I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

The Regulatory Chasm: Navigating Amorphous Privacy and Facial Recognition Technology in Global Law

Dr. Keshva Nand *
Assistant Professor, Faculty of Law, The ICFAI University, Himachal Pradesh, India

Corresponding Author: Dr. Keshva Nand *

DOI: https://doi.org/10.5281/zenodo.17947323

Abstract

The rapid deployment of Facial Recognition Technology (FRT) has created a legal chasm concerning the protection of "Amorphous Privacy"—the systemic right to anonymity in public space challenged by ubiquitous data collection. This analysis evaluates the divergent regulatory responses to FRT across major global jurisdictions: the rights-centric, structural prohibition model of the European Union (EU); the fragmented, high-liability private litigation model of the United States (US); and the constitutional but state-exempted model of India. Findings reveal a critical failure of traditional legal frameworks to address the cumulative harm of perpetual digital tracking and algorithmic bias. Specifically, the EU's proactive bans contrast sharply with the US's reactive statutory damage model (exemplified by BIPA's massive financial exposure) and India's new DPDP Act, which grants broad public order exemptions for government surveillance. The paper concludes that bridging the regulatory chasm requires a unified, prescriptive governance model centred on mandatory Human Rights Impact Assessments and structural accountability to ensure FRT deployment adheres to the principles of necessity and proportionality.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 19-07-2025
- **Accepted:** 29-08-2025
- **Published:** 31-08-2025
- **IJCRM:**4(4); 2025: 722-729

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Nand K. The Regulatory Chasm: Navigating Amorphous Privacy and Facial Recognition Technology in Global Law. Int J Contemp Res Multidiscip. 2025;4(4):698-701.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Facial Recognition Technology; Amorphous Privacy; Biometric Surveillance; Algorithmic Bias; Privacy Regulation; Human Rights Impact Assessment (HRIA).

1. INTRODUCTION

The proliferation of Facial Recognition Technology (FRT) presents a profound legal challenge rooted in the rapidly evolving nature of digital privacy. Traditional legal standards, often structured to address tangible invasions such as trespass or unreasonable physical search and seizure, struggle to encompass the injury caused by ubiquitous, automated digital data collection. This legal dissonance is captured by the term "Amorphous Privacy," which refers to the complex right that must now integrate legal and technical perspectives to address the cumulative, long-term, and often immaterial effects of modern privacy invasions.[1]

1.1. The Nature of Amorphous Privacy and Legal Inertia

Privacy, in the context of advanced surveillance technology, is recognized globally as an "amorphous and evolving concept". [2] The core legal challenge lies in defining harm when continuous identification and tracking are technically feasible at all times, fundamentally undermining the expectation of anonymity in public space. [3]

The intangible nature of these privacy harms necessitates a strategic shift in legal focus. When sophisticated FRT enables pervasive tracking of individuals, the legal framework must move beyond merely governing specific instances of data misuse toward preventing the systemic chilling effect that persistent surveillance generates.[4] The mere capability of automated tracking, even if data is never actively abused by government or corporate entities, can inhibit civil liberties and political expression. This transformation of public space forces the legal system to explore precedents set for deeply intrusive practices, such as wiretapping or searching smartphones, to determine the threshold of permissibility for biometric surveillance and tracking.[5]

To counter this technological pressure, regulators across the globe, including the authors of the General Data Protection Regulation (GDPR), have endorsed "Privacy by Design" (PbD). This framework promotes a holistic, preventative approach, mandating that privacy challenges stemming from emerging technologies are managed across the entire life cycle of the system and within its context of application.[6]

1.2. The Dual Nature of Facial Recognition Technology (FRT): *Utility vs. Peril*

FRT is a dual-use technology offering significant utility while posing profound risks. On the utility side, the technology provides genuine public benefits, enhancing consumer convenience— such as unlocking personal devices or accessing financial institutions [7] and supporting critical societal safety functions, including law enforcement in identifying suspects in serious crimes or locating missing persons.[8]

However, the peril is equally significant. FRT facilitates mass surveillance, increasing the risk of abuse by governments and corporations seeking to monitor populations.[9] This capability poses a direct threat to civil liberties and the exercise of fundamental rights. The fast pace of FRT development, driven by artificial intelligence and deep learning,[10] guarantees that authoritative legal guidance will struggle to keep pace, especially in jurisdictions without a unified federal framework, such as the United States.[11] This lack of cohesive federal policy creates high regulatory uncertainty for multinational organizations and invites aggressive, financially punitive action from private litigants to define the boundaries of acceptable use.[12] This legal vacuum is not merely an absence of law, but an active force that channels regulatory power into state courts, dramatically altering corporate risk profiles through high-stakes litigation.

1.3. Scope, Methodology, and the Regulatory Chasm

This paper analyzes the complex legal dilemmas surrounding FRT by examining the ethical frameworks governing regulation across major global powers. Jurisprudence regarding violations determination varies significantly: the European Union (EU) endorses deontological ethics (rights-based), the United States (US) largely exhibits a form of universal egoism (market-driven), while core FRT legislation in China valorizes utilitarianism (societal benefit).[13] This divergence explains the current chasm in regulatory outcomes and is essential for understanding the compliance landscape for organizations operating internationally.[14]

2. Technical Capabilities, Performance Gaps, and Data Classification

2.1. Mechanics, Biometric Classification, and Risk

Modern FRT systems operate by utilizing trained artificial intelligence models, specifically deep
neural networks, to extract unique facial features and create a biometric template.[15] These templates are then compared against other images or sets of images to produce a similarity score, allowing for rapid and increasingly accurate identification or verification.[16] The market reflects this advancement, demonstrating robust growth, projected to expand to $7.92 billion in 2025. This growth is fuelled by widespread adoption, including extensive government utilisation by seven out of ten global governments, and high-trust commercial applications, such as the 42% of users who access financial institutions using facial verification.[17] Due to its unique link to permanent identity, biometric data used for automated recognition is classified as "special category biometric data" under regimes like the UK GDPR.[18] This high classification is justified because, unlike other forms of personal data that can be changed, compromised biometric data is immutable.[19] A breach of facial templates represents an irreversible, lifetime identity risk for the individual. [20]

This permanent value means that data protection principles like Storage Limitation, which mandates that personal data should not be kept for longer than necessary, become non-negotiable legal mandates. Any policy or system architecture that encourages indefinite retention or centralised storage of facial templates inherently violates international best practices and dramatically increases the permanent risk exposure for individuals and organisations alike.

The only viable path toward compliance and risk minimisation involves the proactive adoption of temporary or decentralised processing models and robust data destruction regimes.

2.2. The Accuracy Paradox and Algorithmic Bias

The technical capabilities of FRT present an accuracy paradox. In controlled settings, top vendors consistently achieve high benchmarks, with False Negative Identification Rates (FNIR) below 0.15% at a False Positive Identification Rate (FPIR) of 0.001. This performance is comparable to leading iris recognition technologies.[21] Organizations like the National Institute of Standards and Technology (NIST) provide independent evaluations of commercially available technology to assist government and law enforcement agencies in determining how FRT can best be deployed.[22]

However, real-world performance degrades significantly when processing images captured "in the wild".[23] Factors such as inconsistent lighting variations, non-frontal facial positioning, occlusions (masks, glasses), and low-resolution images from surveillance cameras can cause a 0.1% lab error rate to increase drastically, sometimes reaching 9.3%.[24]

This discrepancy creates a significant operational and legal accuracy gap. Law enforcement and public agencies often rely on low-resolution or grainy closed-circuit television (CCTV) images, for which "no publicly available or standardized tests" exist to verify accuracy.[25] Consequently, when FRT is used as the primary, or even sole, piece of evidence linking an individual to a crime, the data being relied upon is derived from systems operating outside proven performance thresholds. This dramatically increases the probability of constitutional challenges based on unreliable evidence and, simultaneously, civil rights litigation based on known biases.[26]

Systemic bias further exacerbates the legal risk. Studies show that facial recognition algorithms are consistently "biased and inaccurate," displaying a higher likelihood of misidentifying people of colour, particularly women of colour.[27] This bias is not merely a technical flaw; it is a legal liability, potentially resulting in unlawful data processing under the GDPR's fairness principle [28] and leading to litigation under U.S. civil rights law.[29]

3. The European Union: The Top-Down, Rights-Centric Regulatory Model

The European Union employs a rights-centric, top-down regulatory model, rooted in a deontological ethical framework that prioritizes individual rights over state or corporate utility.[30] This approach imposes structural and philosophical limits on FRT, primarily through the General

Data Protection Regulation (GDPR) and the new EU Artificial Intelligence Act (EUAIA).

3.1. GDPR's Strict Biometric Requirements

The GDPR classifies biometric data processing as requiring special protection. Consequently, the processing of sensitive biometric data generally requires the data subject's explicit consent.[31] This is a high legal hurdle, requiring that consent be informed, specific, freely given, and unambiguous.

Organisations face inherent difficulty in complying with these rules, as cameras placed in public spaces often gather facial data without the explicit knowledge or consent of those being recorded. This practice directly violates GDPR's core principles of lawfulness, fairness, and transparency.[32]

Furthermore, the known algorithmic biases that cause certain FRT systems to perform poorly when identifying individuals with darker skin tones or women translate into a violation of the GDPR's fairness principle, potentially rendering the data processing unlawful.[33]

The regulatory response to deployments perceived as convenient but rights-invasive has been swift and decisive. For example, when Milan's Linate Airport introduced a "Face-boarding" system, Italian data protection authorities suspended the system, citing "insufficient safeguards" for passengers who had not chosen to participate.[34] This action demonstrates that in the EU, FRT convenience is inherently insufficient justification for processing sensitive data; regulatory actions prioritize legal compliance and rights protection over market efficiency, reinforcing the deontological ethic.[35] Compliance efforts must therefore demonstrate necessity and proportionality for a legitimate public interest, not merely competitive advantage.

3.2. The EUAI Act (EUAIA): Prohibitions and High-Risk Classification

The AI Act introduced structural mechanisms to govern FRT. The use of FRT systems is classified

as "high-risk," which triggers extensive compliance obligations for providers. These mandates include establishing a risk management system, conducting robust data governance to ensure that training, validation, and testing datasets are relevant and sufficiently representative, and implementing human oversight throughout the AI system's lifecycle.[36]

Crucially, the AI Act implements systemic, structural prohibitions designed to address the challenges of Amorphous Privacy head-on. The development or expansion of facial recognition databases by "untargeted scraping of facial images from the internet or CCTV footage" is absolutely prohibited, with no exceptions.[37] This prohibition is a mature regulatory response that bypasses the practical failure of GDPR's explicit consent model in public spaces. By neutralizing the core engine of mass surveillance—the untargeted database—the AI Act makes compliance easier to enforce by shifting the burden from obtaining end-user consent to demanding strict developer data governance.

The use of "real-time" remote biometric identification (RBI) in publicly accessible spaces for law enforcement is also subject to a partial ban and is generally prohibited.[38] Narrow exceptions are permitted only for critically defined scenarios, such as searching for missing persons or abduction victims; preventing a substantial and imminent threat to life or a foreseeable terrorist attack; or identifying suspects in serious crimes like murder, rape, or organized crime.[39]

Furthermore, "post-remote" RBI, where identification occurs after a delay, is only allowed for prosecuting serious crimes and requires mandatory court authorisation.

Table 1: Mapping FRT Regulatory Prohibitions and Exceptions (EU AI Act Focus)

AI Act Prohibition Category	Prohibited Activity	Law Enforcement Exception (Real-Time RBI)	Scope
Unacceptable Risk	Untargeted scraping of facial images from the internet/CCTV for databases.	N/A (Prohibition is absolute)	Creation of databases is banned.
Unacceptable Risk	Inferring emotions in workplaces or educational institutions.	N/A (Except for medical/safety)	Protection against psychological profiling.
High Risk (RBI Default)	Real-Time Remote Biometric Identification (RBI) in public spaces.	Searching for missing persons and abduction victims.	Narrow, rights-justified use.
High Risk (RBI Default)	Real-Time RBI in public spaces.	Preventing a substantial and imminent threat to life/foreseeable terrorist attack.	Public safety emergency use.
High Risk (RBI Default)	Real-Time RBI in public spaces.	Identifying suspects in serious crimes (e.g., murder, rape, organised crime).	Requires court authorisation.

4. The United States: A Patchwork of Regulation and High-Stakes Litigation

In contrast to the EU's proactive, unified approach, the US adheres to a model often characterised by "universal egoism" and a self-regulatory mindset.[41] The US approach has historically been "market first, regulation later" [42], resulting in a legislative environment defined by federal hesitation, fragmented state-level actions, and extremely high liability risks driven by private litigation.

4.1. Federal Hesitation and Legislative Fragmentation

There is currently no comprehensive federal law governing commercial or law enforcement use of FRT in the US.[43] While federal agencies such as the FBI and the US Marshals Service utilise FRT systems [44], Regulation remains a patchwork of federal proposals and state and local statutes.[45] Congressional efforts exist, such as the Facial Recognition and Biometric Technology Moratorium Act of 2023 (S. 681), which proposes restrictions on acquiring and using biometric surveillance systems and grants individuals the right to sue.[46] However, comprehensive federal legislation has yet to pass.

This policy vacuum has led to states filling the regulatory void. Eighteen states have enacted statewide FRT regulations for law enforcement or broad public use.[47] Notably, states like Illinois, Texas, and Washington have passed legislation regulating private entities' collection and use of biometric information.[48]

A complication arises when federal operations utilize non-federal FRT systems, potentially insulating themselves from federal civil liability while relying on data derived from systems that may be violating stringent state privacy mandates.[49] This fragmentation compromises accountability and impacts federal agencies' ability to ensure compliance with privacy laws.

4.2. The Illinois BIPA Liability Model

The most impactful piece of US legislation governing biometrics is the Illinois Biometric Information Privacy Act (BIPA). BIPA establishes comprehensive rules for private entities, requiring informed consent, setting reasonable safeguard and retention guidelines, and prohibiting the profiting from biometric data.[50] Crucially, BIPA grants a private right of action to individuals harmed by violations.

Private litigation, empowered by BIPA, has functionally replaced federal regulatory oversight, generating arguably the world's highest statutory liabilities. The Illinois Supreme Court's decision in *Cothron v. White Castle System, Inc*. established that a separate claim accrues each time an individual's biometric data is scanned or transmitted without BIPA-compliant consent.[51] Given that statutory damages range from $1,000 to $5,000 per violation, systems used for routine daily functions, such as fingerprint timekeeping, can generate liabilities that multiply many times over, leading to what is frequently described as "death by a thousand scans". This economic pressure forces compliance instantly.

Furthermore, the ruling in *Tims v. Black Horse Carriers, Inc*. established a five-year statute of limitations for all BIPA claims.[52] This extended look-back period further compounds the financial exposure, necessitating that businesses treat BIPA compliance as an existential, immediate threat.[53] This model confirms that market forces, when amplified by high statutory damages, can enforce strict data protection standards faster than legislative bodies.

5. The Indian Legal Framework: Constitutional Privacy and Nascent Data Protection

The regulatory landscape in India presents a unique challenge, characterised by rapid, largescale deployment of FRT by the state coupled with a delayed, evolving statutory framework for digital privacy. The constitutional bedrock for privacy was definitively established by the Supreme Court of India in 2017, but the subsequent statutory regulation has left significant exemptions for governmental FRT use.

5.1. The Constitutional Bedrock: Puttaswamy and Fundamental Rights

The foundational principle for privacy protection in India is derived from the landmark decision in Justice *K.S. Puttaswamy v. Union of India*, which unanimously declared the right to privacy as an intrinsic part of the right to life and personal liberty guaranteed under Article 21 of the Constitution of

India.[54] The judgment established a three-fold test for any governmental action that infringes upon privacy: it must be backed by law, serve a legitimate state aim, and be proportional to the objective. [55] This constitutional test is the primary tool used by activists and petitioners to challenge the government's extensive deployment of FRT, arguing that such systems often fail the proportionality standard due to the lack of clear governing law and robust oversight mechanisms.[56]

5.2. Deployment and the Regulatory Vacuum

India has embraced FRT at a massive scale, primarily for law enforcement and national security. Projects such as the National Automated Facial Recognition System (NAFRS), which aims to create a centralised database of mugshots for identification nationwide, underscore the state's preference for utilitarian efficiency and societal safety over individual anonymity.[57] Until the enactment of the Digital Personal Data Protection (DPDP) Act in 2023, this extensive surveillance often operated in a legal vacuum, relying only on general provisions of the Information Technology Act, 2000, which offered minimal protection against state intrusion.[58] The lack of clear legal authorisation and standard operating procedures for FRT usage remains a critical concern for civil liberties, with challenges often centred on the lack of transparency in system testing and the documented global algorithmic bias.[59]

5.3. The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act, 2023, marks India's first comprehensive national data protection law, directly impacting the processing of biometric data, which is classified as Personal Data.[60] The Act requires' Data Fiduciaries'(entities collecting data) to obtain clear, informed consent from the 'Data Principal' (the individual) before processing their data, a standard that mirrors the GDPR's requirements for private entities.

However, the DPDP Act introduces broad exceptions that significantly weaken its application against government surveillance. Section 17 grants the Central Government the power to exempt any instrumentality of the state from the Act's provisions in the interests of "sovereignty and integrity of India," "security of the State," or "maintenance of public order."[61] This provision creates a wide regulatory chasm: while private entities face a rights-centric consent requirement, the government can easily bypass the law's core protections when deploying FRT for security purposes. This effectively codifies the utilitarian preference of the state, contrasting sharply with the EU AI Act's structural prohibitions and narrow, defined exceptions for law enforcement.[62] This dual regulatory standard—strict for the private sector, highly flexible for the state—means that Amorphous Privacy remains critically vulnerable to state overreach in India, shifting the entire burden of protection onto the already stressed constitutional framework established in Puttaswamy.[63]

6. Constitutional and Civil Liberties Frameworks

The widespread deployment of FRT fundamentally strains constitutional protections in ways that demand judicial reinterpretation of established legal concepts.

6.1. The Fourth Amendment and the Challenge to Public Anonymity

In the United States, the constitutional inquiry into surveillance must address whether automated, persistent tracking violates a "reasonable expectation of privacy," following the established standard set forth in *Katz v. United States.*[64] While individuals expose their faces to public view, they maintain a subjective expectation of privacy in their identities.[65]

FRT's capability to enable "pervasive tracking of individuals on an automated basis" fundamentally alters the nature of public space, shifting it from anonymous to constantly identified.[66] This technology transforms the constitutional analysis from a retrospective search of already collected evidence to a system of perpetual, prospective surveillance. If the technology is deployed broadly enough, it may be deemed a violation of the reasonable expectation of privacy simply by virtue of its existence and automated capability to track every person entering public space. This demands a legal restriction on deployment proportional to the intrusion.[67] Legal challenges are consequently likely, testing the boundary between legal police observation and unreasonable governmental intrusion, drawing parallels to precedents set for wiretapping and GPS surveillance.[68]

6.2. Systemic Bias and Civil Rights Exposure

The documented accuracy deficits of FRT regarding women and people of color result directly in disparate impacts on communities of color, necessitating careful scrutiny, particularly when used by law enforcement.[70] This algorithmic bias is not merely a technical error; it is a legal compliance failure under existing anti-discrimination frameworks. For instance, all EU member states are bound by the European Convention on Human Rights (ECHR), whose Article 14 prohibits discrimination, a principle that remains directly relevant to algorithmic governance causing disparate impacts.[71] In the US, civil rights statutes offer tools for aggrieved plaintiffs seeking justice against police conduct stemming from biased systems.

To address this legal exposure, organisations must recognise that mitigating discrimination requires robust data governance. Compliance necessitates ensuring that training, validation, and testing datasets are "relevant, sufficiently representative.[72] Therefore, technical standards (like those suggested by NIST [73] and legal governance frameworks (like GDPR's fairness mandate [74] must be adopted simultaneously, acknowledging that investing in representative datasets and continuous auditing processes throughout the AI lifecycle is a legal mandate, not merely an ethical choice.

Furthermore, the evidentiary crisis generated by FRT is acute. The reliance on FRT as the primary or sole piece of evidence linking an individual to a crime is deeply concerning. [75] The combination of known algorithmic bias, unverified real-world accuracy rates (especially with poor

quality inputs), and the potential for wrongful conviction presents a severe civil rights threat that mandates increased transparency, robust accountability measures, and strict auditing of systems used in the criminal justice context.[76]

7. Conclusion and Accountability Frameworks: Bridging the Regulatory Gap

The analysis confirms that the rapid development and deployment of FRT have generated a profound legal dilemma that existing laws, particularly in many common law jurisdictions, are currently inadequate to address.[77] The amorphous nature of the privacy harm—cumulative, intangible, and systemic—demands regulatory frameworks that focus on structural constraints rather than post-incident remedial measures.

7.1. The Necessity of Policy Intervention and Harmonisation

The divergence between the rights-centric, structural prohibition approach of the EU and the market-driven, high-liability litigation model of the US suggests that both regulatory paths offer critical lessons.[78] The passing of comprehensive, appropriate laws to regulate FRT is inevitable. A focused transatlantic dialogue, sharing the EU's proactive experience (bans and high-risk classification) and the US's reactive experience (existential liability), is essential to inform broader international regulatory convergence and establish shared accountability requirements.

7.2. Prescriptive Governance Model: Transparency and Impact Assessment

To ensure that FRT deployment adheres to the principles of necessity and proportionality, particularly in law enforcement and high-risk commercial applications, a prescriptive governance

The model must be universally adopted. All FRT deployments must be preceded by mandatory Data Protection Impact Assessments (DPIA) and Human Rights Impact Assessments (HRIA). [79] These assessments ensure that legal and ethical implications are addressed proactively. Furthermore, accountability must be explicitly exercised, explained, and audited for a range of stakeholder needs, including ensuring that robust complaint and challenge processes are easily afforded to all individuals.[80]

7.3. The Ten Critical Questions for Future Governance

The successful, ethical, and lawful development and deployment of FRT necessitates that the law

makers, policy makers, AI developers, and adopters collaboratively address ten fundamental, critical questions that clarify governance expectations: [81]

1. Control and Bias Challenge: Who should control the development, purchase, and testing of FRT systems, ensuring proper management and processes to challenge bias?

2. Acceptable Contexts for Image Capture: For what purposes and in what contexts is it acceptable to use FRT to capture individuals' images?

3. Fairness and Transparency for Capture: What specific consents, notices, and checks and balances should be in place for fairness and transparency for these purposes?

4. Basis for Data Banks: On what basis should facial data banks be legitimately built and used in relation to which purposes?

5. Fairness and Transparency for Data Bank Accrual and Use: What specific consents, notices, and checks and balances should be in place for fairness and transparency for data bank accrual and use, and what should not be allowable in terms of data scraping, etc.?

6. Performance Limitations: What are the limitations of FRT performance capabilities for Different purposes, taking into consideration the design context (i.e., real-world accuracy)?

7. Accountability for Usages: What accountability should be in place for different usages?

8. Exercising, Explaining, and Auditing Accountability: How can this accountability be explicitly exercised, explained, and audited for a range of stakeholder needs?

9. Complaint and Challenge Processes: How are complaint and challenge processes enabled and afforded to all?

10. Counter-AI Initiatives: Can counter-AI initiatives be conducted to challenge and test law

enforcement and audit systems?

Addressing these questions in granular detail is essential to bridge the regulatory gap and define a legally viable future for facial recognition technology.

REFERENCES

1. Vela PM. Amorphous privacy and the law: a new paradigm for digital rights. J Technol Law. 2024;123.
2. Vela PM. Amorphous privacy and the law: a new paradigm for digital rights. J Technol Law. 2024;123.
3. Solove DJ. Conceptualizing privacy. Calif Law Rev. 2002;90:1087.
4. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
5. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
6. Vela PM. Amorphous privacy and the law: a new paradigm for digital rights. J Technol Law. 2024;123.
7. Grand View Research. Facial recognition market size, share and trends analysis report. 2023.
8. Gates B. The promise and peril of biometric technology. Harv J Law Technol. 2022.
9. Chen K. Facial recognition and police surveillance. Stan Law Policy Rev. 2020;31:15.
10. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
11. Smith S. Facial recognition in the age of AI. MIT Law Rev. 2023.
12. Smith S. Facial recognition in the age of AI. MIT Law Rev. 2023.
13. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.

14. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.
15. Cothron v. White Castle System Inc. 2023 IL 128004 (Ill. 2023).
16. Habermas J. The communicative structure of the public sphere. Commun Res. 1985;12:50.
17. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
18. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.
19. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.
20. Grand View Research. Facial recognition market size, share and trends analysis report. 2023.
21. Grand View Research. Facial recognition market size, share and trends analysis report. 2023.
22. European Union. General Data Protection Regulation (EU) 2016/679. Art. 9(1).
23. Gates B. The promise and peril of biometric technology. Harv J Law Technol. 2022.
24. European Union. General Data Protection Regulation (EU) 2016/679. Art. 5(1)(e).
25. National Institute of Standards and Technology. Face recognition vendor test (FRVT). 2023.
26. National Institute of Standards and Technology. Interpreting face recognition performance. 2022.
27. National Institute of Standards and Technology. Interpreting face recognition performance. 2022.
28. National Institute of Standards and Technology. Interpreting face recognition performance. 2022.
29. Anand S. The trouble with facial recognition evidence. Geo Law J. 2021;39:25.
30. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
31. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
32. European Union. General Data Protection Regulation (EU) 2016/679. Art. 5(1)(d).
33. European Union. General Data Protection Regulation (EU) 2016/679. Art. 5(1)(a).
34. Chin JL. Algorithmic bias and civil rights law. NYU Law Rev. 2022;11:120.
35. Habermas J. The communicative structure of the public sphere. Commun Res. 1985;12:50.
36. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
37. European Union. General Data Protection Regulation (GDPR). Art. 9(1).
38. European Union. General Data Protection Regulation (GDPR). Art. 5(1)(a).
39. European Union. General Data Protection Regulation (GDPR). Art. 5(1)(d).
40. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
41. Habermas J. The communicative structure of the public sphere. Commun Res. 1985;12:50.
42. Chen K. Facial recognition and police surveillance. Stan Law Policy Rev. 2020;31:15.
43. European Union. Artificial Intelligence Act. 2024.
44. European Union. Artificial Intelligence Act. 2024.
45. European Data Protection Board. Guidelines on the use of facial recognition technology. 2023.
46. Chen K. Facial recognition and police surveillance. Stan Law Policy Rev. 2020;31:15.
47. Habermas J. The communicative structure of the public sphere. Commun Res. 1985;12:50.
48. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
49. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
50. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
51. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.
52. Anand S. The trouble with facial recognition evidence. Geo Law J. 2021;39:25.
53. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
54. Brown JK. State laws on biometric data: an overview. CRS Report. 2023.
55. S.681, 118th Congress (US). 2023.
56. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
57. Brown JK. State laws on biometric data: an overview. CRS Report. 2023.
58. Brown JK. State laws on biometric data: an overview. CRS Report. 2023.
59. Anand S. The trouble with facial recognition evidence. Geo Law J. 2021;39:25.
60. Illinois Compiled Statutes. 740 ILCS 14/15.
61. Cothron v. White Castle System Inc. 2023 IL 128004 (Ill. 2023).
62. Burns TM. Biometric data: a new frontier in class action litigation. Chic Law Rev. 2023;45:10.
63. Cothron v. White Castle System Inc. 2023 IL 128004 (Ill. 2023).
64. Feldman PM. BIPA and the calculus of liability. Law Technol J. 2024;33.
65. Cothron v. White Castle System Inc. 2023 IL 128004 (Ill. 2023).
66. Justice KS Puttaswamy v. Union of India. (2017) 10 SCC 1.
67. Manchanda R. India's data protection law weakens right to information and poses surveillance risk. The Conversation. 2023 Aug 15.
68. SFL v. Union of India. W.P. (C) No. 711 of 2020 (Delhi High Court).
69. The Digital Personal Data Protection Act, 2023. Gazette of India. No. 22 of 2023.
70. The Digital Personal Data Protection Act, 2023. Gazette of India. No. 22 of 2023.

71. The Digital Personal Data Protection Act, 2023. Gazette of India. Sec. 17.
72. The Digital Personal Data Protection Act, 2023. Gazette of India. Sec. 57.
73. The Digital Personal Data Protection Act, 2023. Gazette of India. Sec. 17.
74. Solove DJ. Conceptualizing privacy. Calif Law Rev. 2002;90:1087.
75. Solove DJ. Conceptualizing privacy. Calif Law Rev. 2002;90:1087.
76. Katz v. United States. 389 U.S. 347 (1967).
77. Katz v. United States. 389 U.S. 347 (1967).
78. Solove DJ. Conceptualizing privacy. Calif Law Rev. 2002;90:1087.
79. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
80. Bode M. The chilling effect of pervasive surveillance. Yale J Law Technol. 2013;15:1.
81. Electronic Frontier Foundation. Facial recognition: the good, the bad, and the ugly. 2023.
82. Chin JL. Algorithmic bias and civil rights law. NYU Law Rev. 2022;11:120.
83. European Convention on Human Rights. Art. 14.
84. European Union. Artificial Intelligence Act. 2024.
85. National Institute of Standards and Technology. Interpreting face recognition performance. 2022.
86. European Union. General Data Protection Regulation (GDPR). Art. 5(1)(a).
87. Anand S. The trouble with facial recognition evidence. Geo Law J. 2021;39:25.
88. Anand S. The trouble with facial recognition evidence. Geo Law J. 2021;39:25.
89. O'Connor M. Facial recognition and the threat to due process. Harv Law Technol Rev. 2020;10:30.
90. Liu R. Deep learning and biometric systems. ACM J Emerg Technol. 2023;12:45.
91. O'Connor M. Facial recognition and the threat to due process. Harv Law Technol Rev. 2020;10:30.
92. European Data Protection Board. Guidelines on the use of facial recognition technology. 2023.
93. Riley JC. Governing automated decision-making. Law Policy J. 2023;55.
94. Riley JC. Governing automated decision-making. Law Policy J. 2023;55.
95. Riley JC. Governing automated decision-making. Law Policy J. 2023;55.