Facial Recognition Technology (FRT): A Strategic Briefing for Victoria Police Senior Management

Executive Summary

Facial Recognition Technology (FRT) represents one of the most transformative and contentious technological developments for modern law enforcement. Its capabilities are advancing at an exponential rate, offering unprecedented potential to enhance investigative efficiency, identify victims, and ensure officer safety. Simultaneously, the proliferation of this technology has ignited profound societal and legal debates, creating a complex and high-stakes operating environment for police agencies. Victoria Police stands at a strategic crossroads, where the decision to adopt, expand, or restrict the use of FRT will have lasting operational, legal, ethical, and reputational consequences.

This report provides a comprehensive strategic analysis of FRT within the specific context of Victoria Police. It is structured into three parts. Part 1 delineates the operational landscape, providing a clear typology of law enforcement applications, distinguishing between reactive (post-event), live (real-time), and officer-initiated uses. It highlights the significant operational benefits, particularly in high-impact areas such as child victim identification.

Part 2 delivers a multi-layered risk analysis. It examines the foundational human rights implications, including the right to privacy and the potential for a chilling effect on democratic freedoms. It assesses critical technical and operational risks, most notably algorithmic bias, data security vulnerabilities, and the consequences of misidentification. This analysis is grounded in the current Australian legal framework, including the Commonwealth *Privacy Act 1988*, the Victorian *Charter of Human Rights and Responsibilities Act 2006*, and the significant push for bespoke regulation as embodied by the University of Technology Sydney's (UTS) *Model Law*. This section also confronts the organisational context, including the legacy of the "Clearview AI

debacle" and the critical need to build and maintain public trust.

Part 3 looks to the future, surveying the rapid technological evolution in FRT over the last two years. It details key advancements in algorithmic accuracy, efficiency, and the ability to overcome persistent operational challenges such as poor lighting and facial occlusions. This section explores the emerging capabilities these advancements could enable, from revolutionising cold case analysis to providing real-time officer safety intelligence, while also flagging the new ethical dilemmas they will inevitably introduce.

The central conclusion of this report is that FRT is not a simple tool to be procured but a complex socio-technical system that demands a sophisticated and proactive governance strategy. The path forward requires a delicate balance between leveraging the technology's potential benefits and upholding the fundamental rights and expectations of the Victorian community. This report culminates in a set of strategic recommendations designed to guide Victoria Police in navigating this complex terrain, advocating for a cautious, transparent, and principles-led approach to the evaluation and potential deployment of Facial Recognition Technology.

Part 1: The Operational Landscape of Facial Recognition Technology in Law Enforcement

1.1 Introduction to Law Enforcement Applications

Facial Recognition Technology is a form of artificial intelligence (AI) that identifies or verifies a person from a digital image or video frame. The technology functions by analysing distinctive facial features to create a unique biometric template, which can then be compared against a database of other templates.[1] In the context of law enforcement, its application is generally categorised into two primary functions: verification, a one-to-one comparison to confirm an identity (e.g., 'Is this person who they claim to be?'); and identification, a one-to-many comparison to determine an unknown person's identity by searching a database for a match.[3]

To provide a clear operational framework, it is useful to adopt the taxonomy used by international counterparts, such as UK policing agencies. This framework distinguishes between three primary use cases, which differ significantly in their operational purpose, intrusiveness, and risk profile: Retrospective Facial Recognition (RFR), Live Facial Recognition (LFR), and Operator-Initiated Facial Recognition (OIFR).[6] Understanding these distinctions is fundamental to any strategic discussion about the role of FRT in Victoria Police.

1.2 Reactive (Post-Event) Applications: Retrospective Facial Recognition (RFR)

Retrospective Facial Recognition (RFR) is the most common and least controversial law enforcement application of the technology. It is fundamentally a post-event investigative tool.[6] Its purpose is to help investigators generate leads by identifying unknown subjects from images captured during or after a crime has been committed.[7]

Operational Workflow and Data Sources

The RFR process begins with a "probe image" of an unknown person of interest. This image is typically obtained from evidence related to a criminal investigation, such as footage from CCTV, a bystander's mobile phone, a vehicle's dashcam, a smart doorbell, or images supplied by the public.7 This probe image is then compared against a controlled, pre-existing reference image database, which for police is almost always the agency's own database of custody photographs.7

The system generates a list of potential candidates ranked by a similarity score. Crucially, this list of potential matches does not constitute positive identification. It serves only as an investigative lead.[11] A trained human operator must first review the potential matches to assess their viability. If a candidate is deemed a likely match, the information is passed to the investigating officer, who must then corroborate the lead with other independent evidence to establish probable cause for an arrest or search warrant.[8] The FRT match itself is not the basis for legal action.

Benefits and Current Use

The primary benefit of RFR is a dramatic increase in investigative efficiency and effectiveness. A study by South Wales Police in the UK found that identifications that would typically take around fourteen days using traditional methods could be achieved in minutes with RFR.8 This speed allows police to identify suspects more quickly and accurately, leading to faster case resolution and prevention of further offences.8 In 2019 alone, the New York Police Department used RFR to generate over 2,500 leads in cases involving murder, rape, robbery, and other serious crimes.11 The technology is also valuable for solving "cold cases," as algorithms can

identify suspects even after many years have passed and their appearance has changed due to aging.12
Within Victoria Police, an RFR system known as "iFace" is currently in use. This suite of tools is available to officers for conducting searches against the force's offender image database for intelligence and investigative purposes, aligning with the standard RFR model.[10]

1.3 Live (Real-Time) Applications: Live Facial Recognition (LFR)

Live Facial Recognition (LFR) operates in a fundamentally different manner from RFR and carries a significantly higher degree of public concern and privacy intrusion. LFR is a real-time, proactive surveillance tool that compares a live video feed from cameras against a predetermined "watchlist" of individuals.[6] It has been described as the digital equivalent of having police officers manually scan a crowd for persons of interest, but performed with far greater speed, scale, and accuracy.[8]

Operational Workflow and Data Management
LFR deployments are designed to be targeted, intelligence-led, and limited in time and geography.8 Before a deployment, a specific watchlist is created. This list is not a general database of all known offenders; rather, it is a bespoke list tailored to the specific operation. It may include individuals wanted on warrants, registered missing persons, or those who are assessed as posing a significant risk of harm to themselves or the public.6
Cameras are focused on a specific, clearly demarcated area, and the public is typically informed of the deployment through signage and other communications.[8] As people pass through the designated zone, their faces are captured and their biometric data is compared against the watchlist. If the system does not find a match, the individual's biometric data is instantaneously and automatically deleted.[8]

If the system generates an alert for a potential match, this information is relayed to a police officer on the ground. It is always the officer who makes the final decision on whether to approach and speak with the individual. The LFR alert is an intelligence prompt, not an order to act.[6] Because of its speculative nature, LFR is considered an indicative screening tool, and its results are generally not intended to be used as evidence in a prosecution. Should an evidential comparison be required, the more rigorous RFR process would need to be followed.[9]

1.4 Officer-Initiated (In-Field) Applications: Operator Initiated Facial Recognition (OIFR)

Operator-Initiated Facial Recognition (OIFR) is a mobile application that provides officers in the field with a tool to help establish a person's identity during an encounter.[6] This use case is still in early trial stages in some jurisdictions but is showing promise.[8]

Operational Use Cases
The primary purpose of OIFR is to allow an officer, after engaging with a person of interest, to take their photograph with a mobile device and compare it against a specific watchlist or database.6 This is particularly useful in situations where an individual is uncooperative, provides false or misleading details, or is unable to communicate their identity due to injury, incapacitation, or a medical event.7
A key benefit of OIFR is its potential to reduce unnecessary arrests. Instead of taking a person into custody solely for the purpose of establishing their identity, an officer can perform this check in the field, de-escalating the encounter and saving police resources.[8]

1.5 Specialized Investigative Applications

Beyond the three main categories, FRT is being applied to highly specialized and impactful investigative areas. One of the most compelling and publicly defensible use cases is in the fight against Child Sexual Abuse Material (CSAM). Members of Australian law enforcement, including from Victoria Police's own victim identification team, have described AI-powered biometric tools as "essential" for identifying both victims and perpetrators from the vast volumes of digital material they must analyse.[13] This technology has been directly credited with the rescue of children who may not have been identified through other investigative means.[5]

Another critical specialized application is the identification of deceased persons where other methods have failed, or the identification of missing persons by matching their images against various data sources.[6] In the context of national security, FRT can also be used as a counter-terrorism tool, for example by comparing images of known or suspected terrorists against footage from public cameras.[12]

The following table provides a consolidated overview of these primary law

enforcement applications.

Table 1: Typology of Law Enforcement FRT Applications

Application Type	Primary Purpose	Typical Probe Data Source	Typical Reference Database	Operational Mode	Key Benefit	Primary Risk Factor
Retrospective (RFR)	Generate investigative leads for past crimes.	Still image from CCTV, mobile phone, dashcam.	Custody image database.	Post-Event, Reactive	Drastically reduces investigation time; solves cold cases.	Misidentification leading to wrongful investigation.
Live (LFR)	Real-time identification of persons on a specific watchlist.	Live video feed from cameras in a public space.	Bespoke, time-limited watchlist of persons of interest.	Real-Time, Proactive	Potential to prevent imminent crime or locate high-risk individuals.	Mass surveillance; chilling effect on public life.
Operator-Initiated (OIFR)	In-field identity verification of a person of interest.	Still image captured by an officer's mobile device.	Watchlist or custody image database.	Real-Time, Officer-Initiated	Avoids unnecessary arrests for identification purposes.	Potential for misuse in routine street encounters.
Specialized (e.g., CSAM)	Identify victims and perpetrators in specific, high-harm crime types.	Images/videos from seized digital material (CSAM).	Victim/offender databases; commercial tools.	Post-Event, Reactive	"Essential" for processing vast data volumes and rescuing victims.	Ethical use of commercial databases (e.g., Clearview AI).

The clear distinctions between these applications are not merely technical; they are profoundly ethical and legal. RFR can be framed as a digital enhancement of a traditional policing function: matching evidence from a crime scene to a database of known offenders. It is a targeted, post-facto process. LFR, in contrast, introduces a form of pre-emptive, population-level screening that is far more controversial. It involves the speculative scanning of every individual within a public space to see if they are a person of interest. This difference in methodology is the source of much of the public's fear of FRT as a "continuous police line-up" [9] and is why regulators like the Office of the Australian Information Commissioner (OAIC) have identified live FRT as being "highly intrusive" to an individual's privacy.[1] Consequently, the political, legal, and social barriers to implementing LFR are substantially higher than those for RFR. This strategic reality suggests that any discussion of adopting FRT within Victoria Police must decouple these applications. Pursuing enhanced RFR capabilities represents a far less contentious path than pursuing LFR.

Furthermore, a significant internal tension exists within Australian law enforcement. On one hand, there is a strong operational desire for these advanced AI tools, particularly within specialized units like Victoria Police's victim identification team, who see them as indispensable for their work.[13] On the other hand, this is hampered by a broader institutional "trepidation" and "big resistance" to using AI, a sentiment that stems directly from past controversies where police forces were "burned pretty badly" by the use of certain products.[13] This reveals a critical disconnect: the units with the most compelling and publicly defensible use cases feel constrained by the reputational damage caused by poorly managed or ethically questionable trials of other FRT applications. This points towards a strategic need to rebuild public trust and internal confidence by championing the most critical and justifiable use cases first, rather than attempting a broad, all-encompassing AI strategy that fails to differentiate between high-risk and low-risk applications.

Part 2: Comprehensive Risk Analysis and Strategic Considerations

2.1 Introduction to Risks and Governance

The adoption of Facial Recognition Technology is not a simple procurement decision; it is an entry into a complex ecosystem of significant and intersecting risks. These risks span the technical, legal, ethical, and reputational domains. For Victoria Police, navigating this landscape requires a sophisticated understanding of the technology's inherent limitations, the intricate web of legal obligations, and the fragile nature of public trust. This section provides a comprehensive analysis of these considerations, moving from universal human rights principles to the specific legal and organisational context of policing in Victoria.

2.2 Foundational Human Rights and Privacy Implications

At its core, the debate over FRT is a debate about fundamental human rights in the digital age. The technology's deployment directly engages and potentially limits several rights that are foundational to a democratic society.

The Right to Privacy

The most direct impact of FRT is on the right to privacy. This right, protected under international law such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which Australia is a signatory, is central to human dignity and autonomy.14 FRT systems operate by collecting, analysing, and storing biometric information, which is considered "sensitive information" under Australian law and is afforded a higher level of protection.1 The use of FRT, particularly in public spaces, enables the collection of this sensitive data on a mass scale, often without the individual's specific or meaningful consent, creating the conditions for a pervasive surveillance society.16

The Chilling Effect on Other Rights

Beyond privacy, the widespread use of FRT poses a significant threat to other fundamental freedoms. The knowledge or perception of being constantly monitored by government agencies can create a "chilling effect," discouraging individuals from participating in lawful democratic activities.17 This directly implicates the rights to freedom of assembly, freedom of association, and freedom of expression.4 Individuals may become hesitant to attend protests, join political groups, or express dissenting opinions for fear of being identified, tracked, and potentially targeted. This concern is a primary driver of opposition from human rights organisations, who argue that FRT gives the state an unprecedented power to monitor and control civic life.16

Mass Surveillance and the Erosion of Anonymity

The combination of ubiquitous CCTV cameras—both public and private—with powerful FRT algorithms fundamentally alters the nature of public space. It threatens to erode the practical

anonymity that has historically been a feature of urban life.20 While proponents argue that law-abiding citizens have nothing to fear, critics contend that this creates a society where every individual's movements and associations can be logged and analysed, constituting a form of mass surveillance.20 This is the core fear that animates public resistance to LFR, which is seen as a tool for constant, indiscriminate monitoring rather than targeted investigation.9

2.3 Technical and Operational Risks

Beyond the philosophical and rights-based concerns, FRT systems present significant technical and operational risks that can have severe real-world consequences.

Algorithmic Bias and Discrimination
One of the most well-documented and damaging flaws of FRT is algorithmic bias. Numerous independent studies, including those by the U.S. National Institute of Standards and Technology (NIST), have consistently found that many FRT algorithms are significantly less accurate when identifying people of colour (particularly women of colour), women, and the elderly, compared to their performance on middle-aged white men.20 Some studies have found that Asian and African American individuals can be up to 100 times more likely to be misidentified by certain algorithms than white men.22
This is not merely a technical issue; it has profound operational and ethical consequences. When used by law enforcement, biased algorithms can lead to false investigative leads, wrongful arrests, and the reinforcement of existing patterns of systemic discrimination.[18] The case of Robert Williams in the United States, who was wrongfully arrested in front of his family based on a flawed FRT match, illustrates the devastating real-world harm that can result from these inaccuracies.[22] This bias often originates from the data used to train the algorithms, which may lack diversity and reflect historical biases in data collection.[20] For a police force operating in a multicultural society like Victoria, deploying a technology with known biases against certain demographic groups poses an unacceptable risk to the principle of equality before the law.

Data Security and Integrity
The databases used by FRT systems contain highly sensitive, immutable biometric information. Unlike a password or a credit card number that can be changed if compromised, a person's facial template cannot.20 This makes biometric databases an extremely high-value target for malicious actors. A data breach could lead to mass identity theft, fraud, harassment, or the creation of "deepfakes" for malicious purposes, with very limited recourse for the affected individuals.20 The 2020 data breach of Clearview AI, which exposed its global client list including Australian police agencies, serves as a stark reminder of the vulnerability of

these systems.25

Accuracy, Consent, and Transparency

Even without bias, the accuracy of FRT is a major concern. System performance can be significantly degraded by real-world conditions such as poor lighting, low-resolution imagery, unusual camera angles, and partial occlusions (e.g., hats, glasses, or face masks).20 Systems can produce both false positives (incorrectly matching two different people) and false negatives (failing to identify a person who is in the database), both of which have serious operational consequences.1

Under Australian law, obtaining consent for the collection of sensitive information is a cornerstone of privacy protection. The *Privacy Act* requires that consent be informed, voluntary, current, and specific.[1] For FRT, especially LFR, meeting this standard is practically impossible. Simply posting signs about the use of the technology is generally considered insufficient to constitute meaningful consent.[1] This creates a significant legal and ethical hurdle for any public-facing deployment. Furthermore, the inherent complexity of the technology makes it difficult for organisations to be fully transparent with the public about how their personal information is being collected, used, and stored, undermining trust and accountability.[1]

2.4 The Australian Legal and Regulatory Framework

Victoria Police does not operate in a legal vacuum. The use of FRT is governed by a patchwork of existing laws and is the subject of intense debate regarding future regulation. Any strategy must be built on a firm understanding of this legal landscape.

2.4.1 The Commonwealth Privacy Act 1988 and the OAIC

The Privacy Act and its Australian Privacy Principles (APPs) are the primary federal legislation governing the handling of personal information by Australian government agencies. As established, biometric information is "sensitive information" under the Act, triggering higher privacy protections.1 APP 3 stipulates that an agency may only collect sensitive information if it is "reasonably necessary" for one or more of its functions or activities, and the individual consents.1 The "reasonably necessary" test is objective and requires a balancing act, weighing the public interest against the intrusion on privacy.1 A less privacy-intrusive means of achieving the same goal must always be considered.1

The Office of the Australian Information Commissioner (OAIC) is the federal regulator responsible for enforcing the Act. The OAIC has demonstrated its willingness to act decisively in this area. Its investigation into Clearview AI found the company had breached the *Privacy Act* by scraping Australians' images from the internet without consent and ordered the company to cease collection and delete the data.[13] The OAIC

also made a formal determination that the Australian Federal Police (AFP) had failed to comply with its privacy obligations through its trial use of Clearview AI, highlighting the agency's failure to conduct a proper privacy impact assessment.[28] These rulings send a clear signal that regulatory scrutiny is high and that procedural compliance is non-negotiable.

2.4.2 The Victorian Charter of Human Rights and Responsibilities Act 2006
As a public authority, Victoria Police has a direct legal obligation under Section 38 of the Charter to act in a way that is compatible with the 20 human rights it protects and to give proper consideration to those rights when making a decision.29 The use of FRT squarely engages multiple Charter rights, including the right to privacy and reputation (Section 13), and potentially the rights to freedom of movement (Section 12), freedom of expression (Section 15), freedom of assembly and association (Section 16), and the right to equality and non-discrimination (Section 8).18
This means that any decision to deploy FRT must be preceded by a rigorous assessment of its impact on these rights. Any limitation of a right must be "reasonable and demonstrably justified" under the limitations clause (Section 7(2)). This requires Victoria Police to demonstrate that the use of FRT is necessary to achieve a legitimate purpose and that the intrusion is proportionate to that purpose.[18] Given the known risks of FRT, particularly regarding bias and mass surveillance, justifying its use under the Charter would be a significant legal undertaking. Failure to do so could render the decision to deploy the technology unlawful.[30] Civil society groups like Liberty Victoria have explicitly stated their view that the use of FRT in public spaces is not a reasonable or proportionate limitation on human rights and may be inconsistent with the Charter.[18]

2.4.3 The Push for Bespoke Regulation: The UTS Model Law for Facial Recognition
There is a broad consensus among civil society, legal experts, human rights bodies, and even some industry players that Australia's current laws are inadequate for governing FRT.16 They were not drafted with this technology in mind and contain significant gaps.21 In response, the University of Technology Sydney's (UTS) Human Technology Institute published a landmark report in 2022 proposing a
Model Law for Facial Recognition.[31]

This proposal is not merely an academic exercise; it represents the most likely blueprint for future federal regulation. The Model Law advocates for a risk-based approach grounded in international human rights law.[31] It would categorise FRT applications into low, elevated, and high-risk tiers.[33] Before any deployment, developers and deployers would be required to conduct a comprehensive "Facial Recognition Impact Assessment" and register it with a regulator.[16] The model law would prohibit the use of FRT in high-risk contexts unless stringent conditions are

met. For law enforcement, this would include satisfying a "minimum seriousness threshold" for the crime being investigated.[16] It would also explicitly prohibit its use for certain purposes, such as identifying journalistic sources or monitoring peaceful protestors.[16] The model proposes giving the OAIC enhanced powers to act as the national regulator.[16]

The intellectual and policy lineage from earlier human rights reports to this model law, and its subsequent positive reception by the Federal Attorney-General, is clear. The 2021 report from the Australian Human Rights Commission first called for a moratorium on high-risk uses of FRT.[35] The UTS Model Law then provided the detailed legislative framework to achieve this. In February 2023, the Attorney-General's

Privacy Act Review report explicitly "referred positively" to the UTS Model Law, endorsing its risk-based approach as a way of striking the right balance.[31] This indicates a clear direction of travel for federal policy. Any internal Victoria Police policy on FRT should therefore be developed with the principles of the Model Law in mind, as a form of "future-proofing" against impending legislation.

2.5 Organisational and Reputational Considerations for Victoria Police

The history of FRT use by Australian police forces is fraught with controversy, which has created a challenging internal and external environment for Victoria Police.

The "Clearview AI Debacle" and its Legacy
In 2020, freedom of information documents revealed that members of Victoria Police's anti-child exploitation team had registered for and trialled Clearview AI.10 This platform is built on a database of billions of images scraped from social media sites without user consent, a practice the OAIC later found to be in breach of the
Privacy Act.[13] While Victoria Police quickly distanced itself, stating the technology was deemed "unsuitable" and was never used in an operational investigation [10], the damage was done. This incident, along with similar revelations about the AFP and other state police forces using tools like PimEyes and FaceCheck.ID [28], has severely eroded public trust.

Internally, these episodes have had a profound impact. A senior manager from Victoria Police's victim ID team has spoken of the "trepidation" and "big resistance" to using AI within the law enforcement community, a direct result of having been "burned pretty badly a few years ago".[13] This has created a cycle where the lack of clear

regulation leads to ad-hoc, controversial trials, which in turn leads to public backlash and regulatory sanction, which then fuels internal resistance and stalls the adoption of potentially beneficial tools. This cycle highlights a critical strategic vulnerability: any move to adopt new FRT in the current legal and social climate is high-risk and will likely accelerate the very calls for restrictive regulation that the force may be concerned about.

The Trust Deficit and the Need for a Social License
The Clearview AI affair and other incidents have created a significant trust deficit. Police leaders across Australia now recognise that a reactive, defensive communications strategy is no longer viable.13 There is an acknowledged need to be "very transparent" about how these technologies are used and to build a "positive public narrative" around their benefits.13 This is an implicit recognition that law enforcement requires a "social license" from the community to operate these powerful technologies. This license is not granted by law alone; it must be earned and maintained through transparency, accountability, and a demonstrated commitment to ethical use.
The incidents also point to a potential internal governance gap. The fact that individual officers or units could trial such powerful and controversial technologies, seemingly without a formal, centralised risk assessment or command-level approval, suggests a need for stronger internal controls and accountability mechanisms.[25]

The following table summarises the key risks and proposes corresponding mitigation strategies for consideration by senior management.

Table 2: Risk and Mitigation Matrix

Risk Category	Specific Risk	Potential Impact on Victoria Police	Proposed Mitigation Strategy
Legal & Human Rights	Breach of Vic *Charter* (Privacy, Equality, Assembly).	Legal challenges, decisions deemed unlawful, reputational damage.	Conduct and publish a comprehensive Human Rights Impact Assessment (HRIA) for any proposed use, demonstrating necessity and proportionality.
Legal & Human Rights	Breach of Cth *Privacy Act*.	OAIC investigation, adverse findings, public loss of confidence.	Develop a strict FRT policy aligned with the APPs. Mandate a Privacy Impact

			Assessment (PIA) for any new system. Prohibit use of illegally sourced databases.
Technical & Operational	Algorithmic Bias and Discrimination.	Wrongful arrests of innocent people, reinforcement of systemic bias, loss of trust with minority communities.	Mandate independent testing of any considered algorithm against NIST standards for demographic accuracy. Implement robust human-in-the-loop protocols.
Technical & Operational	Data Breach of Biometric Database.	Mass identity theft, irreversible harm to citizens, catastrophic loss of public trust.	Enforce stringent data security standards (encryption, access controls). Favour solutions that minimise data retention and centralisation.
Reputational & Organisational	Public Backlash / Loss of Social License.	Political pressure to ban the technology, reduced community cooperation, damage to VicPol brand.	Proactive, transparent engagement strategy. Public consultation *before* deployment. Clear, accessible public-facing policies.
Reputational & Organisational	Unauthorised / Unmanaged Use by Officers.	Repeat of "Clearview AI" incident, undermining of command authority, legal and reputational liability.	Implement a centralised governance body for all AI/FRT procurement and use. Mandate comprehensive training and certification for all

			users.

Part 3: Technological Evolution and Future Capabilities (2023-2024)

3.1 Introduction to the Technological Frontier

While the risks and regulatory challenges are significant, the pace of technological advancement in FRT is relentless. The capabilities of these systems are evolving rapidly, driven by breakthroughs in AI and machine learning. The global FRT market, valued at $5 billion in 2022, is projected to grow to $19 billion by 2032, signalling massive investment and innovation.[38] This section surveys the most significant developments from the last two years and explores the new policing paradigms they might enable.

3.2 Recent Advances in Core FRT Algorithms

The performance of FRT systems is fundamentally determined by the power of their underlying algorithms. Recent research has focused on improving accuracy, efficiency, and robustness.

Improved Accuracy and New Architectures
In controlled, ideal scenarios, the best algorithms now achieve accuracy rates exceeding 99%.38 This improvement is being driven by a move beyond traditional Convolutional Neural Networks (CNNs). A key trend is the development of hybrid architectures that combine the strengths of CNNs with Vision Transformers (ViTs).40 ViTs are adept at modelling global relationships within an image, and when combined with the local feature extraction capabilities of CNNs, they can produce more robust and accurate results.40
Another significant development is the creation of highly efficient, lightweight models designed for "edge" deployment (i.e., running on devices like mobile phones or smart

cameras rather than a central server). Models like EdgeFace, a top performer at the 2023 Efficient Face Recognition Competition, can achieve state-of-the-art accuracy with a fraction of the computational power and memory of larger models.[40] Furthermore, new approaches using Contrastive Language-Image Pretraining (CLIP) models, which learn relationships between images and text, are showing promise in reducing the rate of false positives in real-world deployments.[42]

The Rise of Synthetic Data

A major shift in the field is the increasing use of synthetically generated facial data for training AI models.43 This approach has several advantages. It can help mitigate the significant privacy and ethical concerns associated with scraping billions of real images from the web without consent.44 It also allows researchers to create vast, perfectly balanced datasets, which is a crucial strategy for reducing the demographic and racial biases that plague models trained on skewed real-world data.43 While models trained purely on synthetic data still tend to underperform those trained on real data, the technology is rapidly improving and is a key focus of major research conferences like CVPR.43

3.3 Overcoming Persistent Operational Challenges

Much of the recent research and development has been squarely aimed at solving the practical problems that have historically limited FRT's effectiveness in real-world policing scenarios.

Low-Light and Poor Illumination

Poor lighting is a major cause of FRT failure. However, research published in 2023-2024 has demonstrated novel techniques to overcome this. One promising approach involves using a multi-stage process where a specialized network, such as a Deep Retinex Decomposition Network (DRDN), is first used to intelligently enhance the low-light image—brightening features and reducing noise—before it is passed to the main recognition algorithm. This pre-processing step has been shown to dramatically improve performance, with some studies achieving over 80% recognition accuracy in very challenging low-light conditions.46

Occlusions and Pose Variation

The COVID-19 pandemic highlighted the challenge posed by facial occlusions like masks. Recent research, presented at leading conferences like CVPR, has focused on developing algorithms that are robust to such occlusions.48 These methods work by focusing on the visible parts of the face, using multi-scale feature extraction to capture both fine-grained local details and the overall global structure, and paying special attention to key facial points (e.g., around the eyes) that are less likely to be obscured.48 Similarly, to combat issues with non-frontal poses, 3D facial models are proving to be inherently more robust than 2D systems, as they can model the geometry of a face and are less affected by changes in viewing angle

or lighting.26

Low-Resolution Imagery

A common problem for law enforcement is that images from long-range CCTV are often of very low resolution. A 2024 study detailed a new method that uses bilinear pooling and multi-scale feature networks to significantly improve recognition on low-resolution images. This technique achieved a remarkable 54% accuracy rate on images as small as 15x15 pixels, a task that would be impossible for older systems.53

3.4 Emerging Use Cases and Future Policing Paradigms

These technological advancements are not merely incremental; they have the potential to enable entirely new modes of policing, which will in turn raise new and more complex ethical questions.

"Cold Case" Revolution

The combined improvements in handling aging, low-quality historical footage, and varied poses could enable a systematic re-analysis of unsolved major crimes.12 Victoria Police could potentially create a dedicated "cold case" FRT initiative, running historical evidence from unsolved homicides, sexual assaults, and other serious offences against current and historical databases to generate new leads that were previously impossible to find.

Real-time Situational Awareness and Officer Safety

While the deployment of general LFR for public surveillance remains highly controversial, the advent of efficient edge computing models opens up a different possibility. An OIFR-style application running on an officer's device or in-car computer could potentially provide real-time, highly localized alerts. For example, it could identify if a person the officer is approaching is on a specific watchlist for having a history of violent assaults on police or is the subject of an active arrest warrant for a violent offence. This shifts the paradigm from post-event investigation to pre-emptive officer safety intelligence. However, the potential for "mission creep" and the risk of such a tool being used for routine, non-critical identity checks would need to be managed by extremely strict policy and oversight.

Attribute and Emotion Recognition

The frontier of the technology is moving beyond simple identification. Systems are increasingly being developed to infer attributes such as age and gender, and even to attempt "emotion recognition" or "affective computing".31 While proponents might see applications in, for example, identifying agitation in a crowd before a riot breaks out, this capability is fraught with peril. The science of emotion recognition is highly contested, and the potential for bias and misinterpretation is enormous. Deploying such a technology for pre-crime analysis or crowd control would face extreme legal, ethical, and scientific challenges and would likely be seen as a profound overreach of state power.

The rapid pace of these advancements creates a significant strategic challenge. For

years, a valid criticism of FRT has been its unreliability in real-world conditions. However, the technology is quickly improving to the point where these technical objections are becoming less tenable. As the systems become more accurate and robust against challenges like low light and occlusions, the debate will be forced to shift away from "Does it work?" to the more fundamental question: "Should we use it, even if it works perfectly?" This means that relying on technical shortcomings as a reason to delay forming a definitive policy on FRT is an unsustainable strategy. The core ethical and rights-based questions must be confronted directly, because the technology will likely soon be "good enough" for almost any scenario, forcing a decision based on principles rather than performance limitations.

Furthermore, the trend towards lightweight models and edge computing signals a major architectural shift. The traditional model of sending video to a central server for analysis will be supplemented or replaced by a decentralized network of intelligent devices performing analysis on-board.[40] This will complicate regulatory efforts. A legal framework focused on governing large, centralized police databases may be ill-equipped to oversee thousands of semi-autonomous edge devices. Future policy, both internal to Victoria Police and at the government level, must therefore consider not just

what the technology does, but *where* the processing happens.

Conclusion and Strategic Recommendations

Facial Recognition Technology presents Victoria Police with a profound strategic dilemma. The technology offers a potent suite of capabilities that could significantly enhance public safety and investigative effectiveness. Yet, its deployment is fraught with substantial risks to human rights, privacy, and public trust, all within a legal framework that is struggling to keep pace. The legacy of past controversies has created a climate of caution, both internally and externally. Navigating this complex environment requires a strategy that is not merely reactive, but principled, transparent, and forward-looking.

The analysis in this report demonstrates that the path of ad-hoc experimentation in a regulatory vacuum is unsustainable and counterproductive. It erodes public trust, invites regulatory sanction, and creates internal resistance, ultimately hindering the responsible adoption of even the most beneficial applications. A deliberate and

carefully governed approach is the only viable way forward.

Based on the comprehensive analysis of the operational landscape, the multifaceted risks, and the direction of technological and regulatory change, the following strategic recommendations are proposed for consideration by Victoria Police Senior Management:

1. Establish a Formal and Proactive Governance Framework
Victoria Police should move immediately to establish a centralised governance structure for all emerging AI technologies, including FRT. This should take the form of an internal AI/FRT Governance Board or Steering Committee, with senior representation from operations, legal, policy, and technology divisions. The first task of this body should be to draft a comprehensive internal policy on the assessment, procurement, and use of FRT. This policy should be explicitly and demonstrably aligned with the legal obligations of the Victorian Charter of Human Rights and Responsibilities and the Commonwealth Privacy Act. Critically, it should proactively incorporate the risk-based principles of the UTS Model Law as a "best practice" standard, thereby future-proofing the force against impending national legislation.
2. Prioritise Low-Risk, High-Value, and Defensible Applications
Any initial consideration of new or enhanced FRT capabilities should be strictly focused on applications where the public benefit is clear and compelling, and the privacy intrusion is justifiable and proportionate. This means prioritising reactive (RFR) use cases for the investigation of serious crimes, such as homicide, serious sexual assault, and the identification of victims and perpetrators in Child Sexual Abuse Material. Pursuing highly controversial Live Facial Recognition (LFR) for mass screening of public spaces should be subject to a moratorium until there is an explicit and clear legislative framework in Victoria and a demonstrated public consensus supporting its use. This phased approach will allow the force to build expertise and public confidence with less contentious applications first.
3. Commit to Radical Transparency to Build Public Trust
To overcome the existing trust deficit, Victoria Police must shift from a reactive to a proactive communications posture. This involves a commitment to radical transparency. Before any new FRT system is trialled or deployed, the force should commit to conducting and publishing a comprehensive Privacy Impact Assessment (PIA) and a Human Rights Impact Assessment (HRIA). It should engage in genuine public consultation to explain the proposed use, its benefits, the safeguards in place, and to listen to community concerns. Building a social license to operate requires treating the public as partners in the decision-making process, not as subjects of surveillance.
4. Mandate Rigorous Independent Testing and Robust Human Oversight
Victoria Police must not rely solely on vendor claims of accuracy. Any FRT system under consideration for procurement must be subjected to rigorous and independent testing for both accuracy and demographic bias, preferably against established benchmarks like those from the U.S. National Institute of Standards and Technology (NIST). Furthermore, policy must mandate that FRT is always used as an assistive tool, never as an automated decision-maker. Robust "human-in-the-loop" protocols must be enforced for all applications, ensuring that a

trained human officer always makes the final determination based on a holistic assessment of all available evidence. Comprehensive training and certification should be mandatory for any officer who operates or uses the results of an FRT system.

By adopting this principled, cautious, and transparent strategic pathway, Victoria Police can navigate the complexities of Facial Recognition Technology, positioning itself not as a passive recipient of technological change, but as a responsible leader in ensuring that innovation serves the cause of justice while upholding the values of the community it serves.

Works cited

1. Facial recognition technology: a guide to assessing the privacy risks - OAIC, accessed August 11, 2025, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks
2. Facial Recognition - What it is and how it works - Fraud.com, accessed August 11, 2025, https://www.fraud.com/post/facial-recognition
3. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, accessed August 11, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC8320316/
4. Facial Recognition Technology in Policing and Security—Case Studies in Regulation, accessed August 11, 2025, https://www.mdpi.com/2075-471X/13/3/35
5. 2024 Update on DHS's Use of Face Recognition & Face Capture Technologies, accessed August 11, 2025, https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies
6. Facial Recognition Technology | South Wales Police, accessed August 11, 2025, https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/
7. Live Facial Recognition | Metropolitan Police, accessed August 11, 2025, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/
8. Police use of Facial Recognition: Factsheet - Home Office in the media, accessed August 11, 2025, https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/
9. Members' Viewpoints: The Use of Facial Recognition in Policing - Biometrics Institute, accessed August 11, 2025, https://www.biometricsinstitute.org/wp-content/uploads/Use-of-Facial-Recognition-in-Policing-2025.pdf
10. Victoria police distances itself from controversial facial recognition ..., accessed August 11, 2025,

https://www.theguardian.com/australia-news/2020/jun/19/victoria-police-distances-itself-from-controversial-facial-recognition-firm-clearview-ai
11. Facial Recognition - NYPD - NYC.gov, accessed August 11, 2025, https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page
12. Facial Recognition & Law Enforcement – The Value Proposition - Aware, Inc., accessed August 11, 2025, https://www.aware.com/blog-facial-recognition-used-in-law-enforcement/
13. Aussie police want AI facial recognition to fight child abuse | Information Age | ACS, accessed August 11, 2025, https://ia.acs.org.au/article/2024/aussie-police-want-ai-facial-recognition-to-fight-child-abuse.html
14. Full article: Government surveillance and facial recognition in Australia: a human rights analysis of recent developments - Taylor & Francis Online, accessed August 11, 2025, https://www.tandfonline.com/doi/full/10.1080/10383441.2023.2170616
15. Human Rights Act Factsheet: - Squarespace, accessed August 11, 2025, https://static1.squarespace.com/static/660249bd40e1686fe5cab7d1/t/670508ffde43484469b66288/1728383237037/Right+To+Privacy+2024+Final.pdf
16. Australia needs dedicated facial recognition technology law - Human Rights Law Centre, accessed August 11, 2025, https://www.hrlc.org.au/news/2022-9-27-australia-needs-dedicated-facial-recognition-law/
17. Safeguarding the Right to Privacy | Australian Human Rights Commission, accessed August 11, 2025, https://humanrights.gov.au/about/news/safeguarding-right-privacy
18. An open letter to the city of Melbourne: Facial recognition technology ..., accessed August 11, 2025, https://libertyvictoria.org.au/an-open-letter-to-the-city-of-melbourne-facial-recognition-technology-is-not-the-future-we-want/
19. Human rights concerns as facial recognition technology use expands | Te Kauhanganui Tātai Ture / Faculty of Law - Victoria University of Wellington, accessed August 11, 2025, https://www.wgtn.ac.nz/law/research/our-research/automatic-facial-recognition-technologylegal-and-ethical-issues
20. Ethics of Facial Recognition: Key Issues and Solutions, accessed August 11, 2025, https://learn.g2.com/ethics-of-facial-recognition
21. Call for law reform to regulate facial recognition technology - Lander & Rogers, accessed August 11, 2025, https://www.landers.com.au/legal-insights-news/call-for-law-reform-to-regulate-facial-recognition-technology
22. The Dangers of Facial Recognition Technology - SURFACE at Syracuse University, accessed August 11, 2025, https://surface.syr.edu/cgi/viewcontent.cgi?article=2479&context=honors_capstone
23. Review of Demographic Bias in Face Recognition - arXiv, accessed August 11,

2025, https://arxiv.org/html/2502.02309v1
24. The Civil Rights Implications of the Federal Use of Facial Recognition Technology, accessed August 11, 2025, https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf
25. Australian police are using the Clearview AI facial recognition system with no accountability, accessed August 11, 2025, https://www.swinburne.edu.au/news/2020/03/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability/
26. Past, Present, and Future of Face Recognition: A Review - MDPI, accessed August 11, 2025, https://www.mdpi.com/2079-9292/9/8/1188
27. CMC | Free Full-Text | A Comprehensive Review of Face Detection/Recognition Algorithms and Competitive Datasets to Optimize Machine Vision, accessed August 11, 2025, https://www.techscience.com/cmc/v84n1/61736/html
28. Australian federal police tested controversial facial recognition search engine, FOI documents reveal - The Guardian, accessed August 11, 2025, https://www.theguardian.com/australia-news/2023/oct/24/australian-federal-police-afp-pimeyes-facial-recognition-facecheck-id-search-engine-platform
29. The Charter of Human Rights and Responsibilities, accessed August 11, 2025, https://www.humanrights.vic.gov.au/legal-and-policy/victorias-human-rights-laws/the-charter/
30. Charter of Human Rights Bench Book - BarNet Jade - Judicial College of Victoria, accessed August 11, 2025, https://resources.judicialcollege.vic.edu.au/summary/mnc/2023/JCV/Charter_of_Human_Rights
31. Facial recognition technology: Towards a model law | University of ..., accessed August 11, 2025, https://www.uts.edu.au/research/centres/human-technology-institute/projects/facial-recognition-technology-towards-model-law
32. facial-recognition-model-law-report.pdf - University of Technology ..., accessed August 11, 2025, https://www.uts.edu.au/globalassets/sites/default/files/2022-09/facial-recognition-model-law-report.pdf
33. New report offers blueprint for regulation of facial recognition technology | ScienceDaily, accessed August 11, 2025, https://www.sciencedaily.com/releases/2022/09/220927133419.htm
34. Facial Recognition Regulation Model Law Proposed | SEN.news - No. 1, accessed August 11, 2025, https://sen.news/facial-recognition-regulation-model-law-proposed/
35. Australians Deserve Technology that Protects Human Rights ..., accessed August 11, 2025, https://humanrights.gov.au/about/news/media-releases/australians-deserve-technology-protects-human-rights
36. Human Rights and Technology Final Report, accessed August 11, 2025, https://humanrights.gov.au/sites/default/files/document/publication/ahrc_rightstech_2021_final_summary_1.pdf

37. Facial Recognition Technology: Federal Law Enforcement Agency Efforts Related to Civil Rights and Training - GAO, accessed August 11, 2025, https://www.gao.gov/products/gao-24-107372
38. Facial Recognition Statistics and Facts (2025) - Market.us Scoop, accessed August 11, 2025, https://scoop.market.us/facial-recognition-statistics/
39. five generations of facial recognition usage and the Australian privacy law - Oxford Academic, accessed August 11, 2025, https://academic.oup.com/idpl/article/14/3/247/7697406
40. EdgeFace : Efficient Face Recognition Model for Edge Devices - arXiv, accessed August 11, 2025, https://arxiv.org/html/2307.01838v2
41. Characterizing Face Recognition for Resource Efficient Deployment on Edge - ICCV 2023 Open Access Repository - The Computer Vision Foundation, accessed August 11, 2025, https://openaccess.thecvf.com/content/ICCV2023W/RCV/html/Biswas_Characterizing_Face_Recognition_for_Resource_Efficient_Deployment_on_Edge_ICCVW_2023_paper.html
42. CLIP Unreasonable Potential in Single-Shot Face Recognition - arXiv, accessed August 11, 2025, https://arxiv.org/html/2411.12319v1
43. Second Edition FRCSyn Challenge at CVPR 2024: Face Recognition Challenge in the Era of Synthetic Data - arXiv, accessed August 11, 2025, https://arxiv.org/html/2404.10378v1
44. Enhancing Domain Diversity in Synthetic Data Face Recognition with Dataset Fusion - arXiv, accessed August 11, 2025, https://arxiv.org/html/2507.16790v1
45. How to Boost Face Recognition with StyleGAN? - ICCV 2023 Open Access Repository, accessed August 11, 2025, https://openaccess.thecvf.com/content/ICCV2023/html/Sevastopolskiy_How_to_Boost_Face_Recognition_with_StyleGAN_ICCV_2023_paper.html
46. (PDF) Enhancing Facial Recognition Accuracy in Low-Light Conditions Using Convolutional Neural Networks - ResearchGate, accessed August 11, 2025, https://www.researchgate.net/publication/380040329_Enhancing_Facial_Recognition_Accuracy_in_Low-Light_Conditions_Using_Convolutional_Neural_Networks
47. Track: Poster Session 1 & Exhibit Hall - CVPR, accessed August 11, 2025, https://cvpr.thecvf.com/virtual/2024/session/32083
48. Occlusion-Robust Facial Expression Recognition Based on Multi-Angle Feature Extraction, accessed August 11, 2025, https://www.mdpi.com/2076-3417/15/9/5139
49. D2SP: Dynamic Dual-Stage Purification Framework for Dual Noise Mitigation in Vision-based Affective Recognition. - CVPR, accessed August 11, 2025, https://cvpr.thecvf.com/virtual/2025/poster/32629
50. Facial Recognition Algorithms: A Systematic Literature Review - MDPI, accessed August 11, 2025, https://www.mdpi.com/2313-433X/11/2/58
51. Advancements and Challenges in Face Recognition Technology, accessed August 11, 2025, https://ijcttjournal.org/archives/ijctt-v72i11p110
52. Advancements and Challenges in Face Recognition Technology, accessed August 11, 2025, https://www.ijcttjournal.org/archives/ijctt-v72i11p110
53. Research shows improved facial recognition accuracy and low ..., accessed

August 11, 2025, https://www.biometricupdate.com/202403/research-shows-improved-facial-recognition-accuracy-and-low-resolution-performance
54. Advances in Facial Expression Recognition: A Survey of Methods, Benchmarks, Models, and Datasets - MDPI, accessed August 11, 2025, https://www.mdpi.com/2078-2489/15/3/135