus, our research critically considers the concept of transparency as best practice for FRTs by asking: *What does transparency as best practice mean in the development and implementation of facial recognition systems?*

Based on semi-structured interviews with 30 expert stakeholders, including technology industry, policy, and academic professionals involved in shaping FRT policy in Australia, the research offers a grounded account of how transparency is understood and enacted. The findings show that the concept of transparency is frequently misused in the Australian context by both public and private actors to justify the use of FRTs. By critically mapping a typology of transparency as best practice, this study identifies what is required to meaningfully operationalize transparency in algorithmic technologies and contributes to the growing literature on FRT governance.

The article is structured as follows: a review of the literature, an outline of the research design and methods, presentation of the findings, a discussion introducing the transparency typology, and a concluding section.

2. Literature review

2.1. A socio-technical view of governing algorithmic surveillance systems

Facial recognition constitutes a variety of heterogeneous technologies. FRTs are part of computer vision that use AI-based algorithms to recognize and learn from patterns in digital images, particularly facial properties (Andrejevic & Selwyn, 2022). FRTs must also be understood as socio-technical algorithmic systems, the perceived fairness of which is deeply shaped by the social contexts in which they are deployed (Dolata et al., 2022). FRTs can be embedded within software and hardware – most commonly video surveillance cameras for real-time monitoring and recognition – or applied to existing video footage and photographs after image or video capture.

The socio-technical viewpoint emphasizes technical solutions, data, and models, as well as the interdependence between social context and technological capabilities (Dolata et al., 2022). From this socio-technical perspective, facial data, the foundation of FRT, connects social context and technological capability. These data are never neutral or disembodied but are best understood as 'digital data from persons' (Wong et al., 2025). For example, FRTs can be used to construct detailed profiles of individuals, including their political beliefs, movements, lifestyles, and consumption patterns, especially when combined with other biometric and data sources (Smith & Miller, 2022). FRT applications must therefore also embody ethical principles, ensure privacy, enhance fairness and obey local informal institutions (e.g., culture, value judgments, norms) throughout the systems' lifecycle. Therefore, *any deployment of FRTs without balancing both – the technical and the social – is problematic*. There are two main schools of thought for the governance of FRTs.

Critical research into FRT governance underscores the arguments that relate to epistemic injustices in FRT development and adoption (Andrejevic & Selwyn, 2022; Introna & Wood, 2004; Yeung, 2017). The scholars provide three important and connected assumptions. First, algorithmic systems, such as FRTs, are not neutral technical tools and have inherited biases that do affect human behavior and have an impact on human rights. Second, algorithmic systems must be understood at the intersection of commercial and political interests, which cannot be detached from surveillance capitalism and control. Finally, transparency in algorithmic systems, including FRTs, is critical, but not sufficient to ensure accountability in automated governance.

Mere disclosure and algorithmic explainability do not address deeper concerns about power structures and accountability. Indeed, emphasizing procedural transparency can lead to 'transparency washing,' where openness distracts from deeper issues like power concentration, major policies, and tech giants' actions (Zalnieriute, 2021). For example, misidentification of individuals from racial, gender, and ethnic minorities has repeatedly demonstrated the potential for human rights violations, particularly in relation to non-discrimination (Buolamwini & Gebru, 2018; Dolata et al., 2022). Hence, the literature points to the idea of epistemic injustice as the problem and contributes to the arguments used in favor of FRT bans.

A second, more pragmatism-driven perspective on FRT governance adopts a risk-based approach. It acknowledges the widescale adoption of FRTs and emphasizes the importance of evaluating how these technologies interact with institutional practices, cultural norms, and legal frameworks to ensure that their benefits outweigh potential harms (Lynch & Campbell, 2024; Smith & Miller, 2022). This viewpoint foregrounds risks to human rights, including threats to privacy, data protection, non-discrimination, constant surveillance, and freedom of movement and expression. For example, Australia's proposed Model Law is based on this perspective as it calls for mandatory reviews of high-risk FRT applications (Davis et al., 2022). Thus, framing FRTs as socio-technical assemblages becomes particularly relevant, especially given the lack of transparency surrounding their use in law enforcement (Matulionyte, 2024; Radiya-Dixit & Neff, 2023).

2.2. Transparency of FRTs and/or algorithmic systems

We define *transparency in FRTs and/or algorithmic systems as the extent to which knowledge about disclosure, explanations, and evaluations is accessible to stakeholders,* such as regulators, affected individuals, civil society, and technical experts. From a socio-technical perspective, knowledge relates to technological solutions, information, and interaction between social and technical components. Transparency should enable stakeholders to monitor, interpret, and verify the design, operations, decision-making processes, and performance of FRTs and/or algorithmic systems. We argue that transparency rests on three interrelated sources: technology, information, and interactions between social and technical components.

Previous empirical work ranges from ethnographic fieldwork on government algorithms (Moats & Trifuljesko, 2025) to algorithmic audits of bias in facial analysis (Buolamwini & Gebru, 2018) and mixed-method studies of police use of FRT (Radiya-Dixit & Neff, 2023). These studies primarily operationalize transparency via disclosure – such as design purpose, institutional context, and bias reports – and evaluation mechanisms like impact assessments, external audits, and inclusive datasets. Conceptual contributions on FRT transparency (e.g., Gikay, 2023; Matulionyte, 2024; Rajendra & Thuraisingam, 2025) expand this by detailing disclosure of system type, procurement procedures, and contextual deployment, alongside evaluation through proportionality assessments, oversight bodies, and explainability frameworks. Accordingly, FRT applications should ensure transparency by collaboratively including disclosures, explanations, and evaluations (Valderrama et al., 2023). These measures help promote algorithmic fairness and align with institutional norms, values, and regulations throughout the system's lifecycle.

Transparency is a central concern in the regulation and governance of algorithmic systems such as FRTs (Fletcher, 2023) and global evidence shows persistent gaps in technical design and implementation (Valderrama et al., 2023). Mechanisms to enhance transparency include model cards documenting data and system details, deployment registers, source code disclosure, and public information requests. However, socio-technical complexities create significant regulatory hurdles, requiring coordinated engagement among diverse stakeholders. The following section explores these challenges through examples from Australia's public and private sectors.

2.3. (Non-)transparency of FRTs in the context of Australia

While FRTs have a clear value for policing, such as serving as a supportive mechanism in criminal lead identification, the Australian Federal Police (AFP) has adopted FRTs from questionable providers without conducting privacy assessments. The most infamous case to date has been the trial of the globally contested Clearview AI Inc., an FRT tool that offers individual identification based on facial data scraped from the Internet without consent. Clearview AI offered a trial to several Australian police departments between October 2019 and March 2020, including the AFP. On 14 October 2021, the Office of the Australian Information Commissioner ordered Clearview AI Inc. to destroy and cease collecting any further images of individuals in Australia. Shortly after, on 16 December 2021, following the Clearview AI ruling, Privacy Commissioner Angelene Falk found that the AFP breached the Australian Government Agencies Privacy Code and APP 1.2 by failing to conduct a privacy impact assessment before using the tool, thereby neglecting its privacy obligations (Office of the Australian Information Commissioner [OAIC], 2021). The legal privacy instruments at the disposal of the OAIC, however, have not been utilized to determine whether Clearview AI has ceased collecting Australians' facial data and deleted it, and further legal action is not being considered by the OAIC (OAIC, 2024).

Despite the 2021 OAIC ruling, the freedom of information requests filed by the Guardian in 2023 revealed that AFP staff continued to trial similar face search engines PimEyes and FaceCheck.ID between 1 January and 4 August 2023 – reportedly without official endorsement or knowledge of the AFP (Bogle, 2023). Unlike Clearview AI, which sells its services to law enforcement, the Seychelles-headquartered PimEyes encourages consumers to search only for their own image but does not offer any guardrails to ensure this singular use, such as a requirement to share a government-issued ID to verify identity (Hill, 2022). Unsurprisingly, their services have been associated with stalking (Harwell, 2021). FaceCheck.ID is a smaller-scale website, similar to PimEyes in its set-up and pricing. Overall, the absence of privacy impact assessments in law enforcement trials involving FRTs, combined with a lack of transparency around the objectives of deploying these technologies, underscores significant transparency concerns (Edelman, 2023), especially considering declining public trust in Australian governmental agencies (Flew, 2025).

Beyond Australian government services and law enforcement, broader regulation is failing to keep pace with the swift adoption of FRTs by private providers in Australia, resulting in insufficient protection for privacy, consumer, and human rights alike (Fletcher, 2023; Lynch & Campbell, 2024). In Australia, the Privacy Act specifically

mentions biometric information, including facial data, stipulating that such information cannot be collected without a person's consent. The consent, however, can be either expressed or implied and is thus heavily reliant on the notification about the collection of biometric data (Whitfield-Meehan, 2022). What this means in practice is that minimal notification makes it legal to have your facial data collected at a supermarket (Kelly, 2024), hardware store (Office of the Australian Information Commissioner, 2022), or stadium (Blakkarly, 2023). Complaints can be made to the OAIC only when no or insufficient notification is made available in private spaces, as was the case in complaints made against Australian entities, hardware store Bunnings, department store Kmart, and electronics retailer Good Guys' use of FRTs (Office of the Australian Information Commissioner, 2022).

In Australia, the ongoing ambiguity surrounding transparency, combined with the absence of a robust regulatory framework, has fueled public mistrust of FRTs. Over one in four Australians (27%) consider facial recognition technology to be among the most serious threats to privacy today, while just 3% believe it is fair for retailers to require biometric data to access their services (Kind, 2024). This resistance is increasingly reflected in calls to limit or ban the use of algorithmic systems (Aniulis, 2022; Davis et al., 2022; Fletcher, 2023).

These contextualized understandings raise serious concerns about democratic accountability and human and privacy rights protections in contexts where FRTs are allowed to be applied. There is a strong technological pull from private FRT providers, which has been met with an eager uptake by public sector actors, often without sufficient scrutiny or public consultation. Additionally, law enforcement agencies have deployed FRTs with little to no transparency, covertly bypassing essential procedural safeguards. Accordingly, the Office of the Australian Information Commissioner has found these actors to breach privacy impact assessment obligations, yet FRT trials and covert implementation persist. The absence of enforceable regulatory frameworks enables operational secrecy and shields the deployment of FRTs from public oversight. Therefore, there is an urgent need to map out transparency for algorithmic systems, such as FRTs.

3. Research design and methods

Acknowledging the varied forms and uses of FRTs, we took a multi-stakeholder approach to recruit experts in governance and regulation for semi-structured interviews. Our sample included experts from the technology industry (n = 12), academic (n = 9), and policy (n = 14) backgrounds, with five individuals having dual expertise (see Table 1). We defined an 'expert' as someone with direct experience in FRT and the capacity to influence policy, and who had 'comprehensive and authoritative knowledge in a particular area not possessed by most people' (Caley et al., 2014, p. 232). Inclusion criteria were: (1) experience in designing or advising the use of FRT, (2) a minimum of three years of experience with FRTs, and (3) affiliation with one or more of the following Australian organizations: Commonwealth or state government agencies, independent institutes and think tanks, universities, or public or private technology development organizations. On average, the experts we spoke to had 10.5 years of experience in the field of FRT.

We recruited participants using a combination of convenience and snowball sampling strategies. To recruit participants, we compiled a longlist of Australian tech companies

Table 1. Interviewee description.

Identifier*	Gender	Years of experience in FRT	Types of experiences
T1P1	M	20	FRT development, critical infrastructure, control over facial data and meaningful consent.
T2P2	M	6	Accuracy and bias management in FRT systems, testing, regulatory gaps, black box FRTs.
A1	M	6	Public consultation, performative public deliberation.
T3	M	7	Facial image databases, loose privacy guidelines.
T4	M	23	FRT development, accuracy, reliability, ensuring data privacy and security.
A2	F	20	Implementation of biometric tech, proportionality assessment, data security.
A3P3	F	6	New tech implications for human rights and social justice, regulatory gaps.
A4	M	3	Securitization of public and privacy spaces, tech company reputational politics, lack of clarity around development and deployment of FRTs, individualized harms.
T5	M	5	Technology importation risks, bias in design, responsible deployment based on specific use cases, cyber security of data handling.
T6	M	25	Biased imported tech, international standards (e.g., NIST), unregulated environment allows competition via security benchmarks.
P4	F	22	Gaps in privacy and human rights regulation, adoption based on inflated security narratives, disparate surveillance systems pose risks to civil liberties.
A5	M	3	Mass surveillance, meaningless consent, opaque global FRT supply chains, surveillance capitalism, epistemic injustice.
P5	F	6	Moratorium before protections ensured, Australia's lack of a Human Rights Act, chill factor for civil liberties, surveillance capitalism, lack of public trust.
T7	M	3	Imported FRT security risks, privacy legislation overdue, purpose-limited FRT adoption, 'slow slide' into dystopian surveillance.
P6	F	3	Consumer rights, issues with knowledge and consent to FRTs.
P7	M	4	FRT gender and race biases, current legal guidelines easy to bypass, principle of proportionality, adoption based on inflated security narratives.
P8	F	3	Australia's lack of a Human Rights Act, fundamental right to privacy.
T8P9	F	16	Unregulated FRT use, international standards, data retention limits, inherent bias, mental stress mitigation via FRT use in criminal tasks.
A6	M	3	FRT affordability and reliability, widespread adoption, low public awareness, regulatory gaps, rollback implications of proposed laws, strong public support for policing/public safety, use obfuscation.
T9	M	3	Customer demand for FRT, unclear industry standards, data security.
A7	F	19	Principles of consent, proportionality, review and accountability, Australia's lack of a Human Rights Act, experimental approach, mass facial databases, moratorium before protections ensured.
T10	M	21	Managing customer perceptions, transparency about limitations, clear access rules, scope creep, industry-led guidelines development.
T11P10	M	6	Limited scope searches to help solve crime, evidence triangulation, training and staff selection to avoid operational biases, industry-led guidelines.
P11	F	18	Misidentification risk, lack of legal protections and technical guidelines, purpose-led use of tech, data security, risk-based FRT adoption.
P12	M	3	Mass databases, public pushback dismissal, experimental FRT adoption, civil rights chilling effect, lack of accountability, lack of transparency, necessity and proportionality, risk-based deployment.
A8	F	25	History of FRTs, necessity and proportionality.
A9	M	12	FRT accuracy, accuracy conditions, evidence in court, transparency about limitations.
T12	M	18	Lack of standardization, international standards.
P13	M	3	Oversight, transparency, reporting requirements, technology neutral legislation, lack of model legislation, data security.
P14	F	3	Data security.

*Identifiers were assigned to represent FRT experiences in technical (T), academic (A), and policy (P) domains. A dual identifier was used for respondents with expertise in more than one area.

engaging with best practice bodies, academics who have published on FRT, and policy stakeholders who have advised on or influenced policy. Everyone on the longlist was contacted, with follow-up messages sent as needed. Recruitment was conducted through direct emails, professional platforms such as LinkedIn, and referrals. A key limitation was the difficulty in recruiting law enforcement and industry stakeholders; even leading tech firms often took months to respond and often ended in 'research ghosting,' highlighting the broader opacity reflected in our findings.

Interviews were conducted in a semi-structured format between April 2022 and March 2023. They align with the problem-centered expert interview approach, which emphasizes individual perspectives, provides a defined structure and question set, enables data comparability, and supports inductive-deductive theory building by exploring the implicit dimensions of expert knowledge (Döringer, 2021). Because FRT regulation spans technical design and application, interviewees were first asked about their experience and definitions of FRTs, enabling them to share perspectives and allowing the interviewer to tailor follow-up questions to their expertise. Participants were then asked about best practices in their area of FRT governance, whether current regulation sufficiently prevents social harms, and, if not, what improvements could be made. Prompts were tailored to elicit expert insights. For example, legal scholars were asked how principles like necessity and proportionality could be implemented on the ground and what barriers exist, whereas technical respondents were prompted to talk to industry standards.

For data analysis, we followed Braun and Clarke's (2021) six-step coding process: familiarizing ourselves with the data through repeated reading, generating initial codes, identifying themes, naming and defining them, and producing the final narrative. Throughout, we acknowledged that researchers bring existing theoretical knowledge to the analysis. Our approach combined theory-driven deductive and data-driven inductive methods: we drew on key scholarship in algorithmic system governance. Throughout our analysis, we continually engaged with relevant scholarship on transparency in FRT regulation and governance, arriving at the typology of 'transparency.' This recursive process helped identify codes and themes that were both theoretically grounded and empirically meaningful, supporting theoretical triangulation. As sentiment was not coded, quotes were lightly edited to remove filler words. Ethics approval was granted by the Griffith University Ethics Committee (approval number #2002/007).

It is important to note that participants primarily discussed the regulation of one-to-many FRTs, not one-to-one FRTs. Interviewees mentioned the potential for deploying FRT best practices that effectively preserve the security and privacy of facial data by design, through measures such as on-device data storage and other privacy-by-design and human-centered principles (Rosenbrock, 1989; Schaar, 2010). We, therefore, excluded the regulation of one-to-one FRTs because respondents perceived these applications as having lesser potential for social harms and a manageable impact on human rights, should safeguards be employed.

We present the results in two parts. First, the Results section outlines the spectrum of FRT transparency practices discussed in the interviews, highlighting the various ways stakeholders interpret and operationalize 'transparency' as a best practice. Then, we discuss our novel empirical findings and their policy implications, constructing the transparency typology and situating these insights within the broader scholarly literature.

4. Results

4.1. Technical transparency

The first type of transparency issue we identify is characterized by stakeholders' ability to access and understand the design choices, input features, and training datasets that shape the system's behavior. The purposes of technical transparency are to enable debugging, support local adaptation, and facilitate bias auditing. Therefore, relevant disclosures should be provided about the developer/vendor/platform, the type of training data used, and what is missing or included in the reference dataset. Additional explanations are needed on how the data is collected, whether any part of the data was deleted, and the history of updates, including changes to datasets.

The technical participants we spoke to were confident in their understandings of technical best practices. Participants detailed what technical best practices meant for them in their industry contexts, including a strong understanding of their own FRT supply chains (T9). A technical respondent highlighted a supply chain security issue in the FRT device manufacturing process, explaining that during a routine quality check of imported goods, an X-ray revealed a surveillance device embedded within the plastic casing parts imported from China (T9). The company had rigorous internal quality assurance processes and was able to eliminate that supplier. While this example only relates to FRT hardware (and not software), it shows that technical industry standards for the production and adoption of FRTs are critical at each step.

Participation in international standard-setting was also flagged as a must for technology companies. Technical respondents discussed the need to develop and follow global standards for biometric governance (T8P9), improve accuracy and reliability through advances in machine learning (T4), and strengthen data security by storing data within Australia. They also emphasized avoiding partnerships with companies from countries facing bans or sanctions, participating in international algorithm testing (T6), setting access controls (T10), and engaging with Australian biometrics standards, testing initiatives, and guideline-setting communities of practice (T6, T10).

While technical respondents knew where to get information on technical best practices and many proactively sought benchmarking their products against international standards, respondents also noted that self-regulation was a double-edged sword: while good for innovation, it did not encourage all technology providers to adhere to best practices. Only one respondent (T6) believed current regulation was sufficient, citing the lack of clear industry standards as a competitive advantage for their private firm. One technical participant with over two decades of experience in developing FRTs noted that regulating FRT development that is dispersed via global supply chains was technically very difficult to trace back and audit each part of the system (T6). In Europe, the ethics of biometrics are governed by three standard-setting bodies and a practitioner with experience in Europe and Australia noted that the Australian standard market is not yet mature: 'there's definitely a bit more of a friction in the Australian national context [regarding the ethics of biometric technologies]' (T12), further discussed under the 'Procedural transparency' theme.

4.2. Functional transparency

Technical choices, such as design and input data, significantly shape how a system functions and behaves, which in turn affects its outputs. The second type of transparency we identify focuses on what a system produces and why, emphasizing the accuracy of its outputs and the behavior of the system. This form of transparency responds to concerns about FRT performance reliability, explainability, and interpretability to enhance algorithmic fairness. Developers should explain false positive and false negative rates, along with demographic performance. They should also clarify the algorithmic architecture and any local modifications made to the models.

Concerningly, our research recorded a new finding related to the performance of FRTs deployed in Australia on First Nations Australians, a population that has been historically acutely over-represented in the criminal justice system (Ogilvie et al., 2024). FRT providers often claim a high level of accuracy for their products, some even critiquing the seminal work of Buolomwini and Gebru (2018) for being dated (T6) but failing to note that there are no official results of FRT accuracy levels when working with First Nations Australians (T2P2, P13). A Federal Government employee working in a national security role explained why that was the case:

> When we do get questions like 'how does face recognition perform with Indigenous or African populations?' we rely on anecdotal reports from people that are using face recognition with those populations … The US framed their consent slightly differently so that they could retain data for testing. Australia has chosen to not have that conversation with the Australian public and not in all cases retain data and make it available for testing. (P13)

Indeed, global scholarship has identified race and gender biases perpetuated by FRTs as key issues with deployment. Darker-skinned women are the most often misclassified group as opposed to the most accurate classification rates for white men (Buolamwini & Gebru, 2018). Among some of the most gruesome examples of this bias growing at scale are wrongful arrests of primarily black people due to FR misidentification (including an eight-month pregnant woman who was wrongfully accused of carjacking; see Hill, 2023), Google's identification of black women as gorillas and, most recently, in 2021, Meta's software labeled black men in video footage as 'primates' (Man, 2021). Additionally, real-time, or live FRT, stop-and-frisk initiatives in the United Kingdom were shown to be leading to wrongful stops (Carlo, 2020).

In the absence of functional transparency, the challenge of explaining potential errors made by algorithmic FRT systems was most clearly expressed by a technical stakeholder with over 20 years of experience in developing image-based and FRT applications. Despite having helped design the very system that flagged him at an airport, the respondent noted he would struggle to articulate what would constitute discrimination by an FRT system:

> Usually those stakeholders, those end users who get impacted, don't have the full picture. So, it's difficult to complain or prove the point that there's systematic discrimination against this cohort. An interesting example is, whenever I pass through the Australian border with my family, they get through the automated gates, and I get stopped. I kind of understand because I know what's happening behind it – I'm a male in this age group and they're kids, so they get a different score. But could it be considered discrimination? Is it broad enough to call it out? I don't know, and that's the problem. (T10)

Our data shows that functional transparency is largely black-boxed in Australia, both by intention and due to FRT system complexity. While some stakeholders – such as a law enforcement respondent who emphasized the importance of functional transparency because they 'can't afford false identifications' (T11P10) – expressed this view, the prevailing opinion was that adherence to ethical practices largely depended on individual leaders within teams or organizations.

4.3. Procedural transparency

Turning to institutions, the third mode of transparency that we identify is characterized by the clarity of governance structures for deploying the system, such as OAIC's best practice guide for FRT privacy risk compliance (Office of the Australian Information Commissioner, 2024). The purpose is to achieve legal responsibility and accountability. Therefore, an explanation should be provided on how actors' decisions are made, who is responsible for accounting for continued monitoring of FRT deployment, and what legal frameworks guide the systems' deployment. Such explanations are vital for regulators and watchdogs to evaluate whether proper safeguards, such as data protection, are in place and being followed.

All but one respondent – a technical interviewee with over two decades of experience (T6) – agreed that FRTs can cause a range of harms in the context of current legal and regulatory backgrounds. Indeed, four technical and policy stakeholders affirmed that they knew of real-life cases of FRT providers not following privacy assessments or industry best practices. This is where enforceable legal requirements would be useful, as they could help close accountability gaps and ensure that ethical standards are upheld across the sector, not just by leading or well-intentioned actors, as eloquently put by one of the key FRT policymakers in Australia:

> There are a range of applications for the technology that can be beneficial, but we need to guard against the risks at the same time … I actually think you need to look at all of those things because it really is about creating a complete framework and the fact is there is no single answer that will address this. (P11)

10 of our 30 respondents spoke to the urgency of patching the existing privacy and human rights legislation. Respondents recognized that the existing and recently updated privacy legislation in Australia is over-reliant on notification and has limited use to restrict FRTs in public spaces. Legal frameworks governing FRTs in Australia have long been described as 'patchwork' (Lynch & Campbell, 2024, p. 253). Legal scholarship has suggested that future privacy law reforms should cover all current and future uses of facial recognition technologies, restrictions on consent loopholes used by tech companies, and strict guidelines for data storage, including retention limits, encryption, and government audits. Non-compliance should carry penalties comparable to those under the EU's General Data Protection Regulation to ensure accountability and safeguard individual rights (Conde & Svantesson, 2024; Fletcher, 2023). Additionally, participants noted that while Australia has a Human Rights Commission, it lacks a national Human Rights Act, and only a few states have enforceable human rights legislation.

Respondents' views diverged when asked whether tech-based regulation should be enforced or self-directed. While there were a few, most interviewees with a technical background recognized that without regulatory enforcement, compliance among the

FRT actors would remain fragmented. In evaluating government-based FRTs from both technical and policy standpoints, a technical respondent argued:

> Although we have standards in place and quite well-written standards for following testing and tuning of algorithms, there's no mandate anywhere to actually follow them … It definitely comes down to money and time. (T9)

Literature on industry self-regulation often positions it as the opposite of government-led regulation. However, self-regulatory practices have consistently failed to ensure technical robustness, consumer privacy, human rights, and data security (Chamikara et al., 2020; Rubinstein, 2018). Voluntary privacy codes, in particular, have had ample opportunity to prove their effectiveness but have fallen short (Rubinstein, 2018). A key concern is the readiness of both public and private sectors to launch digital initiatives involving biometrics, despite weak legal protections for privacy and human rights. While tech-based regulation (e.g., communities of practice and technical standards) has received praise, its limitations are clear when standards and best practices remain voluntary. Enforceable regulatory guidelines could support procedural transparency from a legal point of view.

4.4. Public transparency

The fourth mode of transparency that we identify is characterized by the extent to which the community or the general public is aware that FRTs are being used, by whom, and for what purpose. It goes beyond mere disclosure or disclaimer through signs in public spaces, public notices, or organizational disclosure (Andrejevic & Selwyn, 2022; Matulionyte, 2024). It aims to ensure public participation, public scrutiny, and counter governments' techniques in service design and use decisions. It also ensures that citizens and affected individuals are aware when they are being subjected to facial recognition, enabling them to provide informed consent and participate in public debate. Explanations should be provided regarding their rights, how data will be used, where data will be stored and processed, and the mechanisms for filing complaints.

One academic and legal practitioner with two decades of experience described this as the appeal of 'sexy, sexy technology':

> [There needs to be] extensive consultation rather than—you know—you finish work on Friday and on Monday you're logging in with a facial recognition technology, which I've seen happen. (A2)

One participant who has extensively engaged in academic research on FRTs in Australia, shared an anecdote from the field:

> In many cases, municipalities are just implementing that technology without much publicity or much public discussion or debate. We had an interesting case when we went down to Adelaide. We wanted to stage a public discussion about the potential use by the City Council of facial recognition in its CCTV upgrade … They were receiving a lot of media attention and started insisting that they had never considered using that technology … But we found out through media coverage that the police were already using facial recognition technology.

The hesitancy to engage in public opinions in FRT implementation, secrecy and deceptiveness around the deployment of FRTs is seen in numerous cases, such as the case of

Adelaide noted in this article, the expansion of surveillance cameras with FRT capabilities against organized citizen pushback in Perth (Turner, 2019), the covert use of unethical FRT providers by the AFP, or concerns of misidentification of Indigenous people in the Northern Territory (Fletcher, 2023).

4.5. Contextual transparency

Turning to the operating environments, the final mode of transparency is characterized by considering whether the use of FRTs is appropriate and understandable within a specific institution (i.e., value judgment or cultural) context. This mode acknowledges that the meaning and acceptability of FRTs vary across different operating environments (e.g., schools, airports, and border control). Explanation must reflect local values, norms, and expectations. It aims to gain legitimacy and social license to operate, which includes local stakeholders in service design and use decisions. In the words of a legal scholar engaged in policymaking for over two decades, it was important to consider why and where their use was appropriate.

Public deliberation – or rather the lack thereof – was a prominent overarching element among interviewees (A1, A4, P4, P5, P11). A participant reflected on the limited nature of contextual transparency in FRT implementation, observing that it often involves collecting people's facial data without clearly explaining why the technology is needed, necessary, or valuable:

> I want to see this much more decolonized because it's completely, utterly reifying power, and particularly white power. I want to see much more diversity, much more politics, much more engagement of different communities in the story, in the narrative, and hopefully in reshaping how this thing works and everyday life, so it's not going to simply work in the asymmetrical fashion. (A4)

Another academic respondent reflected on the performative nature of public consultations regarding biometrics:

> I think it's important that that public debate inclusion is not just symbolic, that people get sufficient time. It's not that you just throw out one week for people to react to it and work coming legislation, and nobody has the time to actually draw up a coherent advisory on the legislation. (A1)

Although Australia has mechanisms for public consultation, gauging public opinion, and communicating with stakeholders, concerns about contextual transparency persist. One prominent issue is that these government consultations on FRT implementation often appear performative, encouraging a checkbox exercise in consultative democracy, rather than ensuring that FRT implementation is responsive to and aligned with public values.

5. Discussion: toward a typology of transparency in algorithmic surveillance systems

Our findings adopt a socio-technical perspective and identify five distinct modes of transparency in FRTs (see Table 2). These five modes advance the critical governance literature by offering new ways to conceptualize transparency in addition to disclosure and explainability (Andrejevic & Selwyn, 2022; Introna & Wood, 2004; Yeung, 2017). Each mode addresses the needs of various stakeholders including deploying agencies, users,

Table 2. Purpose and required accessible knowledge for each mode of transparency.

Mode of transparency	Required accessible knowledge	Purpose
Technical	• Details on algorithm design (e.g., model types, decision logics) • Training data sources and diversity • Preprocessing and feature extraction methods	To allow experts, auditors, or researchers to inspect biases and integrity in the system's design and reference dataset.
Functional	• Accuracy rate, error rate (e.g., false positive/negative) • Permanence across demographic groups • System architecture	To help auditors, users, and regulators evaluate how the systems perform and behave.
Procedural	• Legal basis for deployment • Roles and responsibilities • Reports on governance framework (e.g., risk assessment, audit, impact assessment)	To ensure that regulators, courts, and policymakers monitor lawful deployment and hold those accountable.
Public	• Notification of where/when FRTs are used • Purpose and justification for deployment • Data retention and rights information (e.g., opt-out mechanism)	To enable citizens and civil society to understand when and how the public is being surveilled.
Contextual	• Explanations of how local values, norms, and culture were considered • Stakeholders engagement reports • Situation-specific justification for deployment	To help courts, auditors, or researchers assess the legitimacy and appropriateness of deployment in a given institutional context.

auditors, legislators, civil society, policymakers, and the general public (Radiya-Dixit & Neff, 2023). The typology also expands the concept of organizational transparency by distinguishing between internal and public-facing practices (Matulionyte, 2024). We explain each mode, progressing from the micro-level foundations of technology and information to the macro-level context of institutions and environments. Our findings indicate that achieving transparency in algorithmic biometric systems is a complex task; simply identifying the target of biometric surveillance amounts to 'transparency washing' (Zalnieriute, 2021). The proposed typology of transparency helps unpack this complexity by making the watchers visible to those under surveillance.

The findings of this article probe transparency as best practice in the design and implementation of FRTs as systems requiring multi-stakeholder governance and regulation. *Technical transparency findings* show that while key technical industry stakeholders are generally engaged in industry-led best practice conversations, they admit that voluntary best practices will always be balancing between 'money and time' for industry stakeholders; many have seen examples of providers that have used the loose regulatory environment to not choose the technical best practices, and some have primary experiences of witnessing efforts of espionage. These insights align with research on industry self-regulation, which finds such practices are usually adopted by leading firms. *Functional transparency* highlights the absence of data on Indigenous Australians in FRT reliability assessments – an omission that is especially troubling, given their overrepresentation in the criminal justice system. Even industry leaders struggle to identify when FRTs are applied in discriminatory ways, leaving doubts about whether functional transparency is even possible when a system is

being implemented. *Procedural transparency* interacts with the necessity and proportionality principles put forth by the OAIC as best practice; enforceable regulatory guidelines can support procedural transparency from a legal point of view. In Australia, further enforceable laws and regulations (e.g., stricter privacy laws, human rights obligations, or mandatory technical standards) are currently insufficient and are required for procedural transparency to be effective. *Public transparency* underscores the need to clearly communicate why FRTs are being adopted to the public. Interviewees critiqued the rapid deployment of FRTs in contexts where their necessity was unclear, referring to these as 'sexy sexy technology' use cases. Finally, *contextual transparency* emphasizes meaningful public deliberation to assess the fit of FRTs. While consultation mechanisms exist, stakeholders noted their performative nature, stressing that these processes must be used as intended, even if that means deciding against the implementation of FRTs.

Our algorithmic system transparency typology serves four key purposes. First, it offers a systemic operationalization of transparency in the algorithmic biometric systems. Second, it provides a practical tool for stakeholders to align transparency efforts with their specific roles and capacities. Third, it supports regulators in identifying gaps and inconsistencies in transparency practices. Finally, by grounding the typology in empirical evidence, we highlight that transparency challenges are not solely technical, but also deeply social and political. A key limitation is that the transparency typology offers conceptual clarity and a tool for alignment, but it cannot explain the larger dynamics of power, control and surveillance of biometric surveillance systems.

6. Conclusion

'Transparency' is often promoted as a best practice in the adoption of algorithmic systems, yet the term can slip into ambiguous normative interpretations that obfuscate larger concerns of power, control, and surveillance. To articulate what transparency of FRTs means in practice, our multi-stakeholder research drew on insights from 30 problem-centered expert interviewees focused on algorithmic surveillance systems, namely facial recognition technologies. Based on these perspectives, we develop a five-part transparency typology that theorizes how transparency should be best articulated to overcome the key oversights in FRT adoption across Australia. Our findings critically probe the operationalization of transparency as best practice, viewed through technical, functional, procedural, public and contextual lenses.

The notion of transparency cannot be reduced to a unilateral logic of asymmetrical visibility, where one actor observes while remaining unobserved, within the context of biometric surveillance. The typology developed in this paper contributes new conceptual clarity to the critical governance literature by distinguishing between transparency as disclosure and transparency as explainability. It also offers a practical framework for policymakers, technologists, and oversight bodies to evaluate and improve transparency measures in algorithmic surveillance. By foregrounding the situated and multi-stakeholder governance nature of transparency, our work underscores the need for more reflexive, inclusive, and context-sensitive approaches to articulating algorithmic transparency.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Ausma Bernot is a Lecturer in Technology and Crime at the School of Criminology and Criminal Justice at Griffith University. Her research focuses on the intersection of technology and crime, with a particular focus on surveillance and technology governance [email: a.bernot@griffith.edu.au].

Rakibul Hasan is a Doctoral Researcher in International Business at the University of Vaasa, Finland. Hasan's research, teaching and publication activities are at the cross-section of space, artificial intelligence, international business, information systems, management, and sustainable development. He obtained his Master of Science in Business Administration and Economics at Aalborg University, Denmark. [email: rakibul.hasan@uwasa.fi]

Milind Tiwari is a Senior Lecturer in financial crime studies at the Australian Graduate School of Policing and Security, Charles Sturt University, and Senior Research Associate at the Centre for Banking Law, Faculty of Law, University of Johannesburg. His work focuses on various facets of money laundering, including the role of technology and databases in detecting and deterring it. [email: mtiwari@csu.edu.au]

Peita L. Richards is a Research Fellow and Lecturer at Centre for Law and Justice at Charles Sturt University, and a current recipient of the Office of National Intelligence, National Intelligence Postdoctoral Grant, 2023 (project 202308). Her research is focused on extending methods developed in her doctoral research to the national intelligence priority area of 'measuring reliable behavioral indicators of multiple social identity features in real world settings.' [email: peirichards@csu.edu.au]

Brendan Walker-Munro is an Associate Professor (Law) with the Faculty of Business, Law & the Arts at Southern Cross University. Brendan's focus is on 'research security,' the use of law and policy to protect university research from national security threats such as espionage, foreign interference, hacking, and technology transfer. He also researches other aspects at the intersection of national security law and higher education, such as research funding, privacy, and digital security. [email: brendan.walker-munro@scu.edu.au]

References

Andrejevic, M., & Selwyn, N. (2022). *Facial recognition*. John Wiley & Sons.

Aniulis, H. (2022). Facial recognition technology, privacy and administrative law. *University of New South Wales*, *45*(4), 1513–1555. https://doi.org/10.53637/LMEY6569

Blakkarly, J. (2023, July 5). Facial recognition technology in use at major Australian stadiums. *CHOICE*. https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/facial-recognition-in-stadiums

Bogle, A. (2023, October 24). Australian federal police tested controversial facial recognition search engine, FOI documents reveal. *The Guardian*. https://www.theguardian.com/australia-news/2023/oct/24/australian-federal-police-afp-pimeyes-facial-recognition-facecheck-id-search-engine-platform

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Conference on fairness, accountability and transparency*, 77–91.

Caley, M. J., O'Leary, R. A., Fisher, R., Low-Choy, S., Johnson, S., & Mengersen, K. (2014). What is an expert? A systems perspective on expertise. *Ecology and Evolution*, *4*(3), 231–242. https://doi.org/10.1002/ece3.926

Carlo, S. (2020). Big brother watch briefing on facial recognition surveillance. https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf

Chamikara, M. A. P., Bertok, P., Khalil, I., Liu, D., & Camtepe, S. (2020). Privacy preserving face recognition utilizing differential privacy. *Computers & Security*, *97*, 1–12. https://doi.org/10.1016/j.cose.2020.101951

Conde, J., & Svantesson, D. J. B. (2024). The five generations of facial recognition usage and the Australian privacy law. *International Data Privacy Law*, *ipae007*, 247–258. https://doi.org/10.1093/idpl/ipae007

Davis, N., Perry, L., & Santow, E. (2022). *Facial recognition technology: Towards a model law*. University of Technology Sydney. https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf

Dolata, M., Feuerriegel, S., & Schwabe, G. (2022). A sociotechnical view of algorithmic fairness. *Information Systems Journal*, *32*(4), 754–818. https://doi.org/10.1111/isj.12370

Döringer, S. (2021). 'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology*, *24*(3), 265–278. https://doi.org/10.1080/13645579.2020.1766777

Edelman. (2023). Edelman trust barometer: Navigating a polarised world. https://www.edelman.com.au/trust/2023/trust-barometer

European Commission. (2024, August 8). AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Farthing, S., Howell, J., Lecchi, K., Paleologos, Z., Saintilan, P., & Santow, E. (2021). *Human rights and technology: Final report*. https://humanrights.gov.au/sites/default/files/document/publication/ahrc_rightstech_2021_final_report_10.pdf

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), 1–33. https://doi.org/10.1016/j.heliyon.2023.e15090

Fletcher, A. (2023). Government surveillance and facial recognition in Australia: A human rights analysis of recent developments. *Griffith Law Review*, *32*(1), 30–61. https://doi.org/10.1080/10383441.2023.2170616

Flew, T. (2025). Trust in government and data: What the Edelman Trust Barometer tells us about Australian society. *Australian Academy of the Humanities*, *82*(2), 414–449. https://humanities.org.au/power-of-the-humanities/trust-government-data-edelman

Gikay, A. A. (2023). Regulating use by law enforcement authorities of live facial recognition technology in public spaces: An incremental approach. *The Cambridge Law Journal*, *82*(3), 414–449. https://doi.org/10.1017/S0008197323000454

Harwell, D. (2021, 14 May). This facial recognition website can turn anyone into a cop — or a stalker. *The Washington Post*. https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/

Hill, K. (2022, May 26). A face search engine anyone can use is alarmingly accurate. *The New York Times*. https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html

Hill, K. (2023, August 6). Eight months pregnant and arrested after false facial recognition match. *The New York Times*. https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html

Introna, L., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, *2*(2/3), 177–198. https://doi.org/10.24908/ss.v2i2/3.3373

Kelly, L. (2024, February 23). The secret sauce of Coles' and Woolworths' profits: High-tech surveillance and control. *The Conversation*. https://theconversation.com/the-secret-sauce-of-coles-and-woolworths-profits-high-tech-surveillance-and-control-224076

Kind, C. (2024). *Facial recognition technology in retail settings: After the bunnings decision*. Office of the Australian Information Commissioner. https://www.oaic.gov.au/news/blog/facial-recognition-technology-in-retail-settings-after-the-bunnings-decision

Koivisto, I. (2021). The digital rear window: Epistemologies of digital transparency. Critical Analysis of Law, 8(1), 64–80. https://doi.org/10.33137/cal.v8i1.36280

Lynch, N., & Campbell, L. (2024). Principled regulation of facial recognition technology: A view from Australia and New Zealand. In R. Matulionyte & M. Zalnieriute (Eds.), *The Cambridge*

handbook of facial recognition in the modern state (pp. 253–266). Cambridge University Press. https://doi.org/10.1017/9781009321211.021

Man, R. (2021, September 3). *Facebook apologizes after A.I. puts 'primates' label on video of black men*. New York Times. https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html

Matulionyte, R. (2024). *Increasing transparency around facial recognition technologies in law enforcement: Towards a model framework*. Information & Communications Technology Law. https://www.tandfonline.com/doi/abs/10.108013600834.2023.2249781

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, *1*(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Moats, D., & Trifuljesko, S. (2025). Valuable actions and actionable values: Tinkering with principles and practices in AI ethics. *The Sociological Review*, *73*(6), 1368–1387. https://doi.org/10.1177/00380261251316661

Moy, L. (2021). Facing injustice: How face recognition technology may increase the incidence of misidentifications and wrongful convictions symposium: Algorithms and the bill of rights. *William & Mary Bill of Rights Journal*, *30*(2), 337–372. https://heinonline.org/HOL/P?h=hein.journals/wmbrts30&i=357

Nirovision. (n.d.). Retrieved 14 August 2025 from https://archive.md/mRHCr

OAIC. (2024, August 21). Statement on Clearview AI. https://www.oaic.gov.au/newsroom/statement-on-clearview-ai

Office of the Australian Information, C. (2024). Facial recognition technology: A guide to assessing the privacy risks. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks

Office of the Australian Information Commissioner. (2021, December 16). AFP ordered to strengthen privacy governance. https://www.oaic.gov.au/newsroom/afp-ordered-to-strengthen-privacy-governance

Office of the Australian Information Commissioner. (2022, July 12). OAIC opens investigations into Bunnings and Kmart. https://www.oaic.gov.au/newsroom/oaic-opens-investigations-into-bunnings-and-kmart

Ogilvie, J. M., Broidy, L., Thompson, C., Dennison, S., Allard, T., Kuluk, A., Crissman, B., Kisely, S., & Stewart, A. (2024). Trajectories of offending and mental health service use: Similarities and differences by gender and Indigenous status in an Australian birth cohort. *Journal of Developmental and Life-Course Criminology*, *10*(1), 97–128. https://doi.org/10.1007/s40865-023-00246-x

Radiya-Dixit, E., & Neff, G. (2023). A sociotechnical audit: Assessing police use of facial recognition. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1334–1346). Association for Computing Machinery. https://doi.org/10.1145/3593013.3594084.

Rajendra, J. B., & Thuraisingam, A. S. (2025). The role of explainability and human intervention in AI decisions: Jurisdictional and regulatory aspects. *Information & Communications Technology Law*, *35*, 1–32. https://doi.org/10.1080/13600834.2025.2537514

Raposo, V. L. (2024). When facial recognition does not 'recognise': Erroneous identifications and resulting liabilities. *AI & Society*, *39*(4), 1857–1869. https://doi.org/10.1007/s00146-023

Rosenbrock, H. (1989). *Designing human-centred technology: A cross-disciplinary project in computer-aided manufacturing*. Springer Science & Business Media. https://doi.org/10.1007/978-1-4471-1717-9

Rubinstein, I. S. (2018). The future of self-regulation is co-regulation. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge handbook of consumer privacy* (pp. 503–523). Cambridge University Press. https://doi.org/10.1017/9781316831960.028

Salko, M., Firc, A., & Malinka, K. (2024). *Security implications of deepfakes in face authentication* Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing. https://doi.org/10.1145/3605098.3635953

Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, *37*(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9

Turner, R. (2019, 8 June). City of Perth rolls out new facial recognition CCTV cameras, but is it surveillance by stealth? *ABC News*. https://www.abc.net.au/news/2019-06-08/city-of-perth-rolls-out-new-facial-recognition-cctv-cameras/11147780

Valderrama, M., Hermosilla, M. P., & Garrido, R. (2023). *State of the evidence: Algorithmic transparency*. Open Government Partnership.

Vladimirova, M. (2024, March 4). Your face for sale: Anyone can legally gather and market your facial data without explicit consent. *The Conversation*. https://theconversation.com/your-face-for-sale-anyone-can-legally-gather-and-market-your-facial-data-without-explicit-consent-224643

Whitfield-Meehan, S. (2022). Privacy: Biometric recognition technology and the "clearview AI" decision. *Law Society Journal*, *86*, 85–87. https://search.informit.org/doi/10.3316informit.20220321063993

Wong, W. H., Duncan, J., & Lake, D. A. (2025). Why data about people are so hard to govern. *Regulation & Governance*, *19*, 236–252. https://doi.org/10.1111/rego.12591

Yeung, K. (2017). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zalnieriute, M. (2021). "Transparency Washing" in the digital age: A corporate agenda of procedural fetishism. Critical Analysis of Law, 8(1), 139–153. doi:10.33137/cal.v8i1.36284