FREEDOM IN THE AGE OF SURVEILLANCE: RE-EXAMINING NOZICK'S MINIMAL STATE

Bhargav Naik, Bengaluru, Karnataka.

ABSTACT

This article examines the conflict between personal freedom and governmental monitoring in modern-day India. The paper critically investigates whether government systems like Aadhaar and facial-recognition technology comply with or transgress these boundaries, drawing on Robert Nozick's libertarian theory of the minimum state, whose only legal duty is to protect individuals from coercion, robbery, and fraud. Nozick's ideas of self-ownership, consent, and negative liberty are placed in the context of India's developing digital governance framework. It contends that although biometric technologies are said to improve efficiency and security, their coercive and opaque implementation frequently expands state authority beyond protective purposes, eroding autonomy and privacy.

The study also examines how technological exclusion, function creep, and mandatory data gathering undermine substantive freedom, especially for vulnerable groups. It draws the conclusion that India's surveillance architecture runs the risk of turning the protecting minimum state into an invasive maximal state based on legislative developments like ***K.S. Puttaswamy v. Union of India and the Digital Personal Data Protection Act (2023).*** In order to balance technological governance with Nozick's vision of a free, rights-respecting society, the research advocates for strong protections based on consent, proportionality, and data sovereignty.

Introduction

One of the hallmarks of modern government is digital monitoring infrastructure, which raises important issues regarding the appropriate balance between individual liberty and state authority. Unprecedented capabilities for tracking, monitoring, and profiling individuals are represented by systems like the Aadhaar biometric database in India and the expanding facial recognition networks. Robert Nozick's argument for the minimum state, which is political philosophy's most rigorous support of limited government, must be revisited in light of this technological revolution.

Nozick contends in Anarchy, State, and Utopia (1974) that the only ***"Night-watchman state"*** that is ethically acceptable is one that is limited to defending people against coercion, theft, fraud, and contract enforcement. He argues that any state that goes beyond these duties routinely breaches people's rights by viewing them as means rather than objectives in and of themselves (Nozick, 1974). In order to determine if widespread data collection actually improves security or essentially undermines the freedoms and privacy rights that the minimum state aims to protect, this study applies Nozick's concept to modern surveillance infrastructures.

Nozick's Minimal State: Theory and Concepts

To apply Nozick, it is essential to understand his core theoretical positions: self-ownership, individual rights, the minimal state, and limits on state action.

Self-ownership and individual rights

Nozick starts with the moral precept that people own themselves; they are ends in and of themselves, not just means to a goal. They have rights to life, liberty, property, and the acquisition and transfer of possessions as a result of his "entitlement theory." These rights must be acknowledged by the state, and it can only supersede them in specific circumstances.

The minimal state

Nozick argues that the only morally justified state is a Minimal or "night-watchman" state: one that protects individuals from force, theft, fraud, and enforces contracts. It is an extremely limited conception: beyond protection, redistribution, public education, health care, economic regulation these are not justified in his view.

He provides a model of how this state could arise spontaneously from a "state of nature" via private protection agencies, without violating rights.

Limits to state power

Nozick emphasizes that people's rights would be violated by any state that goes beyond the minimal. "The state may not use its coercive apparatus to get some citizens to help others or to prohibit activities of people for their own good or protection," he says. According to Nozick, the state can only be legitimate if it upholds individual autonomy and self-ownership while carrying out its protective function.

The framework for utopia and freedom

Nozick describes the minimum state as the "framework for utopia" in his book Anarchy, State, and paradise. This basic structure allows people to freely pursue their own goals in a variety of communities. Here, "freedom" refers to freedom from governmental intervention and compulsion rather than freedom for social good**.**

Implications for data, surveillance and state power

Despite the fact that Nozick wrote in a pre-digital era, his theory implies that state mechanisms that go beyond defending people against outside threats particularly if they entail widespread data collection, monitoring, profiling, or identity systems may be in conflict with the minimal state's normative bounds if they restrict individual autonomy without consent.

Therefore, any Nozickian study of biometric or mass surveillance technologies must ask:

1. Does the system only seek to shield people from damage (fraud, theft, and force)?

2. Does it honor liberty, property (including data as property or under self-ownership), and individual consent?

3. Does it refrain from considering people as nothing more than tools or utilizing them to further the goals of others (for example, by mandating data collecting to help others without consent)?

4. Is there a chance that the state will go beyond its protecting core and start controlling,

coercing, or profiling people?

Surveillance, Biometric Identity and Privacy in India

India offers a particularly rich case for study: large-scale biometric identity (Aadhaar), linking of data across state programmes, increasing deployment of facial recognition and AI surveillance. These raise real questions about freedom, privacy and state power.

Aadhaar: the world's largest biometric ID

Residents are given a 12-digit unique identity number through the Aadhaar program, which is run by the Unique identity Authority of India (UIDAI), based on biometric (iris, fingerprint) and demographic information. According to academics, it is the biggest biometric system globally.

Aadhaar has been defended as a tool for benefit distribution, identity verification, fraud prevention, and governance. However, it has sparked worries about data security, meaningful consent, exclusion of disadvantaged populations, and possible mass monitoring. One study, for example, points out "security threats" in the Aadhaar database and raises concerns about whether connecting it to other systems compromises privacy.

Legal jurisprudence: the right to privacy and Aadhaar

The Supreme Court ruled in ***K. S. Puttaswamy v. Union of India (2017)*** that Article 21 of the Indian Constitution guarantees the right to privacy. The Court upheld the constitutionality of the Aadhaar Act in the ensuing five-judge ruling (2019), but with significant restrictions. The Court acknowledged concerns about data linking and possible surveillance dangers.

Facial recognition and biometric surveillance

In addition to Aadhaar, facial recognition technology (FRTs), video surveillance, and AI-driven security, monitoring, and identification systems are being used more often in India. For instance, a recent study on FRT in India brought attention to concerns about discrimination, consent, and data privacy. Another study that examined commercial facial-processing software on Indian faces discovered substantial mistake rates, particularly for female participants, which raised questions about accuracy and fairness.

Furthermore, although the Digital Personal Data Protection Act, 2023 has made an effort to close the gap, India's biometric data governance is still fragmented and lacks a comprehensive data-protection legislation. The Criminal Identification Act of 2022 was the subject of a recent examination of biometric surveillance legislation, which revealed significant protection vulnerabilities.

Surveillance, exclusion and the freedom question

Linking Aadhaar to welfare programs or mobile SIM verification has resulted in the exclusion of disadvantaged communities when authentication fails or data discrepancies arise (e.g., physically manual laborers whose fingerprints are degraded), as several critics have highlighted. Efficiency is not the only issue; access, autonomy, and the ability to live without invasive government identification or surveillance are other concerns.

Summary of the Indian empirical context

As a result, India has a system of widespread biometric/identity surveillance (Aadhaar), growing face recognition and video surveillance, and a legislative framework that recognizes the right to privacy but is still developing its restrictions over state data collection and surveillance. In the era of digital monitoring, this makes India an ideal place to test the normative claims of Nozick's minimum state.

Applying Nozick: Analysing Freedom, Surveillance and the Minimal State

In this section, we apply Nozick's minimal-state framework to the Indian surveillance context and pose the following question: Does the use of facial recognition software and the collection of biometric and identity data fulfill the protective role consistent with the minimal state, or does it go beyond Nozickian bounds by becoming state-control and interfering with freedom and autonomy?

Does biometric/identity data collection serve protection from force, theft and fraud?

Nozick’s minimal state is characterised by protection of individuals from harm, theft, fraud and enforce contracts. The question: to what extent do Aadhaar and facial-recognition systems serve that protective role?

In favour:

- It is claimed that the Aadhaar system reduces leakages in welfare programs, expedites the distribution of subsidies, helps prevent identity fraud, and offers confirmed identification for service access. According to certain empirical research, Aadhaar facilitates governance.

- In security situations, such as airports and train stations, facial recognition technologies are specifically employed for crime detection and prevention.

Against:

- The protective rationale is frequently asserted, but there is little independent confirmation of the extent of fraud avoided, the trade-offs, or if the same goals might have been met with less invasive methods. For instance, a remark on Reddit stated that "claims of widespread identity fraud and Aadhaar's ability to plug these leakages are not supported by reliable evidence."

- The state has more insight into people's travels and transactions when Aadhaar is connected to various services. The proportionality of the intrusion must be evaluated if surveillance is permissible only for the purpose of stopping fraud, although this is frequently ambiguous.

- Critics point out that while facial recognition technology may offer protection against some threats, it also permits ongoing surveillance, monitoring, and profiling. For instance, the authors of the FRT report inquire about "discrimination, data protection, and the risk of mass surveillance."

Nozickian assessment:

According to Nozick, certain biometric verification may be justified in order to prevent theft or fraud, but only if it is appropriate, required, respects human agreement, and does not treat people like tools or subject them to unwarranted compulsion. Aadhaar and face recognition deviate from what Nozick views as a minimum justifiable state if they go much beyond this protective role into widespread surveillance and data collecting for the purpose of state control.

Consent, data as property/self-ownership and autonomy

One important aspect is Nozick's theory of self-ownership, which holds that people are the proprietors of their labor and its results. In a metaphorical sense, one could contend that people have control over their biometric or personal data (though Nozick did not specifically address data). Is permission, autonomy, and control of data sufficiently respected by Indian biometric systems?

Observations in India:

- Although the Supreme Court specifically said that biometric data could not be forced in some situations, Aadhaar enrollment has been needed in several situations.
- Critics point out that people have less control over how their data is shared, connected, and used.
- In public settings, facial recognition frequently happens without meaningful permission; people may not be aware that they are being scanned, profiled, or mapped.
- Data breaches and biometric cloning have been documented; thousands of Aadhaar-enabled fraud occurrences are mentioned in the examination of biometric data laws in India.

Nozickian assessment:

People's autonomy is jeopardized if they are forced to disclose biometric information or if their information is gathered and utilized against their will. According to Nozick, the state cannot use individuals as simple tools by requiring data collecting for reasons other than protection. Therefore, the necessity of permission and self-ownership is a crucial litmus test: the state must explain why it requires that information and not impose it arbitrarily or in an opaque manner. It appears that many Indian customs don't meet this criterion.

Scope creep, state control and surveillance

Concerns: Transitioning from a small to a large state. Nozick cautions against the government going beyond protection to include redistributive welfare, economic life management, or personal activity control. In a similar vein, surveillance technology and biometric/identity

systems may increase the state's ability to track, categorize, and meddle in the lives of its residents.

In Indian context:

- Beyond the distribution of subsidies, Aadhaar is now used for banking, food rations, school admissions, cell SIM verification, and more. Opponents contend that this "scope creep" turns Aadhaar from a limited form of identity verification into a de facto global ID.

- The state's ability to profile, monitor movement, behavior, and social involvement is increased when services and data points are linked. The Criminal Identification Act 2022 broadens the possibility for gathering "physical and biological samples," according to the article on biometric surveillance legislation.

- "While it enhances efficiency and security, its widespread use raises serious concerns regarding privacy, mass surveillance, and algorithmic bias," the report on FRT says, raising worries about discrimination and the absence of regulatory protections.

Nozickian assessment:

According to Nozick, the smallest state cannot employ coercive tools to achieve goals other than defending rights. Biometric and surveillance technologies run the potential of going against the minimal-state ideal if they are incorporated into a coercive architecture that allows the government to monitor, control, or interfere in individuals' lives without their agreement. The question is whether these technologies are being used for control (prohibited) or protection (justified).

Freedom, privacy and self-determination

From Nozick’s perspective, the minimal state must not use coercive apparatus to further ends beyond protecting rights. If biometric/ surveillance systems become part of a coercive architecture enabling the state to monitor, control or intervene in citizens’ lives without their consent, then they risk violating the minimal-state norm. The question is whether these technologies are being used for protection (justified) or for control (disallowed).

In the Indian surveillance scenario:

- According to Puttaswamy, the freedom of conscience, mobility, identity, and affiliation are all closely related to the right to privacy. The space of freedom decreases when continual state visibility is enforced by facial recognition or biometric technologies.

- The freedom of people impacted is diminished by exclusion brought on by authentication errors (e.g., denial of food, services). The majority ruling in the Aadhaar case said that a person's right to live and get services is jeopardized if their lack of Aadhaar makes them invisible to the government.

- People's ability to protest, travel anonymously, and associate may be curtailed if they are aware that they are being watched.

From a Nozickian lens, when state data-systems reduce individuals' ability to freely pursue their lives without interference, they jeopardize one of the minimal state's core purposes: safeguarding freedom.

Weighing protective gains vs freedom losses

A subtle point: Nozick does not dispute the legitimacy of the state's use of certain identifying systems for citizen protection. However, he maintains that the state's authority must be reasonable and limited. As a result, while assessing biometrics and surveillance, one must balance the liberty costs (data gathering, monitoring, possible coercion, exclusion) against the protective benefits (fraud prevention, security).

In India:

- Benefits include enhanced governance, decreased identity fraud, and perhaps more effective subsidy delivery.

- Costs include extensive data collecting, the possibility of excluding vulnerable groups, opaque database connection, the possibility of function creep and control, and a decrease in autonomy and consent.

The main concerns are whether the costs of liberty are reasonable and if sufficient protections (permission, accountability, openness, and opt-out) are in place. In the absence of these, the

state may have gone beyond Nozick's acceptable limit.

Critical Discussion: Reconciling Nozick with Contemporary Surveillance Challenges, Tensions and Theoretical Depth

In this section, we go deeper into the theoretical conflicts, evaluate Nozick's applicability in the digital era, extract novel arguments, and examine the difficulties posed by Indian practice.

Theoretical tension: self-ownership/data ownership and surveillance

It is possible to construe Nozick's self-ownership to include biometric identification and personal data: your face, body, and biometrics belong to you; governmental acquisition of such data, particularly without authorization, poses significant philosophical questions. It may be argued that rather than seeing people as ends in and of themselves, the biometric database views individuals as "ends for others" (e.g., ends for the state, ends for benefit target-matching).

In the Indian setting, this is evident: Since Aadhaar is being utilized more and more for a variety of purposes (such as welfare, bank KYC, mobile verification, and subsidies), people may be viewed mostly as nodes in a state system due to database connectivity. This contradicts Nozick's assertion that people shouldn't be utilized as tools. As a result, people's ability to manage their identity and data is jeopardized.

Surveillance and the minimal state's boundary

Nozick has a limited minimum state. However, biometric/identity systems may be used for purposes other than security, such as social control, behavioral surveillance, profiling, and automatic exclusion. These roles provide the state authority that goes much beyond preventing fraud and theft.

The introduction of face recognition in public infrastructure, the usage of Aadhaar for school admissions, and its connection to bank accounts and cell SIMs indicate that the Indian government is doing much more than just protecting citizens. This begs the question: At least in its data/surveillance branch, has India's state transitioned from minimum to maximum (or expansive)? From a Nozickian perspective, it appears that the response is in the affirmative.

Exclusion, inequality and freedom for all

A novel aspect: Nozick's theory emphasizes individual protection, yet it may not celebrate strong equality or welfare in its most basic form. It might be argued that biometric systems in India have given rise to new kinds of exclusion. Thus, the most vulnerable people's freedom to live safely may be undermined. This leads to a paradox: a system intended to provide welfare and protection may instead limit some groups' freedom.

Therefore, from a justice perspective (even if one stays within Nozick's libertarianism), vulnerable people's freedom is undermined when they are unable to access services because of authentication failures or a lack of alternatives. Freedom must be protected by the smallest state in reality as well as in theory.

Are surveillance technologies inevitable for protection? Empirical necessity vs normative boundaries

One may contend that technology like biometrics and surveillance are essential to safeguarding people against fraud, terrorism, and identity theft in a contemporary, vast, digitally linked state. However, Nozick would counter that the state's job is still restricted to defending rights; even if monitoring makes protection more effective, it must not infringe upon personal liberty or go beyond its protective mission.

The question in Indian practice is whether biometric technologies are appropriate for the evils they are meant to reduce. Some critics point out the exclusion and authentication flaws, while others contend that Aadhaar's claim to have decreased leaks is exaggerated. It challenges the empirical rationale. In the absence of a compelling empirical argument, the normative threshold is crossed.

The problem of "function-creep" and perverse incentives

An intelligent argument "Function-creep" is one of the risks associated with large-scale biometric/identity systems. Once a system is in place for one reason (welfare), it may be used for many other purposes (banking, SIM, education, monitoring). According to Nozick, this is an increase in the state's ability to use coercion without permission or discussion. The idea of the basic state is compromised.

Additionally, there is an incentive logic: if infrastructure and data are available, connection becomes inexpensive, and the desire to watch increases. As a result, there is a slippery slope

from the minimal state to the condition of extensive data surveillance. The Indian instance has early indications of this kind of slope.

Reconciling protection and autonomy: a balanced normative view

Protection and autonomy in balance: a normative perspective

Although Nozick's minimalism provides a distinct limit, the image is complicated by technology and real-world administration.

A normative compromise might be suggested: biometric and surveillance systems might be allowed if they meet the following requirements:

(i) clear legal purpose limited to protection;

(ii) transparency and auditability;

(iii) minimal collection (data minimization);

(iv) meaningful opt-out or alternative;

(v) explicit individual consent.

They run the danger of weakening freedom without these. Many of these protections such as required connections, unclear procedures, a dearth of options, and exclusion risks are either nonexistent or inadequate in the Indian environment. The spirit of Nozick's minimum state is thus violated by several biometric/identity techniques that fail the aforementioned normative requirement.

Contribution: Extending Nozick to the digital era

An original contribution of this article is to argue that Nozick’s minimal state framework remains highly relevant in the digital era but requires adaptation. Specifically:

- The domain of “protection” must now consider digital harms (identity theft, data breaches, algorithmic discrimination) as well as physical ones (force, theft).
- The question of “data-ownership” and “biometric sovereignty” emerges as an extension

of self-ownership: individuals must own/control their biometric and identity data.

- The coercive capacity of the state is no longer only physical (police, army) but also informational. State surveillance via data is a new kind of coercion. Thus, Nozick's limits must incorporate informational/epistemic domains.

Freedom is threatened in novel ways by the possibility of exclusion (digital exclusion): people's ability to engage in society is reduced if authentication is unsuccessful or data linking excludes them.

Therefore, applying Nozick to biometric/surveillance systems shows that while these technologies may aid in protection, they must be strictly regulated to prevent compromising autonomy.

Conclusion

The issue of how freedom and privacy are affected in a time when biometric data gathering, identification system linkage, and face recognition monitoring are becoming more commonplace calls for careful philosophical consideration. A normative benchmark can be found by reexamining Robert Nozick's minimal state, which was restricted to protection against force, theft, and fraud. This benchmark states that the state must respect individual autonomy, avoid coercion, respect self-ownership (including possibly data as an extension of self), and maintain a minimal scope.

India's experience with Aadhaar and face recognition technologies provides both a warning about how these systems might go beyond safety into surveillance, exclusion, and erosion of autonomy, as well as an illustration of the protective potential of digital identification. While biometric systems may yield gains in security or governance, they pose serious freedom risks when they become mandatory, opaque, linking across domains, or exclude vulnerable individuals from essential services.

REFERENCES

- Nozick, R. (1974). *Anarchy, State, and Utopia*. Basic Books.
- Nozick, R. "The entitlement theory of justice, libertarian rights and the minimal state: a critical evaluation." Journal of Civil & Legal Sciences.
- "Nozick's Theory of Libertarianism (Several Aspects)." PoliticalScienceNotes.com. https://www.politicalsciencenotes.com/liberalism/nozicks-theory-of-libertarianism-several-aspects/809?utm_
- Shah, H. (2023). "Aadhaar Act and its privacy challenges." *Journal of Legal Studies & Research, 9*(3), 263-268. https://jlsr.thelawbrigade.com/article/aadhaar-act-and-its-privacy-challenges/
- Mishra, A. & Kashyap, P.K. (2024). "A critical study of biometric surveillance laws in India and implications of the Criminal Identification Act 2022." *Educational Administration: Theory and Practice, 30*(4),https://kuey.net/index.php/kuey/article/view/9894?utm_
- Pali, I., Krishania, L., Chadha, D., Kandar, A., & Varshney, G. (2020). "A comprehensive survey of Aadhaar and security issues," arXiv. https://arxiv.org/abs/2007.09409?utm_
- "Biometric Data Regulation in India: Legal Landscape and Risks." Mondaq. (2025) https://www.mondaq.com/india/privacy-protection/1666050/biometric-data-regulation-in-india-legal-landscape-and-risks?utm_
- Khera, R. "Aadhaar in Welfare is Pain without Gain," *The Hindu*, 2018.
- "AI-Driven Facial Recognition: Human Rights Concerns and Regulatory Challenges." *MAGLAW: Panjab University Law Magazine*. (2024)
- "Cinderella's shoe won't fit Soundarya: An audit of facial processing tools on Indian faces." Jain, G. & Parsheera, S. (2021) arXiv. https://arxiv.org/abs/2112.09326?utm_
- "The Evolution of Right to Privacy: From K.S. Puttaswamy to Aadhaar." FreeLaw.in.

(2025) Free Law: Get Free Headnotes & Judgments

- Maashin, A.T. (2023). "Robert Nozick's Minimal State: A Critique." *Jurnal Ilmu Sosiologi Dialektika Kontemporer,* https://ojs.unm.ac.id/elektikakontemporer/article/view/46152?utm_
- Internet Encyclopaedia of Philosophy. (2018). "Nozick, Robert." Stanford Encyclopedia of Philosophy
- "The Aadhaar Verdict: How Supreme Court addressed petitioners' arguments on surveillance, privacy." *Indian Express*, Sept 27 2018.https://indianexpress.com/article/india/aadhaar-case-how-supreme-court-addressed-petitioners-arguments-on-surveillance-privacy-5376238/?utm_
- Raju, R.S., Singh, S., Khatter, K. (2017). "Aadhaar Card: Challenges and Impact on Digital Transformation.". https://arxiv.org/abs/1708.05117?utm_
- "BIOMETRIC IDENTITY-AADHAAR, PRIVACY AND PERSONAL DATA PROTECTION IN INDIA." Bhat, M.A. (2022). *South Asian Review, 1*(2). https://www.sairjc.com/assets/img/issue/x9m317_0Hc1a4_8edx9T_t5c3l1_107814.pdf?utm_
- PoliticalScienceNotes.com. "Nozick's Theory of Libertarianism (Several Aspects)." https://www.politicalsciencenotes.com/liberalism/nozicks-theory-of-libertarianism-several-aspects/809?utm_
- Britannica. "Robert Nozick | Minimal State." https://www.britannica.com/biography/Robert-Nozick?utm_
- "The right to privacy in the digital age: Challenges and legal framework in India." Thakur, A. (2025). *International Journal for Legal Research and Analysis.* https://www.ijlra.com/public/details/the-right-to-privacy-in-the-digital-age-challenges-and-legal-framework-in-india-by-aditya-thakur?utm_