Ethical Risks

- **Wrongful Arrests & Bias**
    - Studies show facial recognition systems often have lower accuracy for people of colour, women, and younger individuals2.
    - Misidentification can lead to wrongful arrests, detentions, and reputational harm undermining trust in law enforcement.
- **Privacy Violations**
    - Facial data is biometric and uniquely identifiable. Capturing it without consent in public spaces raises serious privacy concerns.
    - Mass surveillance can chill free speech and peaceful assembly, especially in marginalized communities3.
- **Lack of Transparency**
    - Many deployments occur without public knowledge or oversight. Citizens may not know when or how their faces are being scanned.
- **Function Creep**
    - Systems designed for crime prevention may be repurposed for tracking protestors, monitoring religious gatherings, or enforcing immigration laws.

Recommended Policies for Responsible Deployment

To mitigate these risks, several frameworks have emerged. Here are key principles drawn from global best practices5:

Policy Principle	Description
Transparency & Public Notice	Inform the public when and where facial recognition is used.
Bias Audits & Accuracy Testing	Regularly test systems for demographic bias and publish results.
Strict Use Cases	Limit use to serious crimes or missing persons—not general surveillance.
Human Oversight	Ensure a trained officer reviews all matches before action is taken.
Data Minimization	Delete biometric data immediately if no match is found.
Independent Oversight	Establish ethics panels or watchdogs to monitor deployments and outcomes.
Consent & Opt-Out Mechanisms	Where feasible, allow individuals to opt out or challenge inclusion on watchlists.