9TH INTERNATIONAL STUDENT CONFERENCE ON LOCAL SAFETY AND SECURITY

Faculty of
Criminal Justice and Security

SAFETY AND SECURITY IN ARTIFICIAL INTELLIGENCE ERA: AN ANALYSIS OF AI POLICY DOCUMENTS FROM INDIA, USA, UK, JAPAN & AUSTRALIA

Mr. Muhammed Munavvir P K

(Junior Research Fellow, Parul University)

Introduction

- Modern safety and security majorly depends upon technologies; it's becoming integrating technologies with trained man power.
- Policy documents determine how AI in policing is understood, authorised, and constrained, and how broad legal and ethical principles become operational rules for practice.
- AI is increasingly used in policing through facial recognition, video and audio analytics, predictive tools, automated tracking, and decision support, so governance texts become central for legitimacy and safeguards.
- Governance is challenging because policy guidance is often lengthy, technical, and scattered across instruments and agencies, creating implementation ambiguity.
- AI policing raises high stakes duties on privacy, proportionality, equality, due process, and accountability, so systematic analysis of what policies require is necessary.
- This study compares official policy texts from the USA, UK, Japan, Commonwealth of Australia, and India to map AI policing provisions, dominant framing narratives, and governance safeguards.

Objectives

1. To identify the specific policy sections that are explicitly address AI in policing and law enforcement across the USA, UK, Japan, the Commonwealth of Australia, and India, and to categorise them by use.
2. To analyse and compare the patterns and relationships in how AI policing and surveillance are framed in official policy documents across the USA, UK, Japan, the Commonwealth of Australia, and India.
3. To analyse the ethical and legal framing of AI policing and surveillance in official documents across the USA, UK, Japan, Commonwealth of Australia, and India.

Literature Review

- Policy document analysis is widely considered as a distinctive qualitative approach (e.g. READ technique, computer-assisted qualitative data analysis software-CAQDAS) that views policy documents or texts as instruments of governance rather than neutral guidance (Karppinen & Moe, 2012; Cardno, 2019; Paulus and Lester, 2016).
- Literatures emphasise that robust analysis requires attention to policy context, policy text, and policy consequences, so that researchers can examine the conditions that produced a policy (Kramer et al., 2024).
- Recent comparative work on AI governance has strengthened policy analysis by introducing systematic, feature based approaches for evaluating policy frameworks (Batool et al., 2026).
- Work on smart city & modern policing stresses the need for accountability, procedural fairness and privacy protections to prevent erosion of rights and public trust (Mansoor, 2025; Blount, 2024; Dempsey et al., 2023).
- Literatures also show policy document analysis is also used in quantitative designs when the objective is to track long run policy change and relate it to measurable outcomes. Flander, Meško, and Hacin (2023)

Major Research Gaps

- This creates a clear gap for a cross-national policy document analysis that examines AI policing and police surveillance through the official policy texts.
- Fewer studies systematically analyse how official documents frame legitimacy, define decision authority, and operationalise safeguards such as proportionality, transparency, data governance, oversight, and remedies, but not related to AI and policing directly
- There is also limited country wise comparative work that applies a consistent set of analytic questions to identify similarities and differences in AI policing policy provisions across 5 countries.

Methodology

Study Design:

This study uses a qualitative, comparative policy document analysis with structured ATLAS.ti content analysis to examine how official policy texts across the USA, UK, Japan, Australia, and India frame AI in policing and surveillance, with focus on ethical and legal governance, using a rapid review based, transparent selection procedure.

Data Collection

- A rapid, targeted policy document search was conducted using Google Search as the primary discovery tool.
- To maintain a rapid review boundary; results were screened up to the first four pages for each search string & gathered 33 documents.
- Screening was conducted in three stages: (1) title and source screening to remove irrelevant or non official items, (2) abstract or executive summary screening to confirm relevance to AI governance and policing or surveillance, and (3) full text screening to confirm that the document is in English and connecting AI policing or law enforcement content that could be coded.
- After screening and filtrations N=31 documents considered for the study
- A document metadata was also created.

Data Analysis

- A structured analysis through, computer-assisted qualitative data analysis software (CAQDAS) was applied in ATLAS.ti using primarily deductive coding, with minor refinements during pilot coding.
- Cross country comparisons were also produced using Code Document Tables for theme presence and Code Co occurrence Tables to examine linkages between framings, use cases, and safeguards, with interpretations verified through linked quotations.
- Code Document Tables were used to compare theme presence across countries and document types.
- Code Co occurrence Tables were used to examine how framings were linked to operational use cases and which safeguards were most often connected to specific AI policing applications.

Policy Documents

Country distribution	N=31 (100%)
United Kingdom	10 (32.3)
United States of America	7 (22.6)
India	6 (19.4)
Australia	5 (16.1)
Japan	3 (9.7)

Results

Objective 1. Which AI policing use cases appear explicitly in policy texts

Facial recognition was the most explicitly documented AI policing use case across the corpus, with the highest coding density in the USA and substantial coverage in the UK and Australia, while India showed a more dispersed pattern across predictive policing, automated tracking, video analytics, and decision support, and the Japan subset contained no explicit use case coding in this dataset.

Use case coding by country (counts)

	AUS	IND	JPN	UK	USA
Facial recognition	195	26	0	236	726
Predictive policing	11	56	0	41	210
Automated tracking	0	48	0	4	141
Video analytics	0	76	0	43	37
Decision support	3	34	0	2	57

Main signal: facial recognition dominates across jurisdictions, with wider dispersion in India and the USA.

Results

Objective 2. How oversight and governance connect to AI policing applications

Oversight framing and use case of AI co occurrence shows that policy texts most often connect AI policing to facial recognition through both efficiency and capacity building and public safety narratives, while risk management framing links more strongly to predictive policing and also to automated tracking and video analytics, indicating that different applications are justified through distinct governance narratives in the corpus.

Framing by use case co occurrence (counts)

	Automated tracking	Decision support	Facial recognition	Predictive policing	Video analytics
Efficiency and capacity	27	21	157	58	24
Risk management	35	29	97	70	41
Public safety	32	17	128	39	33

Top links: efficiency with facial recognition, public safety with facial recognition, and risk management with predictive policing.

Results

Objective 3. Ethical and legal governance signals in policy safeguards

Safeguard coding indicates that ethical and legal governance in AI policing policy is anchored most strongly in privacy and data protection, which is especially dominant in the USA and Australia, while transparency is comparatively more emphasized in the UK, India, and Japan; bias and fairness safeguards are most prominent in the USA and UK, and human oversight is uneven across jurisdictions, appearing strongly in Australia and India but absent in the Japan subset within this coded dataset.

Safeguard coding by country (counts)

	AUS	IND	JPN	UK	USA
Privacy and data protection	447	122	49	268	1496
Transparency	106	177	107	357	665
Proportionality and necessity	62	61	56	126	592
Bias and fairness	18	54	73	178	573
Human oversight	144	85	0	55	54

Privacy dominates in the USA and Australia, transparency dominates in the UK, India, and Japan, human oversight is uneven.

Discussion

- **What:** findings: facial recognition dominates, efficiency and public safety are the main justifications, Oversight and governance links more with predictive tools and analytics, safeguards focus on privacy and transparency, human oversight and bias controls are uneven.

- **Why:** AI is moving from testing to routine policing decisions, and legitimacy now depends on clear rules, not just principles. Without strong policy governance, the risks are increasing, biased outcomes, weak accountability, and loss of public trust..

- **When:** Now, Policies should be the first, before scale up becomes irreversible. The right time is before procurement, before integration into workflows, and before high impact deployments like facial recognition, prediction, AI surveillance and investigation assistance become normalised.

- **Where:** Use these technologies only where they have clear public value and clear limits, high volume identification tasks, time sensitive investigations, missing persons support, and evidence review support with proper human oversight.
- Avoid or tightly restrict high risk uses that directly shape liberty outcomes unless strong safeguards and independent oversight exist.

- **Who:** Police and operational commanders for adoption and oversight decisions.
- Legislators and central government for legal basis and binding limits.
- Regulators and oversight bodies for audits, authorisation, and accountability of these technologies.
- Technical teams and vendors for standards, testing, and documentation.
- Courts and grievance bodies for acceptance and remedies.
- Civil society and communities for legitimacy and trust.

- **How:** Develop clear AI policies that define when and how AI can be used in public decision decisions.
- Create AI in policing specific policies that set boundaries, approvals, and accountability for law enforcement use
- Issue practical guidance that is bias aware, culturally appropriate, and aligned with local legal and social norms.
- Provide step by step implementation guidance for police units, including training, standard operating procedures, and auditing
- Separate sessions for data mining and data storage to protect personal information and privacy.
- Apply a harm prevention principle, AI systems must reduce risk and protect rights, not create new harm.

Conclusion

AI is already entering policing through facial recognition, predictive tools, analytics, tracking, and decision support, but safer local policing depends on clear, specific, and enforceable policy rules for how these technologies are used.

What this research shows

- Research purpose: to understand how modern AI technologies are addressed in official policing policy documents, what uses are recognized, and what safeguards are attached to them.
- Main finding: policies speak most clearly about facial recognition and privacy only, there is a clear gap in mentioning other relevant technologies and its integration with policing. Also rules on oversight, bias control, transparency, and human review remain uneven across countries. And among these 5 countries only USA having supremacy in related to technological advancements according to the policy documents.
- For local safety, the goal is not more technology, it is better governed technology, with clear approval authority, use case limits, audit trails, and accessible remedies.
- Local safety implication: AI can strengthen crime prevention, investigation support, and public protection only when it operates within crisp, practical, rights-based policing policies.
- The practical takeaway is a minimum governance package for every AI tool in policing: lawful basis, proportionality, privacy by design, bias testing, named human oversight, transparency, and redress mechanisms, so technology protects people rather than harming them.

Modern AI should not simply make policing faster; it should make local communities safer, fairer, and more accountable.

Thank you

Questions

Muhammed Munavvir P K
munavvirpk862@gmail.com