BIOMETRICS AND SURVEILLANCE AS A TOOL OF TRACING CITIZENSHIP

Ankita Shekhawat, Manipal University

1. Introduction

The heart of the Modern nation-state is the idea of Citizenship. It describes the political and legal relationship between the individual and the state. Earlier Citizenship was created by naturalization, Birth, or Lineage, and was confirmed by records like voter ID cards, passports, and birth certificates.

But in a time of international migration and quick technological advancements, governments and institutions are shifting more and more to biometrics and surveillance to recognize, verify, and regulate citizenship for the protection of national security.

The Greek words bio, which means life, and metric, which means to measure, are the roots of the word biometrics.A brief explanation of biometrics is that they are physical traits or biological measurements that can be used to identify people. Some examples of biometric technology are fingerprint mapping, facial recognition, and retinal scanning; however these are only the most well-known. According to researchers, other distinctive characteristics include a person's ear shape, posture, and gait, as well as their body Odor, hand veins, and even facial expressions. These characteristics help to define biometrics. Biometric identity verification promises accuracy, efficiency, and security when included in governance systems. At the same time, surveillance technologies—from drones and closed-circuit television to facial recognition powered by artificial intelligence—allow governments to watch, monitor, and manage populations on a never-before-seen scale. These systems work together to create a techno-legal identity management regime that has significant ramifications for citizenship.

The AADHAAR Act, 2016 aims to ensure efficient, transparent, and targeted delivery of financial and other subsidies, benefits, and services to individuals in India through unique identity numbers, promoting good governance and transparency.. While primarily intended as a tool for welfare distribution, Aadhaar has become increasingly intertwined with issues of citizenship and governmental legitimacy, particularly in relation to the National Register of

Citizens (NRC) and the Citizenship Amendment Act (CAA), 2019. The NRC process in Assam, for example, revealed the importance of biometrics in establishing who qualifies as a citizen, with far-reaching implications for inclusion and exclusion.

However, the increasing dependence on biometrics and surveillance to regulate citizenship creates a number of constitutional, legal, and human rights concerns. In its landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court of India documented the right to privacy as a basic right under Article 21 of the Constitution, limiting the unfettered use of biometric data. Similarly, in Justice K.S. Puttaswamy v. Union of India (2018), also known as the Aadhaar decision, the Court upheld the validity of Aadhaar while striking down provisions that allowed for excessive surveillance and data misuse, highlighting the importance of balance, purpose limitation, and data protection.

At the international level, Article 15 of the 1948 Universal Declaration of Human Rights (UDHR) guarantees the right to nationality and bans arbitrary citizenship deprivation. Similarly, the International Covenant on Civil and Political Rights (ICCPR) of 1966 emphasizes the right to legal identification and privacy, requiring a careful balance between state sovereignty in deciding citizenship and individual rights to dignity and acknowledgment. The Indian legal landscape has also changed with the passage of the Digital Personal Data Protection Act of 2023, which aims to govern data processing and protect citizens' informational sovereignty, however concerns about state monitoring exemptions persist. This study tries to critically evaluate biometrics and surveillance as methods for tracing citizenship, focusing on India's legal and constitutional framework while placing it in a broader comparative and international context. It contends that, while new technologies may strengthen the state's ability to identify and verify individuals, they also threaten to undermine fundamental rights, widening inequality, and redefining the entire definition of citizenship.

2. Surveillance and Biometric Citizenship

The connection between law, identity, and surveillance has become increasingly significant in debates about citizenship. States have always relied on some ways of identification, whether it is a ration card or an Aadhar card, but the introduction of biometrics has significantly changed this relationship. Where once authentication was done through traditional paper-based documentation methods, it is now being done via biometric markers such as fingerprints, iris scans, etc. In recent years biometric authentication has entered the mainstream; facial

recognition on smartphones, technology to speed up the experience at the airport, fingerprint access to online banking apps, or even biometric payment cards – the examples are endless[1].

The complex connection between citizenship and surveillance practices is a complex topic that has attracted a lot of attention lately. Concerns over the effects on individual liberties and rights are growing as governments and businesses use surveillance technologies more frequently. The goal of this book is to give a thorough analysis of the intricate relationships at work by examining the development of surveillance, how it affects citizens, and the laws and regulations that control its application. In its most basic definition, surveillance is the methodical observation or tracking of people, groups, or activities. In the past, governments have mostly used surveillance for law enforcement, national security, and tax collection. However, the extent and magnitude of surveillance have significantly increased due to technological improvements.

Large volumes of personal data may now be collected and analyzed thanks to the development of digital technology, frequently without the express consent of the subjects. As a result, more widespread and invasive modes of monitoring have replaced more conventional, focused surveillance. Because people actively disclose personal information online, the growth of social media, for example, has opened up new channels for data collecting. For a democratic society to function, citizens' rights are essential. Among these rights are the freedoms of speech, assembly, and privacy. These rights can be greatly impacted by surveillance techniques, frequently in subtle but substantial ways. For instance, free speech and assembly may be suppressed when people are aware that their actions are being watched. For fear of being watched, people may self-censor or refrain from engaging in particular activities. This may result in less civic engagement and the suppression of opposition.

"The impact of surveillance on citizenship is not just about the collection of data, but about the creation of a culture of fear and compliance."[2]

"The use of AI in surveillance is not just about automating existing processes; it's about creating new capabilities that were previously unimaginable." - Dr. Shoshana Zuboff, Author of The

[1] Biometry authentication history (infographic) | Thales
[2] Electronic Frontier Foundation. (n.d.). Surveillance. Retrieved from https://www.eff.org/surveillance

Age of Surveillance Capitalism.[3]

Thus, AI and machine learning make it possible to analyze enormous volumes of data in real time, they are completely changing surveillance. This makes it possible to identify people, behaviors, and patterns more precisely and effectively. AI-powered face recognition software, for example, can recognize people in groups, follow their whereabouts, and even forecast their behavior.

Due to the possibility of illegal tracking, biometric surveillance—which makes use of distinctive physical traits like fingerprints or facial features—is becoming more and more common. However, because biometric data can be prone to inaccuracies and misidentification, this raises questions about accuracy and privacy. Furthermore, biometric data is extremely sensitive, thus strong security measures are required.

Surveillance capabilities are also being greatly impacted by the Internet of Things (IoT). Large volumes of data, such as location and behavioral trends, may be gathered by IoT devices and utilized to improve monitoring capabilities. Along with enabling new types of surveillance, such smart home gadgets that watch people in their homes, these devices may also be used to follow people or keep an eye on public areas. In general, there is increasing worry about the combination of IoT and biometric monitoring.

With ramifications for privacy, autonomy, and other fundamental rights, the proliferation of surveillance technologies is having a substantial influence on citizenship. The loss of privacy is a serious issue as governments and businesses are gathering more information on people, which may violate their rights and liberties. Knowing that one's actions are being watched can have a chilling impact on other fundamental rights, including free expression. Discriminatory results might result from biased monitoring systems that reinforce current social injustices. When personal data is gathered and analyzed for the purpose of manipulating people, it can lead to a loss of autonomy.

The idea of "digital citizenship," which holds that everyone has the right to have their online freedom of expression and privacy protected, is also under attack. Equal access to digital tools

[3] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books. https://www.amazon.com/Age-Surveillance-Capitalism-Future-Frontier/dp/1610399745

and opportunities should be a prerequisite for digital inclusion and engagement.

The necessity for new legal safeguards in the digital era is highlighted by the quick development of surveillance technologies. To secure individuals' personal information, strong data protection laws are required; regulations governing the use of surveillance technologies should be transparent; and rules protecting citizens' digital rights, such as the freedom of expression and assembly online, should be put in place. Responding to the challenges posed by surveillance technology requires a multi-faceted approach involving governments, corporations, and civil society.[4] Legislation, social reactions, and technology advancements can all be used to address the critical role that governments play in controlling emerging surveillance technologies. While civil society may campaign for change, promote alternative ways, and increase awareness of the hazards and consequences of surveillance technology, legislation can regulate it, safeguard data, and foster transparency.

Technology like encryption, anonymization, and surveillance-resistant technology can also be utilized to reduce the hazards associated with surveillance. While anonymization measures help safeguard identities, encryption can prevent unwanted access to sensitive data. Secure communication applications are one example of a technology that may be made to withstand monitoring. Given the complexity and diversity of the future of surveillance and citizenship rights, it is critical to think about and react appropriately to the consequences for citizenship. This will entail technology solutions, societal reactions, and legal remedies. We may strive toward a future that strikes a balance between the necessity of security and the defense of fundamental rights and freedoms by comprehending new developments in surveillance technology and their possible effects on citizenship. In conclusion, for a future that strikes a balance between security and the defense of basic rights and freedoms, it is imperative to comprehend the intricate and multidimensional nature of surveillance and citizenship rights.[5]

3. Current Trend of Surveillance

India's surveillance industry is expanding at a very rapid pace, and the main issue is that the

[4] Lee, S. (n.d.). *The future of surveillance and citizenship rights*. https://www.numberanalytics.com/blog/futuresurveillance-citizenship#:~:text=Biometric%20surveillance%20involves%20the%20use%20of%20unique%20physical,becoming%20increasingly%20prevalent%2C%20with%20significant%20implications%20for%20citizenship.

[5] Lee, S. (n.d.-a). *Surveillance and Citizenship: A Comprehensive guide.* https://www.numberanalytics.com/blog/surveillance-citizenship-guide

country lacks explicit rules controlling it. The operation of governmental entities, their powers, the protection of individual privacy, and the right to free expression all require distinct laws, even if the legislature has approved several acts and regulations that indirectly regulate surveillance. For reasons of public safety, public order, etc., the government may intercept, monitor, or decrypt any data or information kept on computer resources under Section 69 of the Information Technology Amendment Act, 2008; however, it is unclear who has the authority to do so. Despite being created by the Information Technology Act of 2008, CERT-In will only be activated in the event that an assault is launched against Indian systems or resources, or if any Indian servers are compromised or wrecked by a foreign entity or a person from India or another country.

India's surveillance laws are primarily governed by the Information Technology Act, 2000 and the Indian Telegraph Act, 1885. The Indian Telegraph Act allows the Central and State governments to intercept messages in public emergencies, public safety, or in the interest of sovereignty, integrity, security, friendly relations with foreign states, public order, and preventing incitement to offense. Rule 419A of the Indian Telegraph Rules allows for interception orders to be issued by the Secretary of the Ministry of Home Affairs or the State Government in-charge of Home department. A review committee is created to review interception orders, but failure to do so does not make any officer liable. The Committee only has power to revoke orders and destroy data collected if they do not meet the requirements of the People's Union for Civil Liberties case. The Information Technology Act allows the Central and State Government to issue directions for monitoring, interception, and decryption of information. The Ministry of Home Affairs has authorized 10 agencies for interception, monitoring, and decryption of information under the Act. The Central Board of Direct Taxes, the Directorate of Revenue Intelligence, the Central Bureau of Investigation, the National Investigation Agency, RAW, the Directorate of Signal Intelligence (for Jammu and Kashmir, North East, and Assam only), the Enforcement Directorate, the Intelligence Bureau, the Narcotics Control Bureau, the Enforcement Directorate, and the Commissioner of Police, Delhi, are among these organizations.

Although biometric monitoring has been crucial in improving national security and expediting government, it has also generated a global ethical discussion about civil liberties, consent, and individual rights. These issues have gained attention in India because of the introduction of extensive biometric systems like Aadhaar and laws like the Act, 2022. Informed consent,

privacy, data protection, and the disproportionate impact on underprivileged groups are the main ethical topics of discussion.

As to the ruling in K.S. Puttuswamy vs. Union of India, the Indian Constitution guarantees the right to privacy as a basic right. But law enforcement agencies can order surveillance and interceptions without court review, which might result in a situation where the government uses these authorities as it pleases. The fact that there is no data protection legislation makes it difficult since those being watched would be unaware of their monitoring, making it unable to contest the orders. According to the Supreme Court of India, privacy is an inherent component of Article 21 and Part III of the Indian Constitution and is a basic right that cannot be taken away. The court underlined the necessity of proportionality in infringement and the need for a legislative framework to safeguard people's privacy. The court underlined the necessity of a suitable data protection regulation that guarantees proportional involvement and seeks to preserve a democratic society. The ruling also underlined the necessity of safeguards against the misuse of government intervention. The decision emphasizes how crucial a logical connection between goals and methods is to maintaining privacy. The right to privacy in India is a fundamental right, but biometric surveillance often occurs without explicit consent, resulting in limited knowledge and control over data usage. The Aadhaar system, despite its benefits, has been criticized for creating a digital divide and excluding millions. The Act, 2022, allows for the collection of biometric and behavioral data before conviction and extends data retention to 75 years, opening the door for potential abuse and profiling. The vague language of the Act and lack of independent redress mechanisms for wrongful data collection further exacerbate the ethical implications. International legal frameworks, such as the European Union's GDPR, enshrines principles like explicit consent, the right to be forgotten, and data minimization. However, India lacks a central data protection authority with sufficient autonomy to oversee government surveillance projects. The ethical stakes in biometric surveillance extend beyond privacy, affecting dignity, autonomy, and the trust citizens place in democratic institutions. Without robust legal frameworks, consent mechanisms, and oversight, biometric governance in India risks becoming an intrusive tool of control rather than an enabler of digital empowerment.

Indian legislative framework and surveillance policies are inadequate to address future threats, and there is a need for amendments to protect the IT industry and individual privacy. Similar to the UK and US, India should pass laws governing surveillance by governmental departments

and agencies. The existing framework is insufficient to address cyber crimes and terrorism. The government has the power to intercept, monitor, decrypt, or block information on computer resources, but the workings of these agencies and penalties for misuse are not mentioned. The information obtained may be used for political purposes, making it crucial to redefine privacy in the modern age. The existing framework is not enough to deal with future threats, and the government should provide clear guidelines for the protection and destruction of data collected during surveillance.

The conflict over surveillance and privacy stems from our struggles to adjust to technological advancements.

Historically, challenges to privacy and protective measures have often occurred in close succession. The term 'right to be left alone' initially appeared in the 1890s. In the same decade, fingerprinting was adopted to establish and maintain physical databases for personal identification. In the US, a 1928 court order allowed for the seizure of electronic communications during 'threats to national security', but the definition of national security was not specified. From 1967 until 1978, the US government conducted Project MINARET and SHAMROCK, intercepting and collecting electronic communications of US individuals as part of a concerted effort against the USSR. 16 In 1967, the 'Katz-vs-US' court battle established a legal precedent requiring police agents to obtain a warrant before eavesdropping personal communications. The digitization of fingerprinting and enormous personal datasets has increased the risk of digital identity theft, resulting in a surge in the anti-intrusion and antivirus software industries. After the introduction of HTTPS in 1995, malware and bugs Antivirus and antimalware companies gained political relevance in the 2000s as malware became more popular. Study shoes that State sovereignty, integrity, and security depend on surveillance, yet the lack of a data protection legislation has given the government access to people's personal information. As to the ruling in K.S. Puttuswamy vs. Union of India, the Indian Constitution guarantees the right to privacy as a basic right. But law enforcement agencies can order surveillance and interceptions without court review, which might result in a situation where the government uses these authorities as it pleases. The fact that there is no data protection legislation makes it difficult since those being watched would be unaware of their monitoring, making it unable to contest the orders. According to the Supreme Court of India, privacy is an inherent component of Article 21 and Part III of the Indian Constitution and is a basic right that

cannot be taken away.[6] The court underlined the necessity of proportionality in infringement and the need for a legislative framework to safeguard people's privacy. The court emphasised the need for a suitable data protection regulation that ensures proportional involvement and promotes a democratic society. The ruling also underlined the necessity of safeguards against the misuse of government intervention. The decision emphasizes how crucial a logical connection between goals and methods is to maintaining privacy.[7]

4. Privacy and Surveillance: Nexus

It has taken a lengthy and changing process for India to recognize the right to privacy as a basic right. Its origins can be found in the 1962 Kharak Singh case, in which the Supreme Court gave privacy its first legal consideration. But at the time, privacy was not specifically recognized as a right guaranteed by the constitution. The Supreme Court did not fully establish privacy as a basic right under Article 21 of the Indian Constitution until the historic Justice K.S. Puttaswamy ruling in 2017. This decision was a major turning point because it upheld the fundamental right to privacy that is necessary for individual freedom and dignity. India's growing awareness of the necessity to shield people from undue state surveillance and intervention into their private life is shown in this journey from Kharak Singh to Puttaswamy. Although it was not acknowledged as a constitutionally guaranteed right, the bench first took the right to privacy into consideration in its entirety in the Kharak Singh case. The bench emphasized the impact of law enforcement surveillance on the petitioner's privacy rights.[8] In the PUCL case, the bench upheld Justice Subba Rao's minority view in the Kharak Singh case, expanding the meaning of Article 21 to encompass the "right of an individual to be free from restrictions or encroachments on his person." Judicial interventions in India have substantially influenced the debate on governmental monitoring and private privacy. Courts have established limitations for legitimate surveillance while protecting citizens' rights. Judicial opinions have impacted not just the sorts of monitoring allowed, but also the methods and conditions under which it can be carried out. The K.S. Puttaswamy v. Union of India case had a significant impact in this context. This landmark decision by a nine-member Supreme Court bench altered India's privacy rules. The Supreme Court ruled that privacy is a fundamental constitutional right, overturning prior

[6] ARTICLE 19 & 21 WITH RESPECT TO RIGHT TO PRIVACY. (2021). In *Jus Corpus Law Journal (JCLJ)* (pp. 78–80). https://articles.manupatra.com/pdf/59357c8a-7b8d-47ae-a004-9a8de241458f.pdf

[7] Legal Service India. (n.d.). *Surveillance in India and its Legalities*. https://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html

[8] Xiu J., 'The Roles of the Judiciary in Examining and Supervising the Changing Laws of Electronic Surveillance' [2003]

verdicts that denied it, firmly establishing that privacy is an inherent part of the right to life and personal liberty under Article 21 of the Constitution[9]. The Puttaswamy ruling established essential concepts for privacy rights and data protection in India. It clarified the definition of privacy, its importance to human dignity, and the need to preserve it from state overreach. This judgment has influenced policies and legal frameworks, emphasizing the need for justified, required, and reasonable intrusions into privacy to achieve desired objectives. In India, the K.S. Puttaswamy verdict is used to evaluate surveillance, data protection, and privacy laws and practices. It has affected legal rulings that aim to balance state authority and individual rights.

In People's Union for Civil Liberties (PUCL) v. Union of India [10], the Supreme Court established guidelines to prevent arbitrary phone tapping under the Indian Telegraph Act of 1885. The Court noted that wiretapping violates privacy and requires a legally authorized mechanism. This case paved the door for more comprehensive privacy rules, as articulated in Puttaswamy. The Aadhaar judgment, also known as Justice K.S. Puttaswamy (Retd) v. Union of India, is another notable case. Following the 2017 privacy verdict, the Supreme Court considered the legitimacy of the Aadhaar project. The Court allowed the use of Aadhaar for government welfare schemes and PAN linking, but ruled against mandating Aadhaar for mobile connections and bank accounts, citing privacy concerns. The court emphasized that the state may acquire biometric data for legitimate purposes, but it must be necessary, reasonable, and not violate privacy arbitrarily. The Navtej Singh Johar v. Union of India case, while not directly linked to surveillance, broadened the scope of privacy rights. This momentous verdict repealed Section 377 of the Indian Penal Code, decriminalizing consenting same-sex partnerships. The Supreme Court defined privacy as "the right to be alone," emphasizing the importance of protecting personal and private choices, particularly those related to sexual orientation, from outside intervention. The Court's recognition of decisional privacy broadens privacy protections beyond data and monitoring, elevating it to a basic right. These cases impacted India's privacy jurisprudence, requiring the state to conduct surveillance under tight legal safeguards. These verdicts acknowledge both the legitimate security needs of the state and the potential threats to personal freedoms posed by technology. These decisions provide

[9] Aksietha, R. (2025). Surveillance in India and its privacy challenges in the digital Age: a legal and constitutional analysis. In International Journal for Research Trends and Innovation, *International Journal for Research Trends and Innovation* (Vol. 10, Issue 3, pp. a651–a652) [Journal-article]. https://ijrti.org/papers/IJRTI2503083.pdf
[10] Ramachandran C., 'PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age' [2014]

established legal concepts, laying the groundwork for future privacy and surveillance policy in India.

How surveillance poses a threat to Privacy?

State surveillance threatens privacy and alters how personal information is handled and safeguarded. One major worry is the massive gathering of data. Governments may collect vast information on individuals, including correspondence, internet habits, and personal data. Excessive data collection might violate privacy by exposing people's private lives without their consent. Another issue is surveillance's stifling effect on free expression.[11]When individuals are aware they are being observed, they may self-censor or avoid specific activities for fear of consequences. Suppression of free speech and participation can harm democratic processes and prevent healthy public conversation. Furthermore, abuse of power poses a serious risk. Surveillance tools and data can be misused by authorities for personal, political, or discriminatory goals. Misuse can lead to harassment, oppression, or targeted attacks against persons or groups, raising serious ethical and legal implications. The security of acquired data is also a significant problem. Surveillance can expose sensitive information to breaches, hacking, and unwanted access. Compromising this data poses major privacy and security implications for individuals affected.[12]Many surveillance programs lack supervision and accountability, which raises concerns. Inadequate checks and balances can lead to invasive surveillance tactics, eroding public trust and undermining the rule of law. Furthermore, the normalization of surveillance has the potential to steadily erode society privacy norms. As monitoring grows more frequent, the acceptable boundaries of surveillance may extend, compromising privacy and limiting individual freedoms. Surveillance also increases the likelihood of false positives and misidentification.

Automated technologies, such as facial recognition technology, may falsely identify or designate innocent individuals as suspects. This can lead to wrongful behavior, stigma, and a general sense of unease. Finally, the loss of identity is a major problem. Surveillance lowers anonymity, which is crucial for privacy and freedom of expression. This effect applies to both online and offline behaviors, making people more susceptible to observation and control. To

[11] Schauer F., 'Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"' [1978] 58 BU L Rev 693
[12] Addison Litton, "The State of Surveillance in India: The Central Monitoring System's Chilling E s Chilling Effect on Self-Exprect on Self-Expression", Washington University Law Review, 2015 https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_ globalstudies, at 816

address these risks, it's important to strike a balance between security and privacy. Oversight mechanisms should be in place to guarantee that surveillance methods do not violate fundamental rights.

National Security vs Privacy Rights

The debate over national security and privacy highlights a fundamental problem in democracies: should expanded surveillance or personal privacy be prioritized? Proponents say that more monitoring is necessary to combat threats including terrorism, cybercrime, and external aggression. In countries like India, where geopolitical tensions and internal terrorism are major issues, effective surveillance is essential for preventing threats, monitoring cyber activity, and protecting national sovereignty. Surveillance can assist prevent and control cybercrimes, which are becoming more complex in the digital age. Critics argue that prioritizing monitoring over privacy could lead to significant misuse and abuse of power. Without proper controls, collected data could be misused for political repression or rights breaches, threatening democracy. Proponents say that extensive monitoring undermines democracy's core principles of transparency and accountability, limiting free speech and dissent. Individuals may self-censor or change their conduct to avoid inspection, potentially limiting democratic liberties and hindering innovation and growth. The discourse highlights the challenge of balancing security and individual rights.

5. Conclusion: Privacy versus Secrecy – How Much is Too Much?

How can society be certain that decision-makers will utilize secrecy and monitoring to strengthen national security rather than concealing corruption, mismanagement, and misjudgment? How can democratic nations explain to the public that the current surveillance system strikes the optimal balance between maintaining the country's strategic edge over competing states and ensuring society's right to know about political processes? How can a counter-terrorism head advise the public that a specific monitoring strategy has reduced the number of terrorist attacks, hence improving the program's credibility, without giving the method or avenue to the extremist groups targeted? How can the public and/or parliament be confident that if the counter-terrorism chief discloses the success of the surveillance program, he is not selectively utilizing data to conceal the program's shortcomings and abuses? The answers to these concerns are not only difficult, but also cultural, taking into account a country's security, institutional, managerial, and organizational cultures. The twenty-first century has

seen deep transformations such as monitoring, which are being driven by rapid technological improvements.

The growth of government surveillance has led to worries about privacy and individual rights. In India, various rules and regulations govern this complex subject, including the Indian Telegraph Act of 1885, the Information Technology Act of 2000, and the Digital Personal Data Protection Act of 2023. The Unified License Agreement and other regulations distinguish between targeted and mass surveillance authorities, creating a complex environment of state surveillance. Legal and judicial structures provide protection from arbitrary surveillance. These laws include statutory barriers that limit the scope of surveillance.

The Supreme Court's decision in K.S. Puttaswamy v. Union of India established privacy as a fundamental right, breaking down legal barriers. These obstacles try to protect citizens from excessive surveillance powers. However, real-world applications can reveal shortcomings, such as when unlawfully obtained evidence is used to discredit judicial proceedings. The Justice Shah and Srikrishna Committees' recommendations on India's surveillance system emphasize the need to strike a balance between state security and privacy. The Supreme Court's progressive approach raises concerns that recent legislation, including the Personal Data Protection Bill, may still give government agencies too much discretion. The proposed exception clauses in the Bill raise concerns about potential abuses and require immediate legal amendment to conform with international human rights norms. Emerging technologies such as artificial intelligence, facial recognition, and the Internet of Things present potential and difficulties for surveillance and privacy. They offer major privacy and civil rights risks. To address these challenges, legislative and policy reforms should include strong data protection legislation, improved oversight systems, and safeguards against technology breakthroughs that endanger fundamental rights. India must strike a careful balance between national security and privacy. To prevent misuse, we need broad legal reforms, technology-specific solutions, and improved oversight systems. Civil society has a significant role in lobbying for reforms, as seen by successful campaigns against intrusive measures like the Aarogya Setu app mandate. In conclusion, India's surveillance and privacy situation exemplifies the global battle to combine security and personal freedoms. To address rapid technology advances and security problems, the country must prioritize democratic principles, strong legal protections, and transparent governance. Maintaining a balance between protecting individual rights and sustaining democracy is crucial for India's surveillance state. Digital surveillance supervision must strike

a balance between an impetuous executive seeking to maximize authority and an inquiring public concerned with preventing corruption, mismanagement, and abuse. The executive and security-intelligence communities will naturally attempt to escape oversight, and the public will always have a maximalist view of transparency, which will remain impossible given governments' security dilemmas. Oversight mechanisms will fail to balance if they lag behind technology advances in the surveillance-privacy arena or take too long to monitor the secrecy process. This means that, like offline democracy, internet democracy is only as effective as its supervision procedures and safeguards.