*Page 915 - 937* **DOI:** *https://doij.org/10.10000/IJLMH.1112145*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 9 | Issue 3**

**2026**

# Digital Rights versus State Control: A Doctrinal and Documentary Assessment of AI Policing and the Freedom of Assembly

APOORWA PANDEY* AND DR. R. P. CHOUDHARY**

## ABSTRACT

*The paper examines the adequacy of existing legal frameworks in governing AI-enabled surveillance technologies, like facial recognition and predictive crowd-management tools, in relation to the right to peaceful assembly. It analyses the implications of these technologies under Article 21 of the International Covenant on Civil and Political Rights and Article 11 of the European Convention on Human Rights, highlighting case studies from the UK, US, and China. The findings indicate that AI policing tools significantly chill assembly rights, which current proportionality and necessity doctrines fail to address. Although the EU AI Act will ban real-time biometric identification in public from February 2025, retrospective surveillance remains categorised as "high-risk," delaying compliance obligations until December 2027. The UK lacks any statutory regulations. The paper advocates for targeted legislation, mandatory human rights impact assessments, and independent algorithmic audits as necessary regulatory measures.*

***Keywords:*** *Freedom of assembly, AI surveillance, Facial recognition, Chilling effect.*

## I. INTRODUCTION

### A. The Problem of AI Surveillance and Collective Action

The right to freedom of peaceful assembly is not merely a formal legal entitlement; it is the structural precondition upon which organised democratic dissent depends. Yet the spaces in which that right is exercised streets, squares, and public gathering points have, over the past decade, been progressively colonised by artificial intelligence–enabled surveillance infrastructure. Facial recognition systems capable of identifying individuals in real time, unmanned aerial vehicles equipped with high-resolution imaging, predictive crowd-management algorithms, and automated social media monitoring tools now constitute a routine feature of the law enforcement response to public protest in a significant and growing number

* Author is a Research Scholar at Dr. C. V. Raman University, Kota, Bilaspur, Chhattisgarh, India.
** Author is the Dean of the Faculty of Law and Associate Professor at Dr. C.V. Raman University, Kota, Bilaspur, Chhattisgarh, India.

 [ISSN 2581-5369]

of jurisdictions. The legal frameworks governing these technologies have not kept pace with their operational deployment.

This paper investigates a specific and underexamined tension: the relationship between AI-enabled policing tools and the right to freedom of peaceful assembly as protected under international human rights law and domestic constitutional instruments. The central research problem is whether existing legal doctrines proportionality, necessity, and legality are structurally capable of constraining AI surveillance in protest contexts, or whether the distinctive operational characteristics of these technologies their opacity, scalar reach, and capacity for predictive profiling generate harms that conventional doctrine cannot adequately address.

### B. Theoretical Framework

The paper operates within the normative architecture of international human rights law, anchoring its analysis in Article 21 of the International Covenant on Civil and Political Rights (ICCPR)[1] and Article 11 of the European Convention on Human Rights (ECHR).[2] These provisions are supplemented by the UN Human Rights Committee's General Comment No 37, which furnishes authoritative interpretive guidance on the scope and permissible limitations of the assembly right, including in surveillance contexts.[3] The paper additionally draws upon the regulatory framework established by Regulation (EU) 2024/1689 the EU Artificial Intelligence Act and upon constitutional and statutory instruments in the United Kingdom and the United States as comparator jurisdictions.[4]

The paper's theoretical orientation is informed by chilling effect doctrine: the proposition, developed principally within First Amendment jurisprudence and increasingly recognised in European human rights law, that the anticipatory deterrent impact of state surveillance upon expressive conduct may itself constitute a rights violation, independent of any concrete enforcement action, a doctrine examined in full in Section 2.3 below. The Court of Appeal's

[1] *International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), UN Doc A/6316 (16 December 1966), art 21, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[2] *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No 5 (4 November 1950), art 11, https://www.echr.coe.int/documents/d/echr/convention_ENG.

[3] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37 (17 July 2020), https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDjh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

[4] *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*, OJ L 1689/1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

judgment in *R (Bridges) v Chief Constable of South Wales Police*[5] and the European Court of Human Rights' analysis in *Gillan and Quinton v United Kingdom*[6] serve as doctrinal anchors for this proposition in their respective jurisdictions.

### C. Methodology

The paper adopts a combined doctrinal and documentary methodology, with the documentary component comprising systematic analysis of civil society reports, parliamentary records, judicial decisions, and government-published impact assessments relating to AI policing deployments at protest events; no primary data was collected, and the methodology is documentary case study analysis rather than empirical research in the social-scientific sense.

The paper analyses the normative architecture under Article 21 of the International Covenant on Civil and Political Rights and Article 11 of the European Convention on Human Rights, supplemented by comparative case studies from the United Kingdom, the United States, India, and the European Union. Reference is also made to the People's Republic of China as a limiting-case illustration not as a full comparator jurisdiction to demonstrate the outer boundary of what AI surveillance infrastructure operating without independent legal oversight may produce.

### D. Contribution and Structure

This paper contributes three original analytical interventions to the literature. First, it interrogates systematically and doctrinally whether the standards of proportionality and necessity can serve to limit AI surveillance at public gatherings, a lacuna in scholarship that has tended to address facial recognition and predictive policing in isolation rather than in direct relation to assembly rights. Second, it uses documentary case study evidence drawn from AI policing deployments at protest events to assess actual human rights impacts across jurisdictions with materially different regulatory frameworks. Third, it evaluates the EU AI Act's regulatory architecture including its prohibited practices, high-risk designations, and the implementation delays introduced by the AI Omnibus package as both a model for and a warning about the limits of purpose-specific AI governance.

## II. CONCEPTUAL AND THEORETICAL FRAMEWORK

### A. AI Policing as a Modality of Power

AI policing is not merely the next step in evolving surveillance. It is a fundamentally different

[5] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

[6] *Gillan and Quinton v United Kingdom*, App No 4158/05, (2010) 50 EHRR 45, https://hudoc.echr.coe.int/eng?i=001-96585.

 [ISSN 2581-5369]

type of threat to our ability to assemble. To understand why we must go beyond the typical critiques of surveillance. In Discipline and Punish, Foucault helps us understand the function of a surveillance system. Its aim is not to make prisoners visible to a guard. The goal is to make prisoners visible to themselves so that they learn to control themselves. It is the system that is truly self-sufficient and requires a prisoner to adopt the mental state that they could always be being watched. The goal of today's AI surveillance systems is to completely eliminate the resource constraint that has traditionally limited surveillance. To do this, they must be built to operate continuously and at scale to incorporate the panoptic logic Foucault describes. [7]

Today's surveillance systems do more than record actions. They predict behaviour and allocate resources to intervene accordingly. The threat this poses to the right of assembly is clear. Individuals may be profiled, targeted, and subjected to intervention not because of anything they have done, but because of predictive modelling and perceived risk.

### B. The Accountability Gap

The diffusion of responsibility when using automated systems to make decisions presents a particularly difficult challenge for legal accountability. When a human officer makes a decision to stop, photograph, or detain a protestor, a legal subject exists, and accountability mechanisms can be applied. When a decision is made to stop, photograph, or detain a protestor, and the same decision is made by an algorithm, responsibility is spread among the system's designers, the procuring agency, the political authority, the officer, and the act decision. This condition, which is described in the philosophy of technology literature, is called the "problem of many hands." It is a situation in which the attribution of individual culpability is encountered by the law due to a lack of accountability. [8] This problem is further complicated by the phenomenon Frank Pasquale has called the "black box" problem.[9] Due to the lack of transparency of automated decision-making systems to external scrutiny, be it courts, affected individuals, or independent oversight bodies, accountability is impossible. When a system's decision-making processes are so secret that even the system's operators cannot understand it, the law's requirement to make a reasoned, reviewable decision is violated. The consequences are far-reaching. For example, a court cannot determine if surveillance is the least restrictive means of achieving a legitimate purpose if the mechanism which identifies targets of the measure remains unknown.

[7] Foucault, Discipline and Punish, 195–228.
[8] Nissenbaum, "Accountability in a Computerised Society," 25–42, https://doi.org/10.1007/BF02639315.
[9] Pasquale, Black Box Society, 1–18.

 [ISSN 2581-5369]

### C. The Chilling Effect and Categorical Targeting

The chilling effect doctrine holds that state surveillance can constitute a rights violation through its deterrent impact upon protected conduct, independently of any concrete enforcement action against a specific individual, a proposition originating in United States First Amendment jurisprudence in *Laird v Tatum* and progressively received into European human rights law through *Gillan and Quinton v United Kingdom* and *R (Bridges) v Chief Constable of South Wales Police*.[10] AI surveillance generates chilling effects structurally more severe than conventional policing for three reasons: its scalar reach deters all present rather than those individually observed; its data retention capacity makes the deterrent effect temporally unbounded; and its categorical targeting logic deters individuals based on algorithmic profile rather than individual conduct, which is fundamentally incompatible with the individualised assessment that Articles 21 ICCPR and 11 ECHR presuppose.[11] Most critically, those most deterred by AI surveillance individuals who choose not to attend protests at all — are structurally invisible to existing doctrine, generating no record and bringing no claim, which is precisely why legislative prohibition rather than judicial review is the only adequate remedy.[12]

## III. DOCTRINAL ANALYSIS OF FREEDOM OF ASSEMBLY

### A. The International Framework: ICCPR Article 21

Article 21 of the ICCPR provides that the right of peaceful assembly shall be recognised, and that no restrictions may be placed upon its exercise other than those "imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others."[13] The provision's structure is deliberate: the right is stated first as a positive recognition, and the permissible limitations are enumerated exhaustively and interpreted restrictively.

The UN Human Rights Committee's General Comment No 37 (2020) the most authoritative

[10] *Laird v Tatum* 408 US 1 (1972), 11–13; *Gillan and Quinton v United Kingdom*, App No 4158/05, (2010) 50 EHRR 45, [64]– [65], https://hudoc.echr.coe.int/eng?i=001-96585; *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [88]– [89], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

[11] Zuboff, Age of Surveillance Capitalism, 233–235; Pasquale, Black Box Society, 14–17; UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [23], https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDjh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

[12] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [23]; *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [88].

[13] *International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), UN Doc A/6316 (16 December 1966), art 21, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

and comprehensive interpretation of Article 21 establishes several propositions of direct relevance to AI policing contexts.[14] The Comment affirms a presumption in favour of the holding of assemblies; requires that restrictions constitute the least intrusive means available; and addresses the position of participants who face surveillance in connection with their attendance at protests. The Comment's position that participants must be able to attend assemblies without fear of unjustified monitoring or subsequent reprisal carries significant implications for AI policing tools that generate persistent biometric records of protest attendee's records that may be retained, cross-referenced, and operationally deployed well beyond the immediate context in which they were captured.[15]

Critically, General Comment No 37 confirms that the legality requirement under Article 21 demands not merely a formal legal basis but law of sufficient quality: it must be publicly accessible, formulated with adequate precision, and provide effective safeguards against arbitrary application.[16] This "quality of law" standard is exacting; as the analysis in **Section 3.3** demonstrates, it is a standard that many contemporary AI policing deployments fail to satisfy.

### B. The European Framework: ECHR Article 11

Article 11(1) ECHR guarantees the right to freedom of peaceful assembly and to freedom of association. Article 11(2) permits restrictions only where they are "prescribed by law," pursue one of an exhaustively enumerated set of legitimate aims national security, public safety, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others and are "necessary in a democratic society" in pursuit of that aim.[17]

The European Court of Human Rights has developed a substantial body of jurisprudence under Article 11. In *Gillan and Quinton v United Kingdom*, the Court though deciding primarily under Article 8 held that stop-and-search powers exercised against individuals attending a protest lacked the quality of law required by the Convention, in that they conferred a latitude of discretion upon police that was insufficiently circumscribed by procedural safeguards.[18] The Court's reasoning is directly applicable to AI policing contexts: a system that generates

[14] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37 (17 July 2020), https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDjh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

[15] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [30]– [34].

[16] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [36]– [37]; *Gillan and Quinton v United Kingdom*, App No 4158/05, (2010) 50 EHRR 45, [76], https://hudoc.echr.coe.int/eng?i=001-96585.

[17] *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No 5 (4 November 1950), art 11, https://www.echr.coe.int/documents/d/echr/convention_ENG. **[URL NOTE: as per fn 2.]**

[18] *Gillan and Quinton v United Kingdom*, App No 4158/05, (2010) 50 EHRR 45, [76]– [77], https://hudoc.echr.coe.int/eng?i=001-96585.

biometric records of protest attendees pursuant to general policing powers without specific legislative authorisation, articulable standards, or meaningful supervisory oversight fails the prescribed-by-law requirement on materially identical grounds.

In *Kudrevičius and Others v Lithuania*, the Grand Chamber affirmed that Article 11 imposes not only a negative obligation upon states to refrain from unjustified interference with assembly rights, but a positive obligation to take reasonable and appropriate measures to enable lawful assemblies to take place.[19] This positive dimension of the Article 11 duty is engaged by AI surveillance in a manner not previously examined in the Court's jurisprudence: where AI policing tools generate a chilling effect that dissuades individuals from exercising assembly rights, a state's failure to constrain those tools may itself constitute a breach of the positive obligation to facilitate peaceful assembly a proposition with significant implications for regulatory adequacy that existing doctrine has not yet fully resolved.

### C. The Three-Part Limitation Test: Legality, Legitimacy, and Necessity

Both the ICCPR and ECHR frameworks mandate a three-part test for restrictions on assembly rights, focusing on legality, legitimate aims, and necessity with proportionality. The R (Bridges) v Chief Constable of South Wales Police case highlighted unlawful police actions concerning automated facial recognition due to unclear legal standards, inadequate data protection assessments, and breaches of the Data Protection Act 2018. This Act aligns with the EU's Law Enforcement Directive, clarifying that it governs police facial recognition over GDPR.[20] While the legitimacy requirement often supports public safety, issues arise during necessity and proportionality assessments, especially with AI data capture methods that lack transparency. The Supreme Court's ruling in DPP v Ziegler calls for stringent proportionality evaluations, but challenges such as lack of transparency and poor targeting hinder judicial review, highlighting the need for comprehensive legal reforms.[21]

## IV. AI POLICING TECHNOLOGIES IN PROTEST CONTEXTS

### A. Facial Recognition Systems

Live facial recognition (LFR) captures facial images via CCTV or dedicated cameras, creating biometric templates to match against watchlists in real time. Its use in protests is notable for

[19] *Kudrevičius and Others v Lithuania*, App No 37553/05, ECHR 2015 (Grand Chamber, 15 October 2015), [149]–[165], https://hudoc.echr.coe.int/eng?i=001-158910.
[20] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [199]– [221], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html; *Data Protection Act 2018* (UK) pt 3; *Directive (EU) 2016/680*, OJ L 119/89, art 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.
[21] *Director of Public Prosecutions v Ziegler and Others* [2021] UKSC 23, [2022] AC 408, https://www.bailii.org/uk/cases/UKSC/2021/23.html.

 [ISSN 2581-5369]

identifying individuals without suspicion or consent, often based on broadly defined watchlists. The UK, especially the Metropolitan Police, has been actively deploying LFR since 2020, potentially scanning about one million faces annually. Legal challenges, like R (Bridges) v Chief Constable of South Wales Police, highlight its vulnerabilities in absence of specific legal frameworks.[22] In China, the "Sharp Eyes" program connects around 600 million surveillance cameras, illustrating the extensive political monitoring capabilities of LFR. Additionally, accuracy concerns exist, particularly for marginalised demographics, with recent data indicating higher false positive rates for darker-skinned individuals.[23]

### B. Predictive Policing Algorithms

Predictive policing tools, using statistical and machine-learning models, analyse historical crime data, demographics, and geography to generate risk scores for individuals and locations. These tools have been used to identify potential disorder participants at protests, facilitating pre-emptive intelligence and resource allocation. In the U.S., tools like PredPol (now Geolitica) faced criticism for racial bias and were reportedly discontinued by the LAPD around 2020-2021 due to civil liberty concerns. [24] Such algorithms often reflect past policing biases, leading to further inequality. In the U.K., Durham Constabulary's Harm Assessment Risk Tool (HART) aids custody decisions but has faced scrutiny regarding accuracy and fairness, though its judicial review status in protest contexts remains uncertain. [25]

### C. Drone and Aerial Surveillance

Unmanned aerial vehicles equipped with high-resolution imaging, thermal sensors, and in some jurisdictions facial recognition payloads have been increasingly deployed at protest events. Their operational advantages persistent coverage, geographic flexibility, and visual access to large outdoor gatherings render them particularly effective for monitoring demonstrations that cannot be comprehensively observed from fixed ground infrastructure.

---

[22] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [85]– [90], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

[23] IPVM Team, "China Public Video Surveillance Guide: From Skynet to Sharp Eyes," IPVM, 14 June 2018, https://ipvm.com/reports/sharpeyes; Chen, "Surveillance on the Moon? China to Take Its Mass Camera Network to Outer Space," *South China Morning Post*, 4 March 2024, https://www.scmp.com/news/china/science/article/3254054/skynet-20-china-plans-bring-largest-surveillance-camera-network-earth-moon-protect-lunar-assets.

[24] Bhuiyan, Johana. "LAPD Ended Predictive Policing Programs Amid Public Outcry: A New Effort Shares Many of Their Flaws." *Guardian*. 8 November 2021. https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

National Institute of Justice. "Predictive Policing Model in Los Angeles, Calif." *CrimeSolutions*. Posted 28 November 2022. https://crimesolutions.ojp.gov/ratedprograms/predictive-policing-model-los-angeles-calif.

[25] Oswald, "Algorithmic Risk Assessment Policing Models," 223–250, https://doi.org/10.1080/13600834.2018.1458455.

 [ISSN 2581-5369]

In the United States, the deployment of a United States Customs and Border Protection surveillance aircraft over Minneapolis during the civil unrest following the death of George Floyd in May 2020 attracted considerable criticism.[26]

### D. Automated Social Media Monitoring

Automated social media monitoring tools aggregate and analyse publicly posted content including text, images, geolocation metadata, and network connection data to identify protest organisers, map social movement structures, and anticipate planned demonstrations. The deployment of such tools raises concerns distinct from those generated by physical surveillance technologies: unlike facial recognition or drone operations, social media monitoring targets the communicative and organisational phase of collective action, intervening before any assembly has physically materialised.

In 2016, the American Civil Liberties Union revealed that a social media monitoring company, Geofeedia, had obtained developer-level data access from major social media platforms and marketed its analytical product to law enforcement agencies as a tool for monitoring protest activity, including demonstrations associated with the Black Lives Matter movement.[27] Following public disclosure, the relevant platforms revoked Geofeedia's access.

In the People's Republic of China, social media monitoring is institutionalised as a component of the broader political surveillance architecture. Platforms operating domestically are legally required to provide authorities with user data upon request, rendering the distinction between private communication and state surveillance effectively null in the protest context and illustrating the outer boundary of what a system constructed without independent legal oversight may produce.

Automated social media monitoring presents a specific and underappreciated threat to the organisational dimension of assembly rights. If the right to freedom of peaceful assembly is to be practically effective rather than formally recognised it must encompass protection for the communicative processes through which assemblies are planned and coordinated. Surveillance of those processes by law enforcement, prior to any assembly taking place, may chill not merely attendance at protests but the organisational capacity that makes collective action possible. This is a harm that existing assembly rights doctrine focused as it predominantly is upon the physical act of gathering is not presently structured to address.

---

[26] Koebler, "CBP Predator Drone Over Minneapolis," https://www.vice.com/en/article/customs-and-border-protection-predator-drone-minneapolis-george-floyd.

[27] Cagle, "Facebook, Instagram, and Twitter Data Access," https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

 [ISSN 2581-5369]

## V. EMPIRICAL DIMENSIONS

### A. Demographic Disparities:

The most authoritative empirical evidence on facial recognition accuracy derives from NIST Interagency Report 8280, which evaluated 189 algorithms from 99 developers using 18.27 million images of 8.49 million individuals drawn from operational databases provided by the State Department, Department of Homeland Security, and FBI.[28] The findings are directly relevant to protest policing: the study documented higher false positive rates for women, African Americans, and particularly African American women, with false positive differentials across demographic groups varying by up to a factor of 7,203.[29] In one-to-many identification the modality most applicable to crowd surveillance American Indian demographics recorded the highest false positive rates.[30] One countervailing finding warrants acknowledgement: the National Physical Laboratory, independently testing the specific algorithm deployed by the Metropolitan Police Service, found no statistically significant demographic performance differences at operational settings, with an 89 per cent correct identification probability and a false alert rate of at worst 1 in 6,000.[31] This indicates demographic impact is algorithm-specific; however, the persistence of disparities across most NIST-tested algorithms establishes demographic harm as a structural rather than incidental feature of the technology as currently deployed at scale.[32]

### B. Misidentification: Documented Cases and Systemic Patterns

The most extensively documented wrongful arrest attributable to facial recognition misidentification is that of Robert Williams, arrested by Detroit police in January 2020 following a false facial recognition match, detained for thirty hours, and subsequently the subject of a landmark 2024 federal settlement prohibiting the Detroit Police Department from making arrests based solely on facial recognition results and requiring independent corroborating evidence before any facial recognition lead can support enforcement action.[33] Nijeer Parks was similarly wrongfully arrested in New Jersey in February 2019 following a

[28] Grother, Face Recognition Vendor Testing (FRVT) Part 3, 1–3, https://doi.org/10.6028/NIST.IR.8280.
[29] Grother, Face Recognition Vendor Testing (FRVT) Part 3, 6–8, https://doi.org/10.6028/NIST.IR.8280.
[30] Grother, Face Recognition Vendor Testing (FRVT) Part 3, 9, https://doi.org/10.6028/NIST.IR.8280.
[31] Home Office, Police Use of Facial Recognition, https://www.gov.uk/government/publications/police-use-of-facial-recognition.
[32] National Institute of Standards and Technology, "Demographic Effects in Face Recognition," https://pages.nist.gov/frvt/html/frvt_demographics.html.
[33] American Civil Liberties Union, "Strongest Police Department Policy on Facial Recognition," https://www.aclu.org/press-releases/civil-rights-advocates-achieve-the-nations-strongest-police-department-policy-on-facial-recognition-technology; American Civil Liberties Union, "*Williams v City of Detroit*," https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest.

 [ISSN 2581-5369]

false match and detained for ten days despite available alibi evidence.[34] Michael Oliver was likewise wrongfully arrested in Detroit in July 2019 on the basis of an erroneous facial recognition result.[35] All three Detroit wrongful arrests involved Black individuals, directly consistent with the demographic accuracy differentials documented in the NIST study.[36] The ACLU confirms at least fourteen people across the United States have been wrongfully arrested due to police reliance on erroneous facial recognition results, with nearly every known case involving a Black person — establishing a structurally consistent failure mode in which human review operates as an automation bias amplifier rather than a meaningful safeguard.[37]

## VI. COMPARATIVE ANALYSIS

### A. The European Union

The European Union represents the most developed regulatory framework for AI policing globally, and the only jurisdiction to have enacted comprehensive, binding AI-specific legislation with direct application to facial recognition in law enforcement contexts. The EU AI Act Regulation (EU) 2024/1689 prohibits real-time remote biometric identification by law enforcement in publicly accessible spaces from 2 February 2025, subject to narrow carve-outs for terrorism, missing persons, and serious crime investigations.[38] Predictive policing based solely on profiling is classified as an "unacceptable risk" practice, prohibited from the same date.[39] Retrospective facial recognition the analysis of previously recorded footage, including footage of protest events is classified as high-risk rather than prohibited, with compliance obligations deferred to 2 December 2027 under the provisionally agreed AI Omnibus.[40]

The implementation gap is compounded by the divergence between regulatory text and operational reality. A 2024 survey identified at least eleven EU member states already operating police facial recognition systems prior to the prohibited-practices provisions becoming enforceable, and as of mid-2025 only three member states had designated the national

[34] American Civil Liberties Union, "*Parks v McCormac*," https://www.aclu.org/cases/parks-v-mccormac; ACLU of New Jersey, "ACLU-NJ and ACLU File Amicus," https://www.aclu-nj.org/press-releases/aclu-nj-and-aclu-national-file-amicus-challenge-wrongful-arrest-due-face-recognition.
[35] American Civil Liberties Union, "More Than a Dozen Wrongful Arrests," https://www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology.
[36] Grother, Face Recognition Vendor Testing (FRVT) Part 3, 6–8, https://doi.org/10.6028/NIST.IR.8280.
[37] American Civil Liberties Union, "More Than a Dozen Wrongful Arrests," https://www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology.
[38] *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*, OJ L 1689/1, arts 5(1)(d), 5(1)(h), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[39] *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*, OJ L 1689/1, art 5(1)(d), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[40] *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*, OJ L 1689/1, Annex III, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

 [ISSN 2581-5369]

competent authorities required under the Act. Sweden introduced legislation in March 2026, Proposition 2025/26:150, proposing to authorise police use of AI systems for real-time facial recognition for serious crimes, with the proposed law entering into force on 1 July 2026, directly exercising the member-state exception clause a development civil liberties organisations have identified as a structural vulnerability in the Act's prohibition architecture.[41] The processing of personal data by police for law enforcement is governed by Directive (EU) 2016/680, known as the Law Enforcement Directive (LED), rather than the General Data Protection Regulation. The LED mandates obligations such as purpose limitation, data minimisation, and enhanced protections for special data categories, particularly biometric data. Specifically, storage limitations apply to biometric records from protest surveillance, and processing biometric data must meet a 'strictly necessary' standard. Compliance is overseen by national data protection authorities, with additional guidance confirming that real-time facial recognition in public areas also falls under LED obligations alongside the AI Act.[42]

### B. The United Kingdom

The United Kingdom illustrates a jurisdiction that judicially recognised the unlawfulness of AI surveillance yet failed to legislate in response. In *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal held live facial recognition unlawful on three grounds: insufficient legal certainty, an inadequate data protection impact assessment, and breach of Part 3 of the Data Protection Act 2018 the operative data protection instrument for law enforcement processing, derived from the EU Law Enforcement Directive (2016/680).[43] The General Data Protection Regulation is inapplicable, as it expressly excludes law enforcement processing under Article 2(2)(d).[44] Despite *Bridges*, Parliament enacted no purpose-specific legislation. The Metropolitan Police resumed deployments under revised internal guidance,[45] and the Home Office confirmed in November 2025 that no statutory framework exists.[46] The Public Order Act

[41] Swedish Government, *Polisens användning av AI för ansiktsigenkänning i realtid*, Proposition 2025/26:150 (3 March 2026), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/polisens-anvandning-av-ai-for-ansiktsigenkanning-i_hd03150/html/.

[42] *Directive (EU) 2016/680*, OJ L 119/89, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680; European Data Protection Board, "Guidelines 05/2022 on Facial Recognition in Law Enforcement," https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition-technology_en.

[43] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [85]– [90], [199]– [221], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html; *Data Protection Act 2018 (UK) pt 3, https://www.legislation.gov.uk/ukpga/2018/12/contents*..

[44] *Regulation (EU) 2016/679 (General Data Protection Regulation)*, OJ L 119/1, art 2(2)(d), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[45] Metropolitan Police Service, "Live Facial Recognition," https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology.

[46] Home Office, Police Use of Facial Recognition, https://www.gov.uk/government/publications/police-use-of-facial-recognition.

2023 expanded protest policing powers without addressing AI surveillance tools.[47] Assembly rights therefore remain governed by instruments never designed for AI policing.[48]

### C. The United States

The United States presents the starkest contrast with the EU framework. No federal legislation specifically governs the use of facial recognition or AI surveillance tools by law enforcement. That regulatory vacuum has deepened materially since January 2025. On 23 January 2025, President Trump signed Executive Order 14179 "Removing Barriers to American Leadership in Artificial Intelligence" which explicitly revoked President Biden's Executive Order 14110 on safe and trustworthy AI, directing all agencies to identify and suspend any policies taken pursuant to the revoked order that conflicted with the new administration's deregulatory orientation.[49] In July 2025, Executive Order 14319 "Preventing Woke AI in the Federal Government" directed federal agencies to procure only AI systems adhering to "Unbiased AI Principles" defined as truth-seeking and ideological neutrality, with no provisions addressing law enforcement surveillance or biometric accuracy.[50] In December 2025, a further Executive Order directed the Attorney General to establish an AI Litigation Task Force to challenge state AI laws inconsistent with federal policy, and directed federal agencies to condition certain grant funding on states having no "onerous" AI laws.[51] In March 2026, the Trump administration published a National AI Legislative Framework, its primary focus being the pre-emption of state-level AI regulation rather than the imposition of federal standards upon law enforcement.[52]

The consequence for assembly rights is direct: at the federal level, no instrument currently constrains law enforcement deployment of AI surveillance tools at protest events. The primary legislative protection operating below the federal level is the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 *et seq*, enacted in 2008.[53] BIPA requires informed written

---

[47] *Public Order Act 2023* (UK) ss 1–11, https://www.legislation.gov.uk/ukpga/2023/15/contents.

[48] *Human Rights Act 1998* (UK) sch 1 arts 10–11, https://www.legislation.gov.uk/ukpga/1998/42/contents; *Data Protection Act 2018* (UK) pt 3, https://www.legislation.gov.uk/ukpga/2018/12/part/3.

[49] Executive Order No 14179, "Removing Barriers to American Leadership in Artificial Intelligence" (20 January 2025) 90 Fed Reg 8741, s 5, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

[50] Executive Order No 14319, "Preventing Woke AI in the Federal Government" (23 July 2025) 90 Fed Reg 35389, https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-prevents-woke-ai-in-the-federal-government/.

[51] Executive Order No 14365, "Ensuring a National Policy Framework for Artificial Intelligence" (11 December 2025) 90 Fed Reg 58499, https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[52] White House, "President Donald J. Trump Unveils National AI Legislative Framework" (20 March 2026), https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/.

[53] *Biometric Information Privacy Act*, 740 ILCS 14/1 et seq (Illinois, 2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

 [ISSN 2581-5369]

consent before the collection or use of biometric identifiers including facial geometry but critically, the Act expressly applies to *private entities* and excludes government bodies from its definition, meaning it does not directly constrain law enforcement facial recognition deployments.[54] In the absence of applicable statutory protection, civil litigation under 42 USC §1983 has emerged as the primary de facto accountability mechanism a litigation-driven model that, as the Williams settlement demonstrates, can produce significant departmental reform but cannot establish binding national standards or subject the broader landscape of AI surveillance to systematic oversight.

### D. India

India presents a distinct regulatory profile: constitutional provisions with considerable latent protective capacity, operating alongside a formally approved and expanding AI surveillance infrastructure in the near-total absence of purpose-specific legislative governance. Article 19(1)(b) of the Constitution of India guarantees the right to assemble peaceably and without arms, and Article 21's protection of personal liberty has, following the Supreme Court's landmark judgment in *K.S. Puttaswamy (Retd.) v Union of India* (2017), been authoritatively interpreted to encompass a fundamental right to privacy.[55]

The Digital Personal Data Protection Act 2023 Act No. 22 of 2023, which received Presidential assent on 11 August 2023 establishes India's primary data protection framework.[56] However, the Act's protective scope is significantly curtailed in law enforcement contexts by two categories of exemption. First, the rights of data principals and obligations of data fiduciaries do not apply to processing by government entities in the interest of the security of the state and public order.[57] Second, exemptions apply to the prevention and investigation of offences.[58] As the PRS India legislative analysis confirms, these exemptions are framed with sufficient breadth to exclude the majority of police AI surveillance activity from the Act's operative requirements a structural limitation that renders the DPDP Act largely ineffective as a constraint upon AI policing at protest events.[59]

---

[54] *Biometric Information Privacy Act*, 740 ILCS 14/10, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[55] *K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1 (Supreme Court of India), https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[56] *Digital Personal Data Protection Act 2023*, Act No 22 of 2023 (India), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[57] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

[58] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

[59] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

 [ISSN 2581-5369]

The existence of a national Automated Facial Recognition System (AFRS) administered by the National Crime Records Bureau (NCRB) is confirmed by official government sources. A Ministry of Home Affairs parliamentary statement of 4 March 2020 confirmed that approval had been accorded for implementation of the AFRS by the NCRB, stating that it would use police records and be accessible only to law enforcement agencies.[60] No purpose-specific legislative authorisation for the AFRS and no independent judicial oversight mechanism governing its use at protest events has been established. The constitutional framework established by *Puttaswamy* furnishes the doctrinal foundation for such a challenge, but no definitive judicial determination of the AFRS's compatibility with fundamental rights had been reported at the time of writing.

### E. Comparative Assessment

The four jurisdictions examined share a common structural feature: in each, the deployment of AI policing tools has outpaced the regulatory frameworks purporting to govern them. The EU has enacted the most sophisticated legislative response but confronts a critical implementation gap that leaves retrospective protest surveillance largely unregulated until at least 2027. The United States, now operating under a federal policy framework that actively seeks to remove barriers to AI deployment and pre-empt state-level restrictions, relies upon constitutional litigation as its primary and structurally inadequate accountability mechanism. India possesses constitutional foundations that are doctrinally adequate in principle, but has approved and deployed a national facial recognition system without the legislative authorisation, independent oversight, or judicial scrutiny that human rights compliance requires.

The comparative analysis reinforces the paper's central argument: purpose-specific legislative intervention, independent algorithmic auditing, and mandatory human rights impact assessments are not merely preferable improvements upon the existing frameworks they are the minimum threshold of regulatory adequacy that no jurisdiction examined has yet reached.

## VII. FINDINGS AND SUGGESTIONS

Legislatures should enact purpose-specific statutes expressly governing AI surveillance at protests, specifying authorisation conditions, permissible data categories, maximum retention periods, and designated supervisory authorities — following the legislative architecture established by Article 5 of the EU AI Act, which prohibits real-time biometric identification in

[60] Ministry of Home Affairs, "Automated Facial Recognition System," https://mha.gov.in.

 [ISSN 2581-5369]

publicly accessible spaces.[61]

Governments should mandate human rights impact assessments prior to any AI surveillance deployment at protests, expressly requiring evaluation of chilling effects upon assembly rights adopting the compatibility assessment mechanism under the New Zealand Bill of Rights Act 1990 as the operative model for rights-proofing at the point of legislative design.[62]

Independent regulatory authorities should require mandatory demographic bias auditing of all AI surveillance systems before protest deployment, with results publicly disclosed — modelled on the bias audit obligations established under the Illinois Artificial Intelligence Video Interview Act 2019, extended to law enforcement contexts with commensurate public reporting requirements.[63]

States should prohibit retention of biometric records generated at protest events in searchable databases absent individualised suspicion of a specific criminal offence, consistent with the storage limitation obligation under Article 4(1)(e) of the Law Enforcement Directive and General Comment No 37's prohibition on unjustified monitoring of assembly participants.[64]

Legislatures should establish a binding statutory corroboration requirement prohibiting any arrest, detention, or search based solely on an AI surveillance result — elevating the *Williams v City of Detroit* settlement standard, currently the strongest existing departmental policy on facial recognition, into a universally applicable legislative obligation.[65]

## VIII. CONCLUSION

The right to peaceful assembly is the structural mechanism through which democratic societies subject power to organised challenge. AI policing technologies operating through opacity, scalar reach, and categorical targeting threaten that mechanism not by prohibiting protest but by making its exercise asymmetrically costly, most heavily for the communities the empirical record shows are most likely to be misidentified.

---

[61] *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*, OJ L 1689/1, art 5, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

[62] *New Zealand Bill of Rights Act 1990*, https://www.legislation.govt.nz/act/public/1990/0109/latest/whole.html; *New Zealand Human Rights Act 1993*, s 7, https://www.legislation.govt.nz/act/public/1993/0082/latest/whole.html.

[63] *Illinois Artificial Intelligence Video Interview Act 2019*, 820 ILCS 42/1, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4212.

[64] *Directive (EU) 2016/680*, OJ L 119/89, art 4(1)(e), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680; UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [23].

[65] American Civil Liberties Union, "Strongest Police Department Policy on Facial Recognition," https://www.aclu.org/press-releases/civil-rights-advocates-achieve-the-nations-strongest-police-department-policy-on-facial-recognition-technology.

 [ISSN 2581-5369]

Existing frameworks were not designed for these harms and have not been adequately adapted. Purpose-specific legislative intervention is not a counsel of perfection. It is the minimum the right demands.

******

**AI-Generated Content Disclosure**

The author has used AI, specifically Claude, for framing and grammatical corrections.

*****

 [ISSN 2581-5369]

## IX. BIBLIOGRAPHY


### International Instruments

1. Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No 5 (4 November 1950). https://www.echr.coe.int/documents/d/echr/convention_ENG.
2. International Covenant on Civil and Political Rights, GA Res 2200A (XXI), UN GAOR, 21st Sess, Supp No 16, UN Doc A/6316 (16 December 1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
3. United Nations Human Rights Committee. *General Comment No 37 on Article 21 of the International Covenant on Civil and Political Rights: Right of Peaceful Assembly*. CCPR/C/GC/37. 17 July 2020. https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDjh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

### Cases

1. *Director of Public Prosecutions v Ziegler and Others* [2021] UKSC 23; [2022] AC 408. https://www.bailii.org/uk/cases/UKSC/2021/23.html.
2. *Gillan and Quinton v United Kingdom*, App No 4158/05, (2010) 50 EHRR 45 (European Court of Human Rights). https://hudoc.echr.coe.int/eng?i=001-96585.
3. *K.S. Puttaswamy (Retd.) and Another v Union of India and Others* (2017) 10 SCC 1 (Supreme Court of India). https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
4. *Kudrevičius and Others v Lithuania*, App No 37553/05, ECHR 2015 (European Court of Human Rights Grand Chamber, 15 October 2015). https://hudoc.echr.coe.int/eng?i=001-158910.
5. *Laird v Tatum*, 408 US 1 (1972).
6. *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (England and Wales Court of Appeal). https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

### Legislation and Regulations

1. Biometric Information Privacy Act, 740 ILCS 14/1 et seq (Illinois, 2008). https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
2. Data Protection Act 2018 (UK) pt 3. https://www.legislation.gov.uk/ukpga/2018/12/contents.
3. Digital Personal Data Protection Act 2023, Act No 22 of 2023 (India). Presidential assent received 11 August 2023. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
4. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA. OJ L 119/89. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.
5. Human Rights Act 1998 (UK). https://www.legislation.gov.uk/ukpga/1998/42/contents.
6. Illinois Artificial Intelligence Video Interview Act 2019, 820 ILCS 42/1. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4212.
7. New Zealand Bill of Rights Act 1990. https://www.legislation.govt.nz/act/public/1990/0109/latest/whole.html.
8. New Zealand Human Rights Act 1993. https://www.legislation.govt.nz/act/public/1993/0082/latest/whole.html.
9. Public Order Act 2023 (UK). https://www.legislation.gov.uk/ukpga/2023/15/contents.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). OJ L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). OJ L 1689/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

 [ISSN 2581-5369]

12. Sweden. *Polisens användning av AI för ansiktsigenkänning i realtid*. Proposition 2025/26:150. Submitted to the Riksdag 3 March 2026. Proposed entry into force 1 July 2026. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/polisens-anvandning-av-ai-for-ansiktsigenkanning-i_hd03150/html/.

13. Washington State. Substitute Senate Bill 6280: Concerning Facial Recognition Services. Enacted 31 March 2020. Codified as RCW 43.05. https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false.

**Executive Orders and Administrative Instruments**

1. United States. Executive Order No 14179, "Removing Barriers to American Leadership in Artificial Intelligence." 20 January 2025. 90 Fed Reg 8741. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

2. United States. Executive Order No 14319, "Preventing Woke AI in the Federal Government." 23 July 2025. 90 Fed Reg 35389. https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/.

3. United States. Executive Order No 14365, "Ensuring a National Policy Framework for Artificial Intelligence." 11 December 2025. 90 Fed Reg 58499. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

**Secondary Sources**

1. ACLU of New Jersey and American Civil Liberties Union. "ACLU-NJ and ACLU National File Amicus in a Challenge to a Wrongful Arrest due to Face Recognition." Press release. 29 January 2024. https://www.aclu-nj.org/press-releases/aclu-nj-and-aclu-national-file-amicus-challenge-wrongful-arrest-due-face-recognition.

2. American Civil Liberties Union. "Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on Facial Recognition Technology." Press release. 28 June 2024. https://www.aclu.org/press-releases/civil-rights-advocates-achieve-the-nations-strongest-police-department-policy-on-facial-recognition-technology.

3. American Civil Liberties Union. "Michigan Father Sues Detroit Police Department for Wrongful Arrest Based on Faulty Facial Recognition Technology." Press release. 13

April 2021. https://www.aclu.org/press-releases/michigan-father-sues-detroit-police-department-wrongful-arrest-based-faulty-facial.

4. American Civil Liberties Union. "More Than a Dozen Wrongful Arrests Due to Police Reliance on Facial Recognition Technology." Updated 2024–2025. https://www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology.

5. American Civil Liberties Union. *Parks v McCormac*. Case page. Ongoing. https://www.aclu.org/cases/parks-v-mccormac.

6. American Civil Liberties Union. *Williams v City of Detroit*. Case page. Settled June 2024. https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest.

7. Bhuiyan, Johana. "LAPD Ended Predictive Policing Programs Amid Public Outcry: A New Effort Shares Many of Their Flaws." *Guardian*. 8 November 2021. https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

8. Cagle, Matt. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Colour." ACLU of Northern California. 11 October 2016. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

9. Chen, Stephen. "Surveillance on the Moon? China to Take Its Mass Camera Network to Outer Space." *South China Morning Post*. 4 March 2024. https://www.scmp.com/news/china/science/article/3254054/skynet-20-china-plans-bring-largest-surveillance-camera-network-earth-moon-protect-lunar-assets.

10. European Data Protection Board. *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*. Adopted 26 May 2023. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition-technology_en.

11. Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Pantheon Books, 1977.

12. Grother, Patrick, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Testing (FRVT) Part 3: Demographic Effects*. NIST Interagency Report 8280. Gaithersburg,

 [ISSN 2581-5369]

MD: National Institute of Standards and Technology, 19 December 2019. https://doi.org/10.6028/NIST.IR.8280.

13. Home Office. *Police Use of Facial Recognition: Factsheet*. London: HM Government, November 2025. https://www.gov.uk/government/publications/police-use-of-facial-recognition.
14. IPVM Team. "China Public Video Surveillance Guide: From Skynet to Sharp Eyes." IPVM. 14 June 2018. https://ipvm.com/reports/sharpeyes.
15. Koebler, Jason, Joseph Cox, and Emanuel Maiberg. "Customs and Border Protection Is Flying a Predator Drone Over Minneapolis." *Vice/Motherboard*. 29 May 2020. https://www.vice.com/en/article/customs-and-border-protection-predator-drone-minneapolis-george-floyd.
16. Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.
17. Metropolitan Police Service. "Live Facial Recognition." Technology overview page. Accessed 2025. https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology.
18. Ministry of Home Affairs, Press Information Bureau (India). "Automated Facial Recognition System Will Facilitate Better Identification of Criminals, Unidentified Dead Bodies and Missing/Found Children and Persons: Shri G. Kishan Reddy." 4 March 2020. https://mha.gov.in.
19. National Institute of Justice. "Predictive Policing Model in Los Angeles, Calif." *CrimeSolutions*. Posted 28 November 2022. https://crimesolutions.ojp.gov/ratedprograms/predictive-policing-model-los-angeles-calif.
20. National Institute of Standards and Technology. "Demographic Effects in Face Recognition." Table last updated 5 March 2025. https://pages.nist.gov/frvt/html/frvt_demographics.html.
21. National Institute of Standards and Technology. *Face Recognition Vendor Test (FRVT) Part 8: Demographic Effects*. NIST Interagency Report 8429. https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf.

 [ISSN 2581-5369]

22. National Institute of Standards and Technology. “Face Recognition Vendor Testing Programme.” https://www.nist.gov/programs-projects/face-recognition-vendor-testing-frvt.

23. Nissenbaum, Helen. "Accountability in a Compterized Society." *Science and Engineering Ethics* 2, no. 1 (1996): 25–42. https://doi.org/10.1007/BF02639315.

24. Oswald, Marion, Jamie Grace, Sheena Urwin, and Geoffrey Barnes. “Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and ‘Experimental’ Proportionality.” *Information and Communications Technology Law* 27, no. 2 (2018): 223–250. https://doi.org/10.1080/13600834.2018.1458455.

25. Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.

26. PRS Legislative Research. “The Digital Personal Data Protection Bill, 2023.” Legislative analysis. Accessed 2024. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

27. White House. “President Donald J. Trump Unveils National AI Legislative Framework.” Press release. 20 March 2026. https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/.

28. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

*****

 [ISSN 2581-5369]