Biometric Surveillance and Civil Liberties: A Legal Perspective

Arvind Sonawane[1], Surabhi Milind Sangai[2], Dr. Aparajita Mohanty[3], Piyush P. Gawali[4], Rishikesh Balkrishna Pansare[5], Dr.Lalita Kiran Wani[6]

[1]Sandip University Nashik, Nashik, Maharashtra, India. arvind.sonawane@sandipuniversity.edu.in

[2]Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. surbhai.sangai@sitrc.org

[3]Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU) Vimannagar, Pune, Maharashtra, India. amohanty@symlaw.ac.in

[4]Vishwakarma Institute of Technology, Pune, Maharashtra, India. piyush.gawali@viit.ac.in

[5]Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. rishikesh.pansare@sitrc.org

[6]Bharati Vidyapeeth's College of Engineering, Lavale,Pune, Maharashtra, India. Email: lalita.wani@gmail.com

Abstract: Biometric surveillance has become an increasingly prevalent tool in law enforcement and public security. While offering efficiency and precision, its widespread adoption raises concerns about the protection of civil liberties, particularly privacy, freedom of expression, and the right to assemble. This paper explores the legal frameworks governing biometric surveillance, identifying the gaps and inconsistencies in national and international regulations. Key civil liberties at risk, such as privacy breaches, potential discrimination, and the erosion of due process, are examined through case studies, including facial recognition technology use in the United States and GDPR's role in Europe. The analysis further highlights emerging legal safeguards and proposes reforms, such as enhanced oversight, stricter consent requirements, and transparency measures. By balancing technological advancements with civil liberties protection, this paper seeks to contribute to the ongoing debate on the ethical and legal use of biometric surveillance.

Keywords: Biometric surveillance, civil liberties, privacy rights, facial recognition, legal frameworks.

Introduction

Biometric surveillance refers to the use of technology to identify individuals based on their unique biological and behavioral characteristics. Common forms include facial recognition, fingerprinting, iris scans, and gait analysis. These technologies have gained significant traction in security and law enforcement due to their ability to provide precise identification with minimal manual input. The evolution of biometric technologies, particularly in the past two decades, has been driven by advancements in artificial intelligence and machine learning. Biometric systems are now widely deployed in airports, public spaces, and law enforcement agencies to monitor and identify individuals, making them a key tool in security operations globally[1], [2].

Civil liberties, the basic rights and freedoms guaranteed to individuals, play a critical role in safeguarding personal autonomy against government overreach. They are enshrined in constitutional and human rights law, protecting individuals' privacy, freedom of speech, and right to assemble, among others. The implementation of biometric surveillance presents unique challenges to these freedoms. Surveillance technologies collect vast amounts of personal data without explicit consent, raising concerns about privacy breaches and data misuse. Moreover, the use of biometric surveillance in public spaces has the potential to inhibit individuals' freedom of expression and assembly, as constant monitoring can create a chilling effect on lawful protest and dissent[3], [4].

The objective of this research is to provide a comprehensive analysis of the legal frameworks governing biometric surveillance and its implications for civil liberties. By examining the intersections between law, technology, and individual rights, this paper aims to explore potential conflicts that arise from the increasing use of biometric technologies. Additionally, the research will propose legal safeguards and regulatory measures to ensure that the use of biometric surveillance is conducted in a manner that protects civil liberties while addressing legitimate security concerns.

Biometric Surveillance Technologies: Scope and Applications

Biometric surveillance technologies have rapidly advanced, enabling the collection of a wide array of personal data for identification and monitoring purposes. The types of biometric data collected vary, with some of the most prominent methods including facial recognition, voice recognition, and fingerprinting. Facial recognition technology analyzes distinct facial features, enabling identification or verification of individuals in real time. Voice recognition systems capture unique vocal patterns to authenticate users or monitor conversations. Fingerprinting, a long-standing biometric technique, remains integral to law enforcement and security protocols, while emerging technologies such as iris scans, gait analysis, and even DNA-based recognition are becoming more sophisticated, further expanding the reach of biometric surveillance[5].

These technologies have found extensive application in law enforcement and public spaces, where they play a pivotal role in enhancing security measures. Police agencies utilize facial recognition to identify suspects from video footage, aiding in criminal investigations. At national borders, biometrics are used to strengthen security protocols by verifying the identities of travelers, helping to prevent illegal entry or identity fraud. In large public spaces, such as stadiums or city centers, these technologies assist in crowd monitoring and crime prevention by tracking movements and identifying individuals involved in illegal activities[6].

In addition to government uses, the private sector has increasingly embraced biometric surveillance for a range of applications. Corporations employ biometric technologies for security purposes, such as restricting access to sensitive areas through fingerprint or facial recognition systems. Identity verification is another critical use, especially in sectors like banking and healthcare, where robust authentication is required to protect personal information. Additionally, employee monitoring using biometrics is on the rise, allowing companies to track attendance, enhance productivity, and secure internal systems.

The widespread adoption of biometric surveillance across public and private sectors illustrates the growing reliance on these technologies, raising important legal and ethical questions about privacy and individual rights.

Civil Liberties at Risk

The widespread use of biometric surveillance presents significant risks to civil liberties, particularly in the areas of privacy, freedom of assembly and expression, and due process. These fundamental rights are increasingly being challenged by the growing reliance on technologies that collect and process personal data without individuals' full awareness or consent[7].

Right to Privacy

Biometric data collection directly affects the right to privacy, as it involves the capture of personal and often sensitive information, such as facial features, fingerprints, or voice patterns, without explicit consent. Unlike traditional identification methods, biometric data is inherently tied to the individual and cannot easily be changed, making unauthorized collection and misuse particularly concerning. Legal challenges have arisen around this issue, with courts grappling to define the boundaries of privacy in the digital age. A notable case is Carpenter v. United States, in which the U.S. Supreme Court ruled that individuals have a reasonable expectation of privacy in their location data. This case underscores the tension between law enforcement's use of surveillance technology and the constitutional right to privacy, highlighting the need for clearer legal guidelines[8].

Freedom of Assembly and Expression

Biometric surveillance also threatens freedom of assembly and expression, especially in public gatherings and protests. The ability of facial recognition systems to track and identify individuals in crowds poses a serious risk to these rights. Individuals may fear attending protests or political events due to concerns about being monitored or identified by law enforcement, which could stifle lawful dissent and peaceful assembly. Case studies have shown the use of facial recognition at political protests, such as those in Hong Kong or the Black Lives Matter demonstrations in the U.S., where activists reported feeling watched and vulnerable to retaliation.

Due Process and Discrimination

Biometric technology has raised concerns about due process and discrimination. One of the major issues is the accuracy of these systems, as they are prone to errors, particularly false positives, where an innocent person is misidentified as a suspect. This can lead to wrongful arrests or unjustified scrutiny. Studies have also shown that biometric systems often exhibit bias, especially against minority groups. For example, facial recognition technologies have been shown to misidentify people of color at significantly higher rates than their white counterparts. This disproportionate impact on minority communities raises questions about equal protection under the law and highlights the need for more transparent and accountable systems to prevent discrimination and uphold civil liberties[9].

In light of these risks, there is a pressing need to examine and address the legal and ethical implications of biometric surveillance to protect individual rights while balancing security concerns.

Legal and Ethical Challenges

The rapid advancement of biometric surveillance technologies has outpaced the development of comprehensive legal frameworks, leaving significant gaps in regulation and oversight. These challenges present both legal and ethical concerns, particularly regarding individual freedoms, privacy, and the potential misuse of biometric data[10].

Regulation and Oversight of Biometric Surveillance

One of the primary legal challenges surrounding biometric surveillance is the lack of clear legal frameworks in many jurisdictions. While some countries have enacted laws to regulate the collection and use of biometric data, many regions still operate in a legal gray area. For example, the United States lacks a federal biometric privacy law, resulting in a patchwork of state regulations. In contrast, the European Union has implemented the General Data Protection Regulation (GDPR), which imposes stricter controls on the collection and processing of biometric data. This inconsistency creates challenges for global companies and governments attempting to navigate the regulatory landscape, as privacy laws and enforcement vary significantly across borders. The inconsistent application of laws and standards complicates efforts to protect individual rights, with some jurisdictions offering far more robust safeguards than others.

Ethical Dilemmas

The implementation of biometric surveillance also raises a number of ethical dilemmas, particularly when it comes to balancing national security with individual freedoms. Governments and law enforcement agencies often argue that the use of biometric technologies is essential for ensuring public safety and preventing crime. However, these measures frequently come at the cost of personal privacy and civil liberties. Finding a balance between the two is a key ethical challenge, as excessive surveillance can erode trust between citizens and the state, leading to a chilling effect on freedoms like expression and assembly.

Another significant ethical issue is the role of consent in biometric data collection. Many individuals are unaware that their biometric information is being captured, especially in public spaces where surveillance systems like facial recognition are deployed. Informed consent, a cornerstone of ethical data collection, is often bypassed in the rush to enhance security measures. Without clear guidelines requiring consent or transparency, the collection and use of biometric data can feel invasive, raising questions about the right to control one's personal information[11].

Finally, the establishment of biometric databases introduces serious risks related to misuse or hacking. Biometric data is inherently sensitive and, unlike passwords, cannot be easily changed if compromised. Large-scale databases of biometric information are attractive targets for hackers, and any breach could result in severe privacy violations for the individuals affected. Additionally, the potential for misuse by governments or corporations, such as surveillance of dissidents or unauthorized tracking of individuals, raises serious ethical concerns about the long-term implications of storing and managing such sensitive information.

The absence of robust regulatory oversight and the numerous ethical dilemmas surrounding biometric surveillance underscore the need for stronger legal protections and a more thoughtful approach to its deployment. Without these measures, the risks to civil liberties and privacy will continue to grow as the technology becomes more widespread.

Case Studies

The use of biometric surveillance technologies, particularly facial recognition, has sparked widespread legal and ethical debates across the globe. Various countries have approached the regulation of these technologies differently, leading to significant variations in the protection of civil liberties. Table-1 provides a comparative analysis of case studies from the United States, the European Union, and China, highlighting the diverse regulatory frameworks and societal impacts[2], [12][13].

Table 1 Comparative analysis of various Case studies

Case Study	Key Issues	Legal Responses	Impact on Civil Liberties
Facial Recognition Technology in the U.S.	Use of facial recognition in public spaces by law enforcement; privacy concerns	Bans in cities like San Francisco, New York discussions	Ongoing debates about privacy violations and misuse
GDPR and Biometric Data in the EU	Regulation of biometric data collection and processing	GDPR regulates and restricts biometric data collection and storage	Stronger privacy protections, clear legal framework
China's Surveillance State	Extensive use of facial recognition and biometric databases	Little to no privacy protection, state-controlled surveillance	Erosion of privacy, suppression of dissent

- **Facial Recognition Technology in the United States:** In the United States, the use of facial recognition by law enforcement has faced significant public backlash. Several cities, such as San Francisco and New York, have moved to either ban or restrict the use of facial recognition in public spaces, citing privacy violations and concerns over unchecked government surveillance. The ongoing legal battles reflect the growing tension between security measures and the protection of individual privacy. While there is no federal regulation specifically governing facial recognition, these local bans highlight the fragmented legal response to biometric surveillance in the U.S.
- **GDPR and Biometric Data in the European Union**: The General Data Protection Regulation (GDPR) in Europe provides a stringent framework for regulating the collection and use of biometric data. Under GDPR, biometric data is classified as sensitive personal information, requiring explicit consent for collection and strict guidelines for its processing and storage. Several case law examples, such as the Hessen State Commissioner case in Germany, showcase the enforcement of GDPR provisions in regulating biometric surveillance. The GDPR has set a global standard for privacy protections, serving as a counterpoint to more permissive systems like those in the U.S. and China.
- **China's Surveillance State**: In contrast to Western approaches, China has embraced biometric surveillance on an unprecedented scale, with widespread use of facial recognition systems in public spaces and the creation of vast biometric databases. These technologies are integrated into state-controlled surveillance systems, enabling the government to monitor and track citizens with little regard for privacy. The implications for civil liberties are profound, as the Chinese government uses biometric surveillance to suppress dissent and control social behavior. This case presents a stark contrast to the protections offered under the GDPR in Europe and the evolving legal landscape in the U.S.

These case studies illustrate the wide disparity in how biometric surveillance technologies are regulated and implemented across the world. While the United States grapples with localized legal challenges and the European Union leads with robust privacy protections under GDPR, China represents a model of pervasive surveillance with minimal regard for civil liberties. This comparative analysis highlights the critical need for thoughtful regulation to balance security needs with individual rights, especially as biometric technologies continue to evolve and spread globally.

Emerging Legal Safeguards and Proposals for Reform

As biometric surveillance technologies continue to advance and become more widespread, governments and policymakers are increasingly recognizing the need for robust legal safeguards to protect individual rights. Current legislative efforts, both nationally and internationally, seek to regulate the collection, use, and storage of biometric data, while addressing the potential risks posed by these technologies. Alongside existing laws, several policy recommendations have emerged to ensure that biometric surveillance is conducted ethically and transparently[14].

Legislation to Regulate Biometric Data

Several countries have begun implementing laws specifically designed to regulate biometric data collection and usage. In the United States, the Biometric Information Privacy Act (BIPA), enacted in Illinois, has set a precedent for regulating the handling of biometric data. BIPA requires companies to obtain explicit consent from individuals before collecting biometric information and imposes strict guidelines on data retention and usage. Other U.S. states, such as Texas and Washington, have introduced similar laws, though a comprehensive federal biometric privacy law remains absent. Recent federal proposals aim to standardize biometric data regulations across the U.S., focusing on consent, transparency, and accountability.

Internationally, the General Data Protection Regulation (GDPR) in Europe is one of the most stringent legal frameworks for protecting biometric data. GDPR classifies biometric data as sensitive information, requiring explicit consent for its collection and implementing strict guidelines for processing, retention, and storage. Additionally, Convention 108+, an international treaty adopted by the Council of Europe, further strengthens protections for personal data, including biometrics, on a global scale.

Policy Recommendations

To enhance legal protections and ethical use of biometric surveillance, several key policy recommendations are proposed:

- Stronger Consent Requirements: One of the most critical aspects of biometric surveillance is ensuring that individuals are fully aware of and agree to the collection of their biometric data. Clear and informed consent requirements should be standardized globally, ensuring that individuals have control over their personal information. This includes providing transparent information on how the data will be used, who will have access to it, and how long it will be stored.
- Mandatory Audits for Bias and Accuracy: Biometric systems are prone to inaccuracies and biases, particularly in relation to gender, race, and ethnicity. To address this, it is recommended that governments and organizations conduct mandatory audits of biometric systems to ensure their accuracy and to identify and mitigate any potential biases. Regular assessments would help to prevent discrimination and ensure that biometric technologies are deployed fairly.
- Limitations on Biometric Surveillance in Public and Sensitive Spaces: There should be clear legal limits on the use of biometric surveillance in public spaces and sensitive areas, such as protests, polling places, and religious gatherings. These locations are crucial to the exercise of civil liberties, and unrestricted biometric surveillance could infringe on rights such as freedom of assembly and expression. Legislation should ensure that surveillance in these spaces is limited, justified, and conducted transparently.
- Transparency and Accountability: Governments and private sector entities that deploy biometric technologies must implement transparency and accountability measures to ensure ethical practices. This includes public disclosure of how biometric data is being collected, processed, and stored, as well as mechanisms for individuals to access, correct, or delete their data. Additionally, there should be clear procedures for redress in cases of misuse or unauthorized access.

The adoption of these emerging legal safeguards and policy reforms is essential to protect individual rights in an era of increasing biometric surveillance. By strengthening consent requirements, ensuring accuracy and fairness in biometric systems, limiting surveillance in sensitive spaces, and promoting transparency, governments and organizations can better balance security needs with the protection of civil liberties. As biometric technologies continue to evolve, it is crucial that legal frameworks adapt to address their ethical and privacy implications.

Conclusion and Future Scope

The expansion of biometric surveillance technologies has brought significant advancements in security and law enforcement, but it has also generated substantial concerns about civil liberties. As this paper has demonstrated, the collection and use of biometric data—whether through facial recognition, fingerprinting, or other methods—poses serious risks to privacy, freedom of assembly, expression, and due process. The case studies from the United States, the European Union, and China illustrate the varied legal responses to these technologies, highlighting both the progress and gaps in regulatory approaches.

The tension between the need for enhanced security and the protection of individual rights is at the core of the debate surrounding biometric surveillance. While biometric technologies offer efficient tools for public safety, their unchecked use can lead to overreach, discrimination, and privacy violations. Legal and ethical challenges, such as the lack of clear regulation, consent issues, and biases in biometric systems, underscore the urgent need for reform.

Looking ahead, there is a pressing need for comprehensive global frameworks that establish clear, consistent standards for the ethical use of biometric surveillance. International cooperation will be key in setting these guidelines, particularly as biometric technologies continue to advance and spread. Additionally, there must be a continued debate about the ethical implications of biometric technology, ensuring that public discourse and legal reforms evolve alongside technological innovations. Balancing the benefits of biometric surveillance with the protection of civil liberties will require ongoing vigilance, robust legal safeguards, and a commitment to preserving fundamental rights in the digital age.

References

[1] X. Wang, Y. C. Wu, M. Zhou, and H. Fu, “Beyond surveillance: privacy, ethics, and regulations in face recognition technology,” *Front. Big Data*, vol. 7, 2024, doi: 10.3389/fdata.2024.1337465.

[2] P. Singh, “Aadhaar and data privacy: biometric identification and anxieties of recognition in India,” *Information, Commun. Soc.*, vol. 24, no. 7, pp. 978–993, May 2021, doi: 10.1080/1369118X.2019.1668459.

[3] P. Arora, “General data protection regulation—a global standard? Privacy futures, digital activism, and surveillance cultures in the global south,” *Surveill. Soc.*, vol. 17, no. 5, pp. 717–725, 2019, doi: 10.24908/ss.v17i5.13307.

[4] N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, “Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR,” in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 5027–5033, doi: 10.1109/BigData.2018.8622621.

[5] A. Ioannou, I. Tussyadiah, and Y. Lu, “Privacy concerns and disclosure of biometric and behavioral data for travel,” *Int. J. Inf. Manage.*, vol. 54, p. 102122, 2020, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102122.

[6] S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, “Ethical, Legal, and Social Implications of Biometric Technologies BT - Biometric-Based Physical and Cybersecurity Systems,” M. S. Obaidat, I. Traore, and I. Woungang, Eds. Cham: Springer International Publishing, 2019, pp. 535–569.

[7] D. Nandy, “Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns,” *J. Curr. Soc. Polit. Issues*, vol. 1, no. 1, pp. 13–17, 2023, doi: 10.15575/jcspi.v1i1.442.

[8] C. Fontes and C. Perrone, “Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement,” *Inst. Ethics Artif. Intell.*, no. December, pp. 1–11, 2021, [Online]. Available: https://ieai.mcts.tum.de/.

[9] M. M. Kavanagh, S. D. Baral, M. Milanga, and J. Sugarman, “Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations,” *Lancet HIV*, vol. 6,

no. 1, pp. e51–e59, Jan. 2019, doi: 10.1016/S2352-3018(18)30243-1.

[10] J. M. Kizza, "Anonymity, Security, Privacy, and Civil Liberties BT - Ethical and Social Issues in the Information Age," J. M. Kizza, Ed. Cham: Springer International Publishing, 2023, pp. 79–103.

[11] S. Singh, V. Vikram, and B. Singh, "' Government Surveillance and Article 19 (1)(a): The Law Enforcement in Digital Age : A close Inspection on the legal boundaries ,'" vol. 12, no. 1, pp. 3520–3542.

[12] I. Barkane, "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance 1," *Inf. Polity*, vol. 27, pp. 147–162, 2022, doi: 10.3233/IP-211524.

[13] M. Phillips, "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)," *Hum. Genet.*, vol. 137, no. 8, pp. 575–582, 2018, doi: 10.1007/s00439-018-1919-7.

[14] P. De Hert and G. Bouchagiar, "Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices? 1 2," *Inf. Polity*, vol. 27, pp. 193–217, 2022, doi: 10.3233/IP-211525.