https://doi.org/10.48047/AFJBS.6.Si4.2024.6592-6602

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Balancing Biometric Identification And Privacy Rights In India: The Constitutional Perspective

Mohd Faiz Khan[1*], Dr. Naseem Ahmed[2]

[1*]Research Scholar, Faculty of Law, Integral University, Lucknow, India. E-mail: Faizbinkhan96@gmail.com (MCN-0002915)
[2]Professor, Faculty of Law, Integral University, Lucknow, India. E-mail: Deanlaw@iul.ac.in

***Corresponding Author:** Mohd Faiz Khan
Research Scholar, Faculty of Law, Integral University, Lucknow, India. E-mail: Faizbinkhan96@gmail.com (MCN-0002915)

Article History
Volume 6, Issue Si4, June 2024
Received: 20 June
Accepted: 24 July
Published: 03 August
doi: 10.48047/AFJBS.6.Si4.2024.6592-6602

Abstract

One The Indian government implemented a comprehensive biometric identity system known as Aadhaar in 2019. This nationwide programme assigns a unique identification number to Indian citizens and residents, while simultaneously gathering and storing their highly sensitive biometric and demographic data. With the implementation and promotion of the Aadhaar system in India, there was a significant increase in concerns about preserving and safeguarding private information. What measures may Indian people take to enforce and protect their privacy rights? In 2017, the Supreme Court tried to tackle this issue by asserting that an individual's right to privacy is an innate component of the entitlement to life and personal freedom and is therefore implied under Article 21 of the Indian Constitution. After the Apex Court affirmed that privacy is a fundamental right, the concept of a universal identity database raised constitutional concerns. Given the absence of an extensive legal structure for privacy protection and the lack of an express legislative right to privacy in India, it is pertinent to question whether the Indian government is infringing upon individual private rights via Aadhaar. In 2018, the Supreme Court ruled that the Aadhaar system is constitutional in relation to the compulsory linking of Aadhaar numbers to all government benefit programmes and services. Given this ruling, this article argues that the Aadhaar system should be thoroughly scrutinised owing to its encroachment on individual privacy rights.

Keywords: *Aadhaar, Constitution, Privacy, Puttaswamy, Surveillance.*

INTRODUCTION

In the late nineteenth century, the concept of the right to privacy was defined simply as the "right to be left alone."[1] The right to privacy has evolved and become more extensive over time, primarily because of emerging technology and information systems, along with other socio-political changes. These developments have brought about a range of complex issues that highlight the fundamental defining characteristics of privacy in the twenty-first century.[2] According to Alan

[1] Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy,' 4 HARV. L. REV. 193, 205 (1890).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy I), Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017).

Westin, a renowned scholar who extensively studied and defined the limits of privacy within the framework of the United States Constitution for fifty years as "privacy refers to the right of individuals, groups, or institutions to control the disclosure of information about themselves, including the timing, manner, and extent of its communication to others."[3] In 1989, the United States Supreme Court declared that privacy refers to an individual's ability to exercise authority over information pertaining to their own person.[4] President Bill Clinton's National Information Infrastructure Task Force provided a definition of privacy as "the right of an individual to have control over how personal information, which can identify that individual, is obtained, shared and utilised."[5] Privacy, in its current understanding, encompasses "the capacity of an individual or a group to isolate themselves or their personal information and consequently, to choose when and to whom they disclose such information."[6] Therefore, the description that will be employed in this Opinion to encompass privacy rights in the contemporary global structure can be expressed as follows: Privacy refers to the entitlement to manage the distribution of personal data.

CONSTITUTIONAL PRIVACY RIGHTS IN INDIA

Basic rights like "the right to life, dignity, personal freedom, happiness and liberty, originate from societal norms and are enshrined in constitutions and laws."[7] These rights are sometimes referred to as fundamental, inherent or unalienable rights. In contemporary democratic nations, "they cannot be completely restricted or limited by regular laws or the actions of elected representatives."[8] The architects of the Constitution of India held the belief that the enjoyment of liberty is incomplete without the assurance of specific liberties.[9] The primary objective behind the creation of the Indian Constitution was to ensure the attainment of justice, liberty, and equality for the people of India. The Constitution of India has "describe and designate specific rights" for its inhabitants.[10] To have a more comprehensive knowledge of these fundamental rights, it is crucial to refer to the actual language of the Constitution. The Preamble and Part III of the Constitution include provisions that guarantee some liberties such as those outlined in Articles 14, 19 and 21.[11] The Articles provide a detailed and exact list of rights, which include the right to equal protection, freedom of speech and expression, freedom of movement, life and personal liberty.[12] However,

---

[3] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967); see Karen Sparks, Alan Furman Westin, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Alan-Westin; see also Tabrez Ahmad et al., 'Right of Privacy: Constitutional Issues and Judicial Responses in USA and India, Particularly in Cyber Age' 11 (2009) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1440665.

[4] U.S. DoJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

[5] Ahmad et al., supra note 3, at 11.

[6] Id. at 2.

[7] See Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 at 23 (Bobde, J., concurring).

[8] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 at 22–23 (Chelameswar, J., concurring).

[9] Id. at 24.

[10] Id. at 22.

[11] INDIA CONST. pmbl.

[12] Art. 21 ("No person shall be deprived of his life or personal liberty except according to procedure established by law.")

there is no specific constitutional clause that clearly establishes a basic right to privacy, resulting in conflicting interpretations among Indian courts about the private rights of Indian people.[13]

THE PRIVACY JUDGEMENT

The Supreme Court's ruling in '*Puttaswamy v. Union of India*' ('Puttaswamy I')[14] on August 24, 2017, provided some clarification about the matter of basic privacy rights. Before the Puttaswamy I case, there was a widespread recognition of an implicit entitlement to privacy in India, albeit its limits were not well defined.[15] The ancient and holy literature of India has a sophisticated understanding of privacy.[16] In the Ramayana, a woman's visibility to an unfamiliar male is discouraged but the *Grihya Sutras* provide guidance on constructing a house in order to safeguard seclusion. Individuals belonging to a certain Hindu sect, called *the Ramanuj Sampradaya*, abstain from consuming food or beverages while in the company of others. Although privacy has been historically emphasised, the Court in Puttaswamy I established the legal significance of this problem by affirming that an individual's right to privacy is an intrinsic aspect of the right to life and personal liberty and is consequently implicit in Article 21 of the Indian Constitution.[17]

The ruling by Justice Chandrachud said that "privacy constitutes an inherent entitlement to one's life and liberty." [18] The judgement was a response to the widespread influence of both government and corporate entities seeking to control individual liberties.[19] Privacy rights needed to be discussed in the context of India's evolving technological environment where the argument on privacy was being examined within the framework of a global information-based society. The Court's objective was to provide constitutional significance to personal freedom within a globally integrated society. Justice Chelameswar, in his concurring opinion, emphasised that "fundamental rights serve as the only constitutional barrier against governmental intrusion into the essential freedoms that constitute the liberty of an individual."[20] In his concurrence, he finished by highlighting that the right to privacy is an essential freedom and is integral to the concept of liberty as defined in Article 21.

The '*Puttaswamy I*' judgement acknowledged the significance and worth of privacy as a constitutional right not by amending the constitution but by judicial interpretation to determine

---

[13] Ujwala Uppaluri & Varsha Shivanagowda, 'Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India,' 5 NUJS L. REV. 21, 33, 42-44 (2012).

[14] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012.

[15] Graham Greenleaf, 'Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number,' 137 PRIVACY LAWS & BUS. INT'L REP. 24, 24-26 (2015).

[16] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 at 21 (Bobde, J., concurring).

[17] Puttaswamy I, Writ petition (Civil) No. 494 of 2012 at 262 (majority opinion) ("Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution.")

[18] 'Right to Privacy a Fundamental Right,' Says Supreme Court in Unanimous Verdict, WIRE (Aug. 24, 2017), https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy/.

[19] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 at 4-5.

[20] Id. at 40 (Chelameswar, J., concurring).

the nature and scope of the freedoms guaranteed to individuals under the Indian Constitution.[21] The Court referred to Article 21 to clarify and establish this basic right. Justice Chandrachud stressed that the right to privacy is inherent in the right to life and liberty protected by Article 21. He emphasised that people have the entitlement to protect their privacy. Justice Bobde highlighted that the rightful and primary place for a right to privacy is inside Article 21, which is at the very essence of human freedom and existence. He expressed that "the concepts of liberty and privacy are closely linked with privacy frequently being a fundamental need for the exercise of human freedom."[22] In the above statement, Justice Bobde emphasised the need of safeguarding one's privacy to achieve personal satisfaction, happiness and optimal performance.

THE OVERIDING EFFECT

The Supreme Court in *Puttaswamy I* has overturned the rulings of two significant cases, '*M.P. Sharma v. Satish Chandra (1954)'* and '*Kharak Singh v. State of Uttar Pradesh (1962)*.' These landmark cases had previously determined that the right to privacy is not safeguarded by the Indian Constitution.[23] The Indian authorities confiscated papers from a corporation in the '*M.P. Sharma' case* since they were accused of tampering with records.[24] Sharma contested the constitutionality of the search and seizure arguing that it infringed upon his basic rights as guaranteed by Article 19(1)(f), which protects the right to own, possess and transfer property, and Article 20(3), which safeguards against self-incrimination.[25] In the case of *M.P. Sharma*, the Court determined that the right to privacy cannot be inferred from the provisions of Article 20(3) of the Indian Constitution since there is no provision analogous to the Fourth Amendment of the United States Constitution.[26] While Article 19(1)(f) was also under scrutiny, the Court specifically declined to recognise the right to privacy in relation to searches and seizures of documents. The Court adopted a limited and rigid perspective, holding that India lacks a comparable provision to the explicit bar on unauthorised searches included in the American Fourth Amendment.[27]

The '*M.P. Sharma'* ruling did not address whether a right to privacy would derive from other constitutional provisions, such as Article 19 or Article 21. The judgement ruled that Article 20(3) of the Indian Constitution does not include a right to privacy. The ruling does not inherently prohibit private protection under constitutional protections, such as Articles 19 or 21. This case left it opens for future judicial interpretation of whether other articles of the Indian Constitution

---

[21] Id. at 109-10 (majority opinion).

[22] Id. at 25 (Bobde, J., concurring).

[23] M.P. Sharma v. Satish Chandra, District Magistrate, Delhi (1954) 1 SCR 1077, 1096-97 (India); Kharak Singh v. State of U.P., (1964) 1 SCR 332, 351 (India).

[24] M.P. Sharma, 1 SCR at 1079-80; Ananthakrishnan G, M P Sharma and Kharak Singh: The Cases in Which SC Ruled on Privacy, INDIAN EXPRESS (July 19, 2017), http://indianexpress.com/article/explained/m-p-sharma-and-kharaksingh-the-cases-in-which-sc-ruled-on-privacy-4756964/

[25] M.P. Sharma, 1 SCR at 1080-81 (discussing INDIA CONST. arts. 19, 20).

[26] Gautam Bhatia, 'State Surveillance and the Right to Privacy in India: A Constitutional Biography,' 26 NAT'L L. SCH. INDIA REV. 127, 130 (2014).

[27] Sheetal Asrani-Dann, 'The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India,' 47 J. INDIAN L. INST. 53, 62 (2005).

safeguard the right to privacy. In the lack of a constitutional guarantee, the Court may view privacy as part of personal liberty, human dignity or life protection.

The petitioner in '*Kharak Singh'* questioned the legitimacy of police surveillance.[28] After being freed due to insufficient evidence, the petitioner was under police monitoring, including unannounced house visits, mobility reports and occasional queries into his correspondence. He contested the surveillance's legitimacy, alleging it infringed his basic rights of freedom of movement under Article 19(1)(d) and protection of life and personal liberty under Article 21. The Court ruled that Article 21's definition of "life and personal liberty" protects personal security and ruled that unauthorised entry into a person's house violates their right to personal liberty. The unannounced visits did not violate Article 19 since they did not restrict Singh's movements or personal liberty. The second section of the Kharak Singh ruling, invalidating house visits for violating personal liberty under Article 21 appears to recognise the right to privacy.[29] The first section of the opinion, emphasising that privacy is not a protected right under the Indian Constitution, invalidates it as a fundamental freedom.[30] The 2017 Supreme Court ruling in '*Puttaswamy I*'[31] overruled '*M.P. Sharma'* and '*Kharak Singh*,' establishing a new framework for addressing privacy problems in India.

AADHAAR SYSTEM IN INDIA: A PARTICULAR PRIVACY ISSUE

The need for further legal examination of privacy rights becomes apparent in light of the expansion and advancement of technology which has given rise to novel means by which the state may potentially encroach upon individuals' private, such as "surveillance, profiling and data collection." A total of 114 countries are expanding their utilisation of technology due to the rise in worldwide terrorism incidents and increased public safety apprehensions.[32] Analysing digital footprints and extensive data may reveal "patterns, trends and relationships, particularly in relation to human behaviour and interactions."[33] These technological improvements raise worries about the dissemination and processing of sensitive information by the government, particularly as engineers create more powerful algorithms and increase computing capabilities.

The Aadhaar card is at the heart of the on-going data gathering issue. Aadhaar, which was established in 2009, is a unique twelve-digit identification number provided by the 'Unique Identification Authority of India' ('UIDAI') to residents of India.[34] Individuals of all ages and socio-economic statuses are eligible to register for an Aadhaar number without any cost. The applicant is required to provide personal information, including their '*name,' 'date of birth,'*

---

[28] Kharak Singh v. State of U.P., (1964) 1 SCR 332.

[29] Id. at 348-51.

[30] 'Privacy Not a Fundamental Right' Supreme Court Had Held Decades Ago, FIRST POST (Aug. 24, 2017), http://www.firstpost.com/india/mp-sharma-and -kharak-singhs-case-privacy-not-a-fundamental-right-supreme-court-had-helddecades-ago-3966467.html.

[31] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 1, 261 (Sup. Ct. India Aug. 24, 2017).

[32] Id. at 7 (Kaul, J., concurring).

[33] Id. at 10.

[34] Caroline E. McKenna, 'India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System,' 38 BROOK. J. INT'L L. 729, 731 (2013).

'age,' 'gender', 'address,' 'mobile number,' and '*email*.' Additionally, they must supply '*biometric information,'* which consists of *'fingerprints,' 'iris scan' and 'face photos.'*

It serves as a crucial policy instrument for promoting social and financial inclusion, improving public sector service delivery, managing fiscal budgets, enhancing convenience, and facilitating efficient and people-centered governance. It plays a significant role in ensuring the financial inclusion of marginalised and vulnerable sections of society. Aadhaar aims to establish a nationwide identification system that can function seamlessly across different states, languages, and databases. This system aims to provide an identity to the most marginalised and disadvantaged individuals.[35] A significant number of destitute Indian individuals do not own officially acknowledged IDs, which hinders their ability to get 'mobile phones,' 'credit facilities,' 'bank accounts' or 'government assistance.' By possessing an Aadhaar ID, those who previously lacked proper identification may now immediately access 'housing subsidies,' 'healthcare and food assistance' via bank account contributions. Aadhaar may be used in several sectors like as 'food delivery,' 'employment,' 'education,' 'social security,' 'bank accounts' and 'healthcare.' It enables the agency or service provider to verify the identification of a beneficiary by accessing the central Unique Identification database. [36]So far, a total of 1.37 billion individuals in India have acquired Aadhaar identification.

THE PERIL OF BIOMETRIC SYSTEM

The extensive and centralised gathering, retention and use of an individual's demographic and biometric data has significant privacy concerns, particularly given the absence of comprehensive privacy legislation or an independent regulatory body in India. There is a concern among many that the use of a single global identification number may enable government or commercial entities to uncover confidential demographic and biometric data.[37] Indeed, there have been instances when the 'UIDAI system' has been hacked and Aadhaar information has been unlawfully obtained. Anonymous merchants have been using the WhatsApp mobile application to provide unfettered access to information from over one billion Aadhaar numbers. By paying a sum of '500 Rupees,' anyone may get access to another *'person's name,' 'address,' 'date of birth,' 'picture,' 'personal identity number,' 'phone number'* and *'email address.'* After acquiring Aadhaar information, hackers use the numbers to produce counterfeit Aadhaar cards for the purpose of connecting SIM cards and bank accounts of unsuspecting individuals, potentially resulting in identity theft. Paradoxically, the government established Aadhaar as a means to counter corruption and deter fraudulent identity and fraud. Despite the recent hacking events, UIDAI maintains that biometric detail is secured at the source and there is no unauthorised sharing or leaking of the data. They maintained that Aadhaar data including biometric information is completely protected and secure. According to UIDAI, possessing someone's Aadhaar number alone does not provide a risk since

---

[35] Nishant Shah, 'Identity and Identification: The Individual in the Time of Networked Governance,' 11 SOCIO-LEGAL REV. 22, 29 (2015).

[36] Vikas Dhoot, 'UIDAI Tightens Norms for Aadhaar-Bank Account Linking,' HINDU, http://www.thehindu.com/news/national/uidai-tightens-norms-for-aadha ar-bank-account-linking/article21938183.ece.

[37] Rachna Khaira, 'Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details,' TRIBUNE, http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

both their iris and fingerprints are required for effective identification. Merely having access to demographic information without biometrics cannot be exploited. Nevertheless, the claim that biometric authentication eliminates identity fraud has been proven false, since instances of identity fraud continue to occur even without the use of biometric authentication. Scammers have the ability to produce "counterfeit identification cards to use at airports or connect bank accounts to Aadhaar numbers or phone numbers to withdraw money."[38]

UIDAI asserts its commitment to safeguarding users and their information by implementing robust measures such as "a secure and encrypted database, stringent security and storage protocols, penalties for data tampering or unauthorised access, and limited data collection excluding details related to religion, caste, community, class, ethnicity, income, or health." Unfortunately, India lacks a comprehensive legislative framework to safeguard Aadhaar users from potential data breaches. In India, the activities of the state are governed by "sector-specific laws and the jurisprudential development of the right to privacy" due to the absence of comprehensive privacy laws.

LEGAL BASIS OF THE AADHAAR SYSTEM

Is the Indian government infringing on individual privacy rights with Aadhaar? This is because neither the Indian constitution nor any other laws provide for the protection of personal information. After the Supreme Court of India affirmed that privacy is a fundamental right, the constitutional validity of a universal identity database is in susceptibility. The key concern is that the implementation of Aadhaar would lead to extensive government monitoring, perhaps resulting in violations of secrecy and privacy. An identification system that utilises widespread monitoring undermines an individual's independence and personal growth while also infringing against the fundamental rights to privacy and human dignity. The Indian government's approach to handling such information and the potential political and personal repercussions of government abuse of such extensive personal data are uncertain.[39]

In *Puttaswamy I*, Justice Chandrachud elucidated that "informational control grants individuals the ability to utilise privacy as a means to maintain personal authority over information concerning them."[40] According to his viewpoint, information can only be gathered if three conditions are met: (1) legality - there must be a law in place; (2) need - the purpose for collecting the information must be reasonable according to the law; and (3) proportionality - the methods used by the legislature must be appropriate and balanced with the objectives and requirements of the law. It is crucial to take into account the need and applicability of the Act. Although the objective of the Act is notable - to ensure that every Indian has a unique identification number for adequate distribution of aid and assistance, the use of biometric information is an unreasonable method of data collecting. Besides to being irrational, the methods of data collecting are not proportionate with the purpose or requirements of the legislation.

---

[38] Rohan Venkataramakrishnan, 'How Long Can the Indian Government Continue Claiming Aadhaar Is Secure and Foolproof?,' SCROLL (Jan. 4, 2018), https://scroll.in/article/863779/how-long-can-the-indian-government-continue-claiming-aadhaar-is-secure-and-foolproof.

[39] INDIA CONST. pmbl. ('recognizing human dignity in the Constitution').

[40] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 1, 201 (Sup. Ct. India Aug. 24, 2017).

Biometric information refers to the unique and inherent data associated with each individual, including *'fingerprints,' 'retina scans,' 'voice analysis,' 'DNA analysis' and 'face recognition.'* The allure of biometric information lies in its inherent difficulty to counterfeit; nonetheless, there exist significant apprehensions about the effectiveness of biometric analysis. Although the technique is not infallible, every biometric authentication procedure is susceptible to errors. Manual labourers may face challenges with fingerprint scanning due to the wear and changes that occur to their hands over time.

Due to the high cost of biometric programmes, organisations are more likely to engage in data sharing, resulting in a more extensive network of linked personal information. While several nations have successfully adopted ID card programmes, the majority of these schemes do not use biometric identification or have various applications. UIDAI can still achieve its objective of establishing a comprehensive database including every Indian resident by using demographic information. Additional alternatives include of storing biometric data on a disconnected terminal, where the data is not maintained in a singular centralised internet database, or using smartcards, where the biometric information is directly recorded on the card itself.[41] These solutions provide fewer security risks and are more practical approaches to collecting and storing data.

In contrast to the rulings reached by the Indian Supreme Court in '*Puttaswamy I'* and '*II,'* the Aadhaar system is deemed unlawful and infringes upon private rights. Informational privacy is a component of the right to privacy.[42] Although there is a delicate equilibrium between personal interests and the legitimate concerns of the government, the Indian authorities would have challenges in demonstrating an overwhelming national interest that would surpass the safeguarding of private rights. An appropriate objective of the state could involve activities such as safeguarding national security, deterring and examining criminal activities, promoting innovation and the dissemination of information and/or preventing the misuse of social welfare benefits.[43] Although the state interests are significant, a right guaranteed by the Constitution should be given priority over such state objectives.

Nevertheless, while the verdict of the Supreme Court carries legal weight, there is a possibility that 'Article 13(2) of the Indian Constitution' might provide a legal avenue to declare the Aadhaar Act as unconstitutional. Article 13(2) states that the government cannot create any laws that restrict or diminish the rights granted by Part III. Any legislation that goes against this provision would be considered invalid to the degree of the violation. Hence, a legislation that permits the gathering of personal information without sufficient protections infringes against the right to privacy as outlined in Article 21 of the Indian Constitution. Consequently, it should be deemed invalid under Article 13(2). Based on this logic, the '*Puttaswamy I'* court should have ruled that the Act is unconstitutional.

While the constitutionality of the Aadhar Act was ultimately upheld, it is imperative to establish protective measures for the system. The relevant sections of the '*Puttaswamy I'* judgement assert that any gathering of sensitive data that might affect privacy must be supported by legislation. To

---

[41] Kritika Bhardwaj, 'The Mission Creep Behind the Aadhaar Project,' WIRE (Sept. 2, 2016), https://thewire.in/63223/the-mission-creep-behind-the-uidaiscentralisation-ideology/.

[42] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 1, 201 (Sup. Ct. India Aug. 24, 2017).

[43] Id. at 265.

guarantee the longevity of Aadhaar, India must enact extensive privacy legislation that includes provisions for legal remedies and other measures to prevent privacy breaches. Given that the Indian Constitution has recognised the right to privacy as a legally protected right, this undertaking should be facilitated. While the constitutionality of the Aadhar Act was ultimately upheld, it is imperative to establish protective measures for the system. The relevant sections of the 'Puttaswamy I' judgement assert that any gathering of sensitive data that might affect privacy must be supported by legislation. To guarantee the longevity of Aadhaar, India needs to pass extensive privacy legislation that includes provisions for legal remedies and other measures to prevent privacy breaches. Since personal privacy is a constitutionally guaranteed right in India, this should be a less difficult task.

In addition, it is essential to prohibit data sharing across various authorities and service providers. The unauthorised transfer of data across organisations would provide a digital trace of an individual's actions and records, enabling information gathered for one objective to be used for entirely other objectives. For instance, the interconnection of databases might take place when a company, during the job application process, has access to the medical records, financial details, or voter registration information of a prospective employee. Personal data should be restricted or maintained in a manner that is directly related to its intended purpose and used only to the degree that is required for that purpose. Ultimately, people should have the right to seek and acquire information on their personal data, as well as have a mechanism to contest the accuracy or validity of that data. If the challenge is deemed successful, the data should be altered or deleted.

CONCLUSION

'Puttaswamy' did not include surveillance. However, what India received from it is a complex and intricate collection of concepts that elucidate the many aspects of privacy while also directly addressing the consequences of monitoring. In addition to 'Aadhaar,' it establishes a structure for evaluating the current set of laws that regulate surveillance. The Supreme Court examination of the right to privacy under the Indian Constitution is a significant advancement towards the establishment of more precise and enforceable privacy legislation in India. Developing an adaptable and robust understanding of the Indian Constitution would enable future generations to effectively tackle the challenges posed by a system like 'Aadhaar.' Given the fast advancement of technology, it is likely that many current concepts of privacy and security will become out-dated. Therefore, legislation must be adaptable to address the changing needs and concerns of society. The 'Aadhaar' system is increasingly becoming obligatory for both Indian citizens and noncitizen residents while accessing government services in India. Society and lawmakers have the ability and should request comprehensive data privacy laws to avoid the dystopian consequence of widespread monitoring, data gathering and government interference. As an increasing number of individuals acquire used to tolerating state interference in their lives, there is a danger that people may learn to see government data collecting for potentially unlawful reasons as normal.[44] Hence, efficient legislative measures should include external supervision, judicial examination and transparent revelations of information dissemination.

REFERENCES

[44] 'SURVEILLANCE, PRIVACY, AND SECURITY: CITIZENS' PERSPECTIVES', 217 (Michael Friedewald et al. eds., 2017).

1. Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy,' 4 HARV. L. REV. 193, 205 (1890).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy I), Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017).
3. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).
4. U.S. DoJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).
5. Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 at 23.
6. Ujwala Uppaluri & Varsha Shivanagowda, Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India, 5 NUJS L. REV. 21, 33, 42–44 (2012).
7. Graham Greenleaf, Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number, 137 PRIVACY LAWS & BUS. INT'L REP. 24, 24–26 (2015).
8. Right to Privacy a Fundamental Right, Says Supreme Court in Unanimous Verdict, WIRE (Aug. 24, 2017), https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy/.
9. M.P. Sharma v. Satish Chandra, District Magistrate, Delhi (1954) 1 SCR 1077.
10. Kharak Singh v. State of U.P., (1964) 1 SCR 332 (India).
11. Ananthakrishnan G, M P Sharma and Kharak Singh: The Cases in Which SC Ruled on Privacy, INDIAN EXPRESS (July 19, 2017), http://indianexpress.com/article/explained/m-p-sharma-and-kharaksingh-the-cases-in-which-sc-ruled-on-privacy-4756964/.
12. Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Biography, 26 NAT'L L. SCH. INDIA REV. 127, 130 (2014).
13. Sheetal Asrani-Dann, The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India, 47 J. INDIAN L. INST. 53, 62 (2005).
14. 'Privacy Not a Fundamental Right' Supreme Court Had Held Decades Ago, FIRST POST (Aug. 24, 2017) , http://www.firstpost.com/india/mp-sharma-and -kharak-singhs-case-privacy-not-a-fundamental-right-supreme-court-had-helddecades-ago-3966467.html.
15. Caroline E. McKenna, India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System, 38 BROOK. J. INT'L L. 729, 731 (2013).
16. Nishant Shah, Identity and Identification: The Individual in the Time of Networked Governance, 11 SOCIO-LEGAL REV. 22, 29 (2015).
17. Vikas Dhoot, UIDAI Tightens Norms for Aadhaar-Bank Account Linking, HINDU, http://www.thehindu.com/news/national/uidai-tightens-norms-for-aadhaar-bank-account-linking/article21938183.ece.
18. Syed Anas Ansar, Jaya Yadav, Sujit Kumar Dwivedi, Ankur Pandey, Savarni Prakash Srivastava, Mohammad Ishrat, Mohd Waris Khan, Dhirendra Pandey, Raees Ahmad Khan. (2021). A Critical Analysis of Fraud Cases on the Internet. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(1), 424-445. https://doi.org/10.17762/turcomat.v12i1.7950.
19. Rachna Khaira, Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details, TRIBUNE,http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.
20. Rohan Venkataramakrishnan, How Long Can the Indian Government Continue Claiming Aadhaar Is Secure and Foolproof?, SCROLL (Jan. 4, 2018), https://scroll.in/article/863779/how-long-can-the-indian-government-continue-claiming-aadhaar-is-secure-and-foolproof (emphasizing the downsides of biometric identification in relation to bank and identity fraud).

21. Kritika Bhardwaj, The Mission Creep Behind the Aadhaar Project, WIRE (Sept. 2, 2016), https://thewire.in/63223/the-mission-creep-behind-the-uidaiscentralisation-ideology/.
22. SURVEILLANCE, PRIVACY AND SECURITY: CITIZENS' PERSPECTIVES 217 (Michael Friedewald et al. eds., 2017).