ChatGPT

Facial Recognition Technology in Law Enforcement – Uses, Risks, and Recent Developments

Introduction

Facial Recognition Technology (FRT) has rapidly evolved and is attracting significant interest from law enforcement agencies worldwide. This technology analyzes images or video of human faces to find matches against known identities, enabling police to identify suspects, persons of interest, or victims more efficiently than traditional methods. However, alongside its potential benefits, FRT introduces serious **risks and considerations** – from privacy and human rights implications to questions of accuracy, bias, and public trust. This briefing provides an overview of how police can use FRT in both *reactive* and *live* settings, outlines the key risks and ethical considerations, and highlights recent advances (in the last ~2 years) that are enabling new use cases.

Illustrative depiction of facial recognition technology. Modern FRT can automatically detect and analyze faces from images or live video, then compare them against large databases to find possible matches. Law enforcement agencies are trialing and deploying such systems globally to aid investigations and real-time operations. At the same time, the technology's increased capabilities raise new concerns around mass surveillance and misidentification.

How Law Enforcement Uses Facial Recognition (Reactive vs. Live)

Police forces around the world employ FRT in **several distinct ways**, broadly categorized into reactive (after-the-fact investigative) uses and live (real-time) applications. Key use cases include:

- **Retrospective/Investigative Identification:** After a crime or incident, investigators can run facial recognition on images or footage (e.g. from CCTV cameras, smartphones, doorbell cameras, or social media) to identify suspects or victims [1]. The unknown face is compared against law enforcement databases (such as mugshots taken upon arrest) for potential matches [1]. A trained officer typically reviews any candidate match for verification before proceeding. This greatly speeds up suspect identification – studies found FRT can reduce an ID process from weeks to minutes [2]. It's been used to solve violent crimes (e.g. matching a CCTV image of a bus passenger to a known offender within 48 hours [3]) and to identify missing or deceased persons [4]. All Australian police forces, for example, have access to a national facial recognition system for post-incident investigations [5].

- **Live Surveillance and Watch-list Alerting:** In proactive deployments, **Live Facial Recognition (LFR)** systems scan video feeds from public cameras in real time, comparing faces in the crowd against a watch-list of wanted persons. This is essentially an automated, high-tech "wanted poster" system – historically, officers carried photos of suspects to spot them; LFR automates that task at scale [6]. Cameras (fixed or mobile) analyze each face in their field of view and instantly alert on any match to the target list [7]. This can enable *on-the-spot intervention*: for example, London's Metropolitan Police have used live FRT at large events and busy areas, leading to arrests of individuals wanted for serious crimes who were detected in the crowd [8]. Police agencies emphasize that these deployments are intelligence-led and time-bound (e.g. limited to a specific event or location) and that an officer always double-checks the match and makes the final decision to stop someone [9]. If no match is found, most systems purport to immediately delete the scan data to protect privacy [10]. Nevertheless, live face recognition remains contentious due to its resemblance to mass surveillance. Only a few jurisdictions (e.g. South Wales Police, Metropolitan Police in the UK) have used LFR operationally so far [11], but internal documents suggest police hope to make it *"commonplace"* in the future [12].

- **Field Identification via Mobile Devices:** A newer method involves officers using a mobile app to identify a person during street encounters. Termed **Operator-Initiated Facial Recognition (OIFR)**, this approach lets an officer who has stopped someone (for example, who lacks ID or is unconscious) snap a photograph with a smartphone and query it against backend databases for a match [13]. This can confirm identity *in situ* without transporting the person to a station for fingerprinting. Trials of mobile face-recognition apps have shown positive results in speeding up identity checks [13]. Such tools are still in early stages – for instance, UK police began piloting an OIFR app in 2023 [13]. In Australia, Victoria Police similarly use a system called "iFace" – a network of station-based cameras and software – to scan arrestees' faces against a statewide offender image database for investigative leads [14] [15].

- **Open-Source Intelligence and Person-of-Interest Tracking:** Beyond official mugshot databases, police have also tapped **third-party or open-source facial recognition** services to generate leads. Clearview AI is a notable (and controversial) example – it built an enormous database of ~3–50 **billion** faces by scraping public photos from Facebook, LinkedIn and other sites [16] [17]. Investigators can upload a photo of an unknown suspect (e.g. from crime scene CCTV) and get potential identity matches from Clearview's database of faces (essentially searching the entire internet's photos for lookalikes). This has been likened to putting "everyone into a perpetual police lineup" regardless of criminality [18]. Indeed, Clearview reported in mid-2024 that law enforcement searches using its tool had doubled to **2 million** in one year [19]. Police departments in the United States have used it to identify Jan. 6 Capitol riot suspects and even **victims** of child abuse in illicit videos [20]. However, the same capability also allows rank-and-file officers (or even non-police actors – see later sections) to identify virtually anyone from a single photo, raising major privacy alarms. Victoria Police and other Australian agencies briefly trialed Clearview AI around 2019-20 but ceased after it was deemed unsuitable and likely breached privacy laws [21] [14]. They now publicly state they do not use external photo-scraping systems. Still, the use of FRT to comb *open sources* (social media, public records) is an emerging investigative tactic globally. For instance, U.S. agencies use services like Clearview or PimEyes (a paid public face search engine) for leads, despite ongoing legal challenges.

- **Verification and Access Control:** A more straightforward use of face recognition in law enforcement is identity **verification** – e.g. confirming a detainee is who they claim to be by comparing their face to the photo on record (one-to-one matching) [22]. Police booking systems increasingly include facial scans to prevent aliasing. Some forces use FRT to secure facilities as well – e.g. controlling entry to sensitive buildings by matching an officer's face to an authorized personnel database. While not as publicly debated, these are routine biometric applications to streamline authentication (analogous to using a face scan to unlock a phone).

Global adoption: While the degree of use varies, many police forces worldwide have at least pilot programs for FRT. The United States has dozens of federal and local agencies using it (the GAO found 20+ federal agencies using FRT for investigations [23]). China has integrated live facial recognition extensively into public CCTV networks for surveillance purposes [24]. The UK explicitly rolled out both retrospective and live systems in policing, as described above. Australia to date has used FRT mainly in **reactive** modes (e.g. matching suspects against passport or mugshot databases) and for border security, while **real-time** deployments are not yet routine – though proposals have been made (and trialed in limited fashion, such as a 2020 trial using a phone app with facial recognition to enforce home quarantine during COVID-19 [25]). It's worth noting that public transparency about FRT use is uneven: some departments openly publish policies, while others adopted it quietly. For example, Victoria Police quietly rolled out FRT (the iFace system) at 85 police stations by 2019 without widespread public notice [15]. As we turn to risks, this opaqueness itself has been criticized.

Key Risks and Considerations of Police Use of FRT

While FRT offers powerful capabilities, its use in law enforcement raises **serious legal, ethical, and human rights concerns**. Senior police management must weigh these considerations carefully:

- **Accuracy Limitations & False Matches:** No facial recognition system is 100% accurate. Especially in real-world conditions (poor lighting, low-resolution CCTV, face occlusions), even top algorithms can generate incorrect matches. **Misidentifications can lead to wrongful stops or arrests**, which have already occurred multiple times. In the United States, at least **seven people have been wrongfully arrested** due to police reliance on a faulty face recognition match – and notably, almost all were Black individuals [26] [27]. Studies (including a landmark 2019 NIST study) have consistently found that many FRT algorithms misidentify **people of color** at higher rates than whites [28]. This bias means **racially disparate impacts** – e.g. Black men have been disproportionately subjected to false accusations when an FRT system mistakenly "matches" them to someone else's crime [29]. Even one false arrest is unacceptable, yet cases keep coming: Detroit Police, for example, arrested an *eight-months pregnant* African-American woman at gunpoint based on a false face recognition hit [30]. Such incidents highlight that current FRT *cannot reliably distinguish between many individuals*, particularly across different demographics, and thus **should not be treated as positive identification**. Best practice is to use FRT only as an investigative lead that must be corroborated by other evidence [31]. In practice, however, police officers have sometimes over-trusted the technology – skipping proper verification and leading to grievous errors [32]. This **accuracy problem and human error** in its use pose a significant legal risk (e.g. lawsuits for wrongful arrest) and ethical problem, undermining the presumption of innocence. It has prompted calls in some jurisdictions to ban police FRT outright until reliability and oversight improve [33] [34].

- **Bias and Inequity:** As noted, the technical bias in face recognition (higher error rates for certain races, women, younger/older people, etc.) translates into *real-world discrimination*. A system that is less accurate on minority groups can reinforce existing biases in policing – e.g. more false positives against Black or Asian faces could mean those individuals are more likely to be stopped by an FRT-equipped camera [29] [35]. This not only violates principles of equality and non-discrimination but can further erode trust between police and communities. Even if algorithms improve, the **over-**

surveillance of communities of color (already a concern in traditional policing) may be exacerbated by broad FRT deployment [29]. It's also worth noting that if police use mugshot databases for matching, those databases themselves reflect past over-policing of certain communities, which can bake in a feedback loop (e.g. the system is most likely to identify someone already in the criminal justice system, skewing investigations toward prior offenders or marginalized groups). Ethically, law enforcement agencies need to consider fairness and the potential for **machine-driven profiling**. Independent testing and transparency about bias rates are crucial if FRT is to be used responsibly.

- **Privacy and Mass Surveillance: Facial recognition poses a profound threat to privacy and anonymous public life**. Unlike CCTV that merely records, FRT can *identify* and track people automatically, which could enable pervasive surveillance of citizens' movements and associations. Widespread use of live FRT in public spaces means anyone walking in view of a camera could be identified and logged by police without their knowledge or consent. This has a chilling effect on **fundamental rights** – for example, the right to peacefully protest or attend a sensitive meeting without fear of being recorded and flagged to authorities. Even **off-duty police officers** are not immune: there is rising concern that offenders or hostile actors could use facial recognition tools to identify undercover or off-duty officers, effectively **"de-anonymizing"** them and putting them at risk. In fact, what used to require intensive tailing or informants – identifying a police officer by face – can now potentially be done by anyone with a smartphone. A recent **activist-built website is proof of concept**: the site *"FuckLAPD.com"* allows the public to upload a photo of any Los Angeles police officer and uses FRT to match it against **9,000+ official police headshots** (obtained via public records) to reveal that officer's name and badge number [36] [37]. This was created to hold police accountable, but the *same technique could be used by criminals* to dox officers or identify them outside work. Such capability undermines traditional anonymity protections (like undercover identities or even just the ability for an officer to blend into the public off-duty). More broadly, **pervasive facial surveillance blurs the line between typical law enforcement and generalized monitoring** of the populace. Privacy advocates argue it creates an unacceptable **"perpetual line-up"** of citizens [18], where at any moment your face could be scanned by the government to check if you're wanted for something. This is a drastic expansion of police power with implications for the right to privacy, freedom of expression, and freedom of association [38] [39]. Notably, even some tech companies and legislators have acknowledged this – e.g. the European Union's proposed AI Act would **ban real-time remote facial recognition in public spaces** for law enforcement, citing fundamental rights concerns [40]. In Australia, privacy regulators (OAIC) have similarly emphasized that facial images are **"sensitive information"** under law, deserving higher protection, and that any use of FRT must be necessary and proportionate to a legitimate aim [41] [42]. In essence, deploying FRT broadly could turn a democracy into a surveillance state, so strong legal checks (or outright moratoria) are being urged by human rights experts [43].

- **Legal and Regulatory Issues:** The legal framework around police use of FRT is still catching up. In many jurisdictions, there is *no explicit law* governing it – creating a Wild West scenario [35]. This lack of clear rules means police risk overstepping privacy laws or breaching data protection principles. For instance, Australian authorities discovered in 2021 that Clearview AI's data scraping **violated the Privacy Act**, and the company was ordered to stop using Australians' images [44]. In Victoria and other states, current privacy laws (and the absence of specific biometrics legislation) make any live public facial recognition deployment legally fraught. Some U.S. cities (like San Francisco, Boston) responded to concerns by **banning police use of FRT** entirely [34]. At the federal level, the U.S. has no blanket ban, but bills have been proposed to increase oversight. The U.K. and EU are moving toward stricter regulation – the EU AI Act (expected 2024) will likely heavily restrict police use of FRT, especially live use, unless for serious crimes with judicial authorization [40]. Police leadership must also consider **evidentiary implications**: If an arrest or search was initiated due to a face recognition hit, how will that hold up in court? There have been challenges in U.S. courts about whether defendants can obtain information on how the FRT algorithm works (trade secrets often prevent it), and whether a face match alone constitutes probable cause – generally it should not [31]. Clear policies are needed on retention of facial data, audit logs for each use (to detect misuse), and standards for accuracy. Without a supportive legal framework and robust internal policy, use of FRT could lead to evidence being thrown out or civil liability. Senior management should be proactive in shaping policies that align with emerging laws (e.g. mandating **Privacy Impact Assessments**, community consultation, and pilot evaluations before full rollout). As one Victoria Police official noted, **“clear moral and ethical considerations [are] needed”** around facial recognition use [45] – transparency, accountability, and community consent are key components to legitimately using this technology.

- **Public Trust and Ethical Considerations:** The community’s perception of facial recognition is largely skeptical, especially if implemented without oversight. Past incidents (such as police secretly using Clearview AI without public knowledge [46]) have eroded trust. Any implementation of FRT needs to consider the **social license**: Do the public and their elected representatives consent to this use? There are also **ethical questions** about balancing security benefits against privacy invasion. For example, **necessity and proportionality** should be guiding principles (borrowed from human rights law): use FRT only where it’s **necessary** for a clear public safety need and **proportionate** to that need (i.e. no less invasive alternative exists) [42]. In scenarios like identifying child abuse victims or urgent terror threats, the necessity case is strong – and indeed police are arguing for FRT in these domains [47] [48]. But for general surveillance or petty crime, it’s much harder to justify the intrusiveness. Ethically, there’s also the matter of **informed consent** – people in public generally cannot opt out of FRT scanning, raising the question of whether it’s fair to subject the entire population to this technology for the sake of catching a few. Overuse could lead to a “Big Brother” reputation for the police and significantly harm police-community relations. It’s telling that even within law enforcement, there’s caution: Australian Federal Police officials have called for being *“very transparent”* about any AI use and engaging the public to understand the benefits [49], rather than sneaking it in. Agencies are aware that one misuse scandal can set back the technology’s acceptance by years. **Misuse prevention** is thus critical – policies must bar officers from using FRT for personal reasons or without authorization. (In one recent case, a U.S. police officer **resigned after it was discovered he ran facial searches on people’s social media photos for non-official purposes** [50].) Clear governance, audit trails, and penalties for misuse are needed to reassure both the public and rank-and-file officers that FRT will be used responsibly if at all.

In summary, while FRT could be a valuable tool for law enforcement, it presents **multi-faceted risks**: technological shortcomings (false matches), embedded biases, potential for rights violations, unclear legality, and the possibility of abuse. These risks have led prominent organizations like the ACLU and EFF to deem police FRT “too dangerous” and call for moratoria or bans [33]. Even the United Nations High Commissioner for Human Rights has urged a pause on deploying facial recognition in public spaces until robust safeguards are in place [43]. Any police agency considering FRT must approach it with caution, strict controls, and a willingness to halt or adjust use if the harms outweigh the benefits.

Recent Advances (2023–2025) and New Use Cases

The last two years have seen **significant advancements in facial recognition technology** – as well as creative (and sometimes concerning) new applications emerging. Senior management should be aware of these developments, as they foreshadow what police usage (and misuse) might look like in the near future:

- **Improved Accuracy and Speed through AI:** The core algorithms driving facial recognition continue to get better. In July 2024, NIST's ongoing vendor tests reported *"continued improvement in match rates overall"* across the industry [51] . Leading algorithms today are far more accurate than those of just 5–10 years ago [52] , thanks to deep learning techniques and enormous training datasets. False match rates that once were unacceptably high have been driven down dramatically in controlled tests. Modern systems can handle millions of faces in a database and still return a match in seconds – an essential capability for real-time use. High-performance FRT is also becoming more **efficient**, able to run on edge devices (smartphones, smart cameras) due to optimized AI models. This means police could potentially perform face recognition in the field or on-device, without always needing to send data to a central server. Another technical advance is better face recognition across variations: new AI models are improving at recognizing faces *partially covered by masks*, from extreme angles, or as they age. For example, algorithms have been trained to focus on the periocular region (eyes and eyebrows) to improve accuracy on masked faces – highly relevant post-2020. Large-scale competition between AI vendors (from the US, Europe, and Asia) has also accelerated progress: companies like Clearview AI, SenseTime, Innovatrics, and others all submit algorithms to benchmark against each other [53] . This competitive push means **police now have access to extremely capable FRT engines** – far more capable than early systems. However, increased accuracy, while positive, **does not fully solve the risks** discussed (e.g. bias can still be present, and "better" surveillance is still surveillance). It does, though, open up new potential uses (and temptations) because the tech is more viable than before.

- **Integration with Augmented Reality (AR) – Face Recognition Glasses:** A striking new use case demonstrated in 2024 is the pairing of facial recognition with wearable devices like smart glasses. Two Harvard students made headlines by hacking a pair of Meta's **Ray-Ban Stories** camera-glasses to create real-time face recognition glasses [54] . In their demo, an wearer could look at a stranger and within **seconds** see that person's name and background info, identified via online photos. The system worked by streaming the glasses' camera feed to a computer, where software detected faces and then queried a public face search engine (PimEyes) for matches [55] [56] . Once a likely match was found, the students even automated pulling additional personal data (like home address and phone number) from public records [57] . In one scenario, they greeted a random person by name on a train and referenced her workplace – all learned on the fly, to her shock [58] . This experiment, while done ostensibly to raise awareness of privacy risks, shows that **real-time identification of anyone in public via wearable tech is now feasible with off-the-shelf tools**. The Meta Ray-Ban glasses retail for only a few hundred dollars and, though Meta itself has *not* enabled facial recognition on them (and says it includes LED indicators to warn people of recording [59]), that hardware can be repurposed. From a policing angle, this could mean in the future an officer might have FRT in their sunglasses or bodycam, instantly briefing them if the person they're looking at has warrants or a criminal history. Indeed, Clearview AI reportedly partnered with the US Air Force in 2022 to develop a facial recognition goggles prototype for security at border checkpoints [60] . On the flip side, **AR face recognition could be used by bad actors** (as the students showed) or vigilantes. One can imagine stalkers using smart glasses to identify and follow targets (a nightmare scenario for personal privacy). The rapid identification of people in public by anyone raises new challenges for policing – both in terms of how criminals might abuse it and how police might harness it. This technology went from *“Black Mirror”-esque* to reality within a year, catching regulators off guard. It underlines why robust privacy laws (or at least device-level restrictions) are needed – for instance, to prohibit unconsented face scanning of the public. As of now, **no law explicitly forbids what the Harvard students did**, and as they warned: *“Are we ready for a world where our data is exposed at a glance?”* [61] .

- **Massive Face Databases & Open-Web Recognition:** The scale of data available for facial recognition has exploded. Clearview AI, mentioned earlier, reportedly grew its database from 3 billion images in 2020 to **50 billion** by 2024 [17] – likely by scraping practically every publicly accessible photo on the internet. This means almost *everyone* is in a face recognition database somewhere. Even if police don’t build such databases themselves, they may be able to access them via commercial partnerships or investigations. For example, PimEyes (based on images scraped from the web) is open to the public for a fee and has been used by journalists to identify people in photos. In 2023, Business Insider reported Clearview was used nearly **1 million times** by U.S. police up to that point [62] [63] – indicating frequent reliance on this trove of online images for generating leads. This trend – leveraging **big data of faces** – will likely continue. It enables new use cases like identifying individuals in old crime scene photos or recognizing someone in a crowd *even if they have never been arrested* (by matching to a social media picture). It also enables **retrospective surveillance**: for instance, given stored video from a city center, police could (with the right software) flag all instances a particular person appeared over the past month. Technically, this is now possible if archived video and face databases are linked. The clear danger is mission creep; what starts as a tool to find serious criminals could morph into a tool for monitoring citizens of interest over time. Lawmakers in some countries are scrambling to impose limits – e.g. Illinois’ Biometric Privacy law prohibits collecting individuals’ faceprints without consent, under which Clearview has been sued and forced to limit some access [64] . But the **global picture** is that face data is plentiful and largely unregulated, so police (and private entities) have more information at their fingertips than ever. Senior management should ensure any use of such data complies with local privacy laws and consider the reputational risk: indiscriminate use of a “Google for faces” without safeguards can trigger public backlash (as seen when Clearview use was exposed).

- **Emerging Police Use-Cases: Child Protection and More:** Police are innovating new ways to apply FRT in investigations. A salient example is in **combatting child exploitation**. In 2024, Australian Federal Police and state police argued for using A.I. tools including facial recognition to identify victims in child sexual abuse material (CSAM) [47] . The idea is that by comparing faces in seized illegal content to known missing children or using age-progressed face models, authorities might rescue victims faster. They also want to identify perpetrators in those images by cross-matching to criminal databases. Currently, privacy laws have been a barrier to some of this (due to the Clearview fallout, there is hesitancy), but police leaders are lobbying for clearer permissions given the “tsunami” of online abuse cases [65] . This is an example where **highly sensitive use of FRT** (on minors, in evidence images) could be life-saving – but it absolutely must be done with strict controls and likely judicial oversight because of the severity of privacy intrusion (scanning faces in private illegal content). Another growing use-case is identifying **unconscious or deceased individuals** (for example, using FRT in hospitals to identify an unidentified patient, or after disasters to help with victim identification). This overlaps with public safety and humanitarian roles of police. Advances in face recognition (especially 3D reconstruction and recognition from partial faces) are improving capabilities in these scenarios too.

- **Countermeasures and Adversarial Developments:** As FRT rises, so do efforts to counter it. Technologically, there's work on **adversarial fashion or makeup** that confuses face algorithms (some designers produce shirts or glasses frames that throw off detections). From a policing perspective, this means suspects might deliberately try to foil FRT (beyond simply wearing masks or hoodies). At the extreme, one can use AI to generate **deepfake faces** or wear hyper-realistic masks to impersonate someone else – potentially tricking cameras. While not common, these possibilities remind us that FRT is not unbeatable and can be fooled. On the enforcement side, some agencies are looking at integrating **live body-worn cameras with face recognition** to scan faces during encounters for warrants. None have fully deployed this yet (in part due to real-time technical limits and major pushback – e.g. California banned FRT on police bodycams in 2019). But as hardware gets more powerful (the latest bodycams have better processors), this could resurface as a proposal.

To note a positive technical development: companies are also working on reducing demographic bias in algorithms (through better training data and algorithmic tweaks). NIST's 2022 report noted some newer algorithms show much smaller differences in accuracy across races [66]. If bias can be substantially mitigated, one of the ethical strikes against FRT would be lessened (though not the broader surveillance concerns).

In summary, the period 2023–2025 has shown that facial recognition is *becoming ubiquitous*: easier to implement (even hobbyists can do it), more accurate, and integrated into everyday tech like smartphones, glasses, and social media. This amplifies both the *opportunities* for law enforcement (faster identifications, new investigation techniques) and the *risks* (broader abuse, need for updated policies). A telling quote from an Electronic Frontier Foundation report in Jan 2025 stated: *"Even in a world where the technology is 100% accurate, police still should not be trusted with it… the temptation to fly a drone over a protest and use face recognition to ID the crowd would be too great, and the risks to civil liberties too high"* [67]. That encapsulates the current crossroads: technology is advancing rapidly, but society – and police leadership – must decide where to draw the line to balance safety with rights.

Conclusion

Facial recognition technology is a powerful tool with the potential to help police solve crimes faster, apprehend dangerous offenders, and even prevent harms. In a policing context, it can be seen as an extension of what good investigators have always done – recognizing faces and patterns – now supercharged by AI. However, as this report has detailed, the **capabilities of FRT far outpace our current regulatory and ethical safeguards**. Used without restraint, facial recognition can undermine public trust, infringe on privacy and equality, and even put officers at risk (through misuse by adversaries or overreliance on faulty matches).

For Victoria Police (and any modern police force), the path forward should involve *strategic caution*:
- Develop clear policies and **standard operating procedures** for any use of FRT (e.g. require supervisor approval, use only for serious offenses, prohibit as sole evidence for arrest, etc.).
- Engage with legal authorities and lawmakers to **update laws** so that they provide a framework for FRT use (ensuring it aligns with community expectations and privacy rights).
- Invest in **training** officers on the limitations of FRT – emphasizing it provides *leads* not positive IDs, and

instructing on bias awareness.
- Consider establishing an **oversight mechanism** (internal audit or external board) to review FRT deployments and outcomes (similar to how use of wiretaps or firearms are scrutinized).
- Be transparent with the public about if, how, and why the agency uses facial recognition. Public communication and possibly community consultation can help in maintaining trust. Successful use cases (e.g. finding a dangerous criminal) must be weighed against the broader concern of "surveillance creep."

Finally, stay abreast of technological changes. As outlined, new forms of FRT (from AR glasses to giant databases) are emerging. Policing will need to adapt – both to leverage new tools in a controlled way and to thwart malicious uses of the same tech by others. Senior management should treat FRT as a **double-edged sword**: potentially invaluable in specific scenarios, but carrying high liability if mishandled. In the words of one Victorian police manager, there may be *"trepidation in the law enforcement community"* due to past missteps, yet a recognition that these AI tools are becoming essential in certain domains [68] [69]. The goal should be to find a **responsible balance** – ensuring that any use of facial recognition is lawful, ethical, accurate, and necessary for public safety, and that it never undermines the very rights and freedoms that police are sworn to protect.

Sources:

- Home Office (UK) – *Police use of Facial Recognition: Factsheet* [1] [7] [13]
- Security Vision report on Victoria Police biometrics [15]; Guardian (AU) on Vic Police & Clearview [16] [14]
- ACLU – *Face Recognition and Wrongful Arrests* [26]; EFF – *Face Recognition Harms* [27] [67]
- Sky News – *Harvard students' Ray-Ban facial recognition demo* [57]; Thomson Reuters Foundation – *Smart glasses risks* [56] [70]
- 404 Media – *Public tool to identify LAPD officers* [36] [37]
- The Record – *Clearview AI usage statistics* [19] [50]
- OAIC (AU) – *Guide: Facial recognition privacy risks* [41] [42]
- Information Age (ACS) – *Aussie police on AI and FRT* [45] and additional cited references throughout.

---

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [13] Police use of Facial Recognition: Factsheet – Home Office in the media
https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/

[12] Live facial recognition cameras may become 'commonplace' as ...
https://www.theguardian.com/technology/2025/may/24/police-live-facial-recognition-cameras-england-and-wales

[14] [16] [21] Victoria police distances itself from controversial facial recognition firm Clearview AI | Victoria | The Guardian
https://www.theguardian.com/australia-news/2020/jun/19/victoria-police-distances-itself-from-controversial-facial-recognition-firm-clearview-ai

[15] Biometrics in use by Victoria Police - Security Vision
https://www.securityvision.io/wiki/index.php/Biometrics_in_use_by_Victoria_Police

[17] [19] [50] Law enforcement searches of Clearview AI facial recognition doubled in past year | The Record from Recorded Future News
https://therecord.media/clearview-ai-police-searches-doubled-2023

[18] [20] [62] [63] Clearview AI Scraped 30 Billion Images From Facebook to Share With Police - Business Insider
https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4

[22] [41] [42] Facial recognition technology: a guide to assessing the privacy risks | OAIC
https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks

[23] Law enforcement searches of Clearview AI facial recognition ...
https://www.reddit.com/r/privacy/comments/1dq12a7/law_enforcement_searches_of_clearview_ai_facial/

[24] [38] [39] [40] [43] UN urges moratorium on use of AI that imperils human rights | AP News
https://apnews.com/article/technology-business-laws-united-nations-artificial-intelligence-efafd7b1a5bf47afb1376e198842e69d

[25] Australia's two largest states trial facial recognition software to police ...
https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/

[26] [28] [30] [31] Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True. | American Civil Liberties Union
https://www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true

[27] [29] [32] [33] [34] [67] Police Use of Face Recognition Continues to Wrack Up Real-World Harms | Electronic Frontier Foundation
https://www.eff.org/deeplinks/2025/01/police-use-face-recognition-continues-wrack-real-world-harms

[35] [54] [55] [56] [60] [64] [70] Are face-scanning smart glasses a problem or prophecy? | Context by TRF
https://www.context.news/ai/are-face-scanning-smart-glasses-a-problem-or-prophecy

[36] [37] ‘FuckLAPD.com’ Lets Anyone Use Facial Recognition to Instantly Identify Cops
https://www.404media.co/fucklapd-com-lets-anyone-use-facial-recognition-to-instantly-identify-cops/

[44] [45] [46] [47] [48] [49] [65] [68] [69] Aussie police want AI facial recognition to fight child abuse | Information Age | ACS
https://ia.acs.org.au/article/2024/aussie-police-want-ai-facial-recognition-to-fight-child-abuse.html

[51] [53] NIST facial recognition evaluations showcase accuracy gains, new developers | Biometric Update
https://www.biometricupdate.com/202407/nist-facial-recognition-evaluations-showcase-accuracy-gains-new-developers

[52] Facial Recognition Technology (FRT) | NIST
https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0

[57] [58] [59] [61] Students adapt Meta's smart glasses to dox strangers in real time | Science, Climate & Tech News | Sky News
https://news.sky.com/story/students-adapt-metas-smart-glasses-to-dox-strangers-in-real-time-13227034

[66] Federal NIST study confirms bias of many facial-recognition systems ...
https://www.resetera.com/threads/federal-nist-study-confirms-bias-of-many-facial-recognition-systems-casts-doubt-on-their-expanding-use.160642/latest