CONSTITUTIONALITY OF NPR-NATGRID INTEGRATION: A THREAT TO PRIVACY IN INDIA

Surbhi Kaushal, BALLB, Mumbai University, Mumbai

Mahesh Giri, BALLB, Mumbai University, Mumbai

ABSTRACT

Surveillance has occupied much of the discussion in most parts of the world. This paper critically examines the constitutionality of India's National Population Register (NPR) and the National Intelligence Grid (NATGRID) framework, with particular emphasis on their implications on the right to Privacy under Article 21 of the right to life and personal liberty mentioned in Part III of the Indian Constitution. While both frameworks have been justified on multiple grounds, such as administrative efficiency and national security, the heat of the arguments has centered around concerns about the absence of accountability, transparency, and adequate safeguards.

The integration of NPR and NATGRID raises several concerns regarding the scale, scope, and purpose of data collection and their usage. The study first analyses both NPR and NATGRID in isolation, concentrating on their objectives, statutory backing, and their implementation. Further, it evaluates the potential consequences of their integration in light of the aggregation of data for profiling and surveillance.

The paper further focuses on the K. S. Puttaswamy v. Union of India (Adhaar) case, drawing upon the grounds laid down in the judgment. The paper argues that such integration risks undermining the principles of proportionality, necessity, and informed consent. The paper further compares and analyses the surveillance systems of the USA, China, and the UK. And ultimately argues that the integration of NPR and NATGRID poses a significant threat to privacy and asks for constitutional scrutiny, along with the establishment of robust legal frameworks.

INTRODUCTION

"You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized."

- George Orwell, 1984

In the contemporary era, digital interaction constitutes a huge portion of our lives. In each of our activities, whether calls, messages, emails, or financial transactions, we leave an enormous amount of digital footprint behind. This footprint consists of metadata that can be stored, analysed, and surveilled, often without our explicit consent or knowledge.

Surveillance in the digital space is still evolving, posing several challenges to governance and jurisprudence. The concern isn't merely due to the existence of surveillance, but its transformation as a tool for undermining individual autonomy, the misuse of personal data for profiling, and the erosion of a person's personal life, civil liberties and the violation of private person's right to privacy, often exacerbated in the absence of any oversight, be it of judiciary or of any autonomous body coupled with a seemingly fragmented and inadequate legal framework and remedial mechanism.

In India, after the Mumbai terror attack, resulting from a massive intelligence failure in 2008, the concept of the National Intelligence Grid (NATGRID) came into the picture. NATGRID is an integrated, centralized intelligence-sharing framework intended to support the counterterrorism capabilities of the nation-state. NATGRID provides a platform that allows linkage between 21 databases and the 11 major agencies that have access to it. It facilitates the linkage of fragmented data in order to identify, track terrorists, and prevent terrorist activities.[1]

As of April, 2026, NATGRID has been officially integrated with the National Population Register (NPR). NPR is a comprehensive digital database having information on the identity of the usual residents, be it Indian or foreigner, living in the country for at least six months or intending to live for the next six months. The NPR database includes the demographics and biometrics particulars.[2]

[1] BS WEB TEAM, *Natgrid to Scale up surveillance, Offer real-time Intel on Individuals*, Business Standard (2023), https://www.business-standard.com/india-news/natgrid-to-scale-up-surveillance-offer-real-time-intel-onindividuals-123042800263_1.html. (last visited Apr 20, 2026).

[2] NATGRID–NPR integration, Drishti IAS (2024), https://www.drishtiias.com/daily-updates/daily-newsanalysis/natgrid-npr-integration (last visited Apr 19, 2026).

An increase in the amount of integration of citizens' sensitive data raises concerns on the grounds of privacy. After the landmark judgement of K. S. Puttaswamy v. Union of India, a constitutional recognition was given to the right to privacy, declaring it as a fundamental right protected under Article 21 of the right to life and personal liberty. [3]This integration necessitates a critical examination of whether such data integration aligns with the constitutional mandates.

This paper seeks to examine how the integration of the National Population Register within the ambit of NATGRID impacts the right to privacy of the people protected under Article 21 of the Constitution. Further, this paper examines whether this integration is in line with the proportionality test established in the Puttaswamy Judgement. It argues that while such integration may serve legitimate state interests, the absence of adequate safeguards and oversight mechanisms raises serious concerns regarding its constitutional validity.

RESEARCH QUESTION

How does the integration of the National Population Register (NPR) within NATGRID's ambit affect citizens' right to privacy under Article 21 of the Constitution of India?

PART I – THE CONCEPTUALISATION OF NATGRID

After the devastating attack of 26/11 by ten transnational terrorists of Lashkar-e-Taiba (LeT) targeted at prime locations in Mumbai, the entire country was in shock and agony. India had to pay a hefty price of 164 lives.[4] The whole incident raised many questions before the intelligence agencies, did the first responders of the Mumbai police prove to be completely worthless in their position? Was the National Security Guard too slow? Were the State and Centre inadequate to protect their people? The intelligence establishments were in disarray, and hence, in the wake of the 2008 Mumbai terror attack, the then Home Minister, Chidambaram Palaniappan, envisioned NATGRID (National Intelligence Grid).[5]

[3] Fundamental right to privacy, Supreme Court Observer (2025), https://www.scobserver.in/cases/puttaswamy-vunion-of-india-fundamental-right-to-privacy-case-background/ (last visited Apr 20, 2026).
[4] Shanthie Mariet D'souza, *Mumbai terrorist attacks of 2008 | events, Death toll, & facts*, Encyclopædia Britannica (2019), https://www.britannica.com/event/Mumbai-terrorist-attacks-of-2008. (last visited Apr 19, 2026)
[5] Home Ministers Speech at the 22nd Intelligence Bureau Centenary Endowment Lecture :: South Asia Terrorism Portal, Satp.org (2026), https://www.satp.org/satporgtp/countries/india/document/papers/09dec25pib.htm (last visited Apr 19, 2026). [6] The Wire Staff, *Full Text: What the High Level Inquiry Committee on the 26/11 Attacks Had to Say*, The Wire (2019), https://thewire.in/security/26-11-mumbai-terror-attack-inquiry-committee (last visited Apr 20, 2026).

In September 2008, the Research and Analysis Wing (R&AW) of the Government of India intercepted a satellite phone conversation from Pakistan indicating a sea-borne attack on Mumbai hotels.[6] They even tracked the laptop of the technological head of LeT but failed to realise the imminent necessity to take immediate action. In February 2008, the Uttar Pradesh (UP) Police arrested Faheem Ansari, a LeT operative, carrying hand-drawn maps and video footage of the Taj Mahal Hotel, Oberoi Hotel, and CSMT station.[6] The UP Police was not able to communicate this information with R&AW as during those times, there were no channels for the two entities to communicate.

The passive formation of "Information silos," which could have otherwise been prevented turned out to be one of the main reasons for the attack. Multiple agencies held critical data, but as they operated in their own silos with no communication between the agencies, none of the agencies were able to fully grasp the bigger picture.[7]

Consequently, after the attack, as a measure to counter terrorism and make the crucial agencies communicate effectively, in early 2009, NATGRID was conceptualised. It was envisioned that under this framework, 21 sets of databases will be networked to achieve quick, seamless, and secure access to desired information for intelligence and enforcement agencies. These 21 databases included records from public and private Banks, Credit Card companies, the Income Tax Department (PAN/ITR), SEBI, the Financial Intelligence Unit (FIU-IND), VAHAN (vehicles) and SARATHI (licenses) portal, Telecom subscriber KYC and Call Detail Records (CDRs), and movement tracked by the Airlines (PNR), the Indian Railways, and the Bureau of Immigration.[8]

Before becoming operational in July 2023, NATGRID signed an MoU with the National Crime Records Bureau (NCRB) to access Crime and Criminal Tracking Network System (CCTNS) a database that links around 14,000 police stations.[9] Further on, after the DGP/IGP Conference (held in early 2024 and 2025), the Ministry of Home Affairs instructed states to scale up the

[6] Sujit Nath, *Fitting Mumbai"s Terror Jigsaw*, India Today (2008), https://www.indiatoday.in/latestheadlines/story/fitting-mumbai-s-terror-jigsaw-34732-2008-12-07 (last visited Apr 19, 2026).
[7] D'souza, "Mumbai Terrorist Attacks of 2008, https://www.britannica.com/event/Mumbai-terrorist-attacks-of2008. (last visited Apr 19, 2026)
[8] BS WEB TEAM. 2023. Natgrid to scale up surveillance, https://www.business-standard.com/indianews/natgrid-to-scale-up-surveillance-offer-real-time-intel-on-individuals-123042800263_1.html. (last visited Apr 20, 2026).
[9] NATGRID-NCRB Sign MoU to Link 14,000 Police Stations, Gktoday.in (2020), https://www.gktoday.in/natgrid-ncrb-sign-mou-to-link-14000-police-stations/ (last visited Apr 19, 2026).

use of NATGRID for all investigations, the access to NATGRID was then given to the Police Stations, restricted only to officers at the rank of Superintendent of Police (SP) and above.[10]

On 08th April, 2010 a meeting by the Cabinet Committee on Security (CCS) that was chaired by then-Prime Minister Manmohan Singh, directed the Home Ministry to prepare a Detailed Project Report (DPR) which was reviewed a year later by CCS formulating operational boundaries of the system[11] and restricted access of NATGRID to only 11 specific central agencies, like the Intelligence Bureau (IB), the Research and Analysis Wing (R&AW), and the National Investigation Agency (NIA), the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), the Financial Intelligence Unit (FIU-IND), the Directorate of Revenue Intelligence (DRI), the Central Board of Direct Taxes (CBDT), the Central Board of Indirect Taxes and Customs (CBIC), and the Directorate General of GST Intelligence (DGGI), and Narcotics Control Bureau (NCB).[12] Through a formal letter to the DGPs of all states on 06th July, 2025 by Piyush Goyal, the-then CEO of NATGRID requested their district

Superintendents of Police (SPs) to proactively use the NATGRID portal. This expansion of NATGRID access has only increased the systematic risks regarding data security and constitutional privacy.[13]

State-sponsored cyber-attacks are cyber-attacks systematically and financially supported by the government of one nation-state against the organizations, individuals and governments of other nation-states.[15] The proverb *"don't put all your eggs in one basket"* questions the convenience of most databases being integrated to one portal. i.e., NATGRID. State-sponsored cyber-attacks are highly sophisticated and well-resourced as they are backed by fundings from their host nation-state. Such breaches target high-level officials and compromission of personal data collected through the databases. According to CERT-IN, India in 2025 alone reported

[10] Vijaita Singh, *National Intelligence Grid Slowly Gathers pace, Receives 45k Requests a Month*, The Hindu (2025), https://www.thehindu.com/news/national/national-intelligence-grid-slowly-gathers-pace-receives-45krequests-a-month/article70369184.ece (last visited Apr 19, 2026).
[11] Rsd Debate, https://rsdebate.nic.in/bitstream/123456789/595008/1/IQ_223_24082011_U2386_p125_p125.pdf (last visited Apr 20, 2026).
[12] Apar Gupta, *"Natgrid", the Search Engine of Digital Authoritarianism*, Internet Freedom Foundation (IFF) (2026), https://internetfreedom.in/natgrid-the-search-engine-of-digital-authoritarianism/ (last visited Apr 19, 2026).
[13] Express News Service, *MHA Advises States to Use NATGRID Database to Control crimes, Criminals*, The New Indian Express (2025), https://www.newindianexpress.com/nation/2025/Jul/06/mha-advises-states-to-usenatgrid-database-to-control-crimes-criminals (last visited Apr 19, 2026). [15] IMI, *State Sponsored Cyber Warfare*, Identity Management Institute® (2023), https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/. (last visited Apr 19, 2026)

29,44,248 cyber security incidents.[14] The centralized nature of NATGRID makes it an attractive target for the hacking-groups to gain personal information. And the recent integration of NPR within NATGRID has made it even more an attractive target for the cyber-attacks as it can potentially allow the hacker for hyper-personalized attack against their key targets.

PART II – HISTORY OF NPR, RELATION WITH UIDAI AND INTEGRATION WITH NATGRID

The origins of large-scale identity databases can be traced back to the national security concerns raised after the Kargil war in 1999. The issue of immigrants infiltrating into the Indian territories posing as citizens of the nation-state in the border regions stood out particularly. The Indian government's response to this was to establish a comprehensive identity system. This further led to proposals such as a Multi-Purpose National Identity Card (MNIC), and with that, the course of discussions was engrossed on a Centralized population register.[15] The formalization of the same was done through various amendments and legislations under the

Citizenship Act of 1955, laying the foundational groundwork for the population register and verification of identity across the nation. The National Population Register (NPR) is a database containing information on the identity of the usual residents regardless of their status, prepared under the provisions of the Citizenship Act, 1955, and the Citizenship (Registration of Citizens and issue of National Identity Cards) Rules, 2003. Under the acts, it has been made mandatory for every usual resident of the country to register under the NPR.[16]

After the initial conceptualization, NPR was conducted through a pilot project in the coastal areas between 2009 and 2011. The first nationwide data collection was conducted in 2010 (during the 2011 census house-listing phase), which recorded basic demographic details such as the name, age, sex, and address of the residents. In 2015, the database was updated via doorto-door listing and started integrating Aadhaar Numbers and mobile details to enable digital linkage.[19] The proposal of 2020-21(now postponed) aimed at the expansion of

[14] Assistance to States to Tackle Cyber Incidents, Pib.gov.in (2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504®=1&lang=1 (last visited Apr 19, 2026).
[15] Multipurpose National Identity Card, Recall from 2003, Sabrangindia (2020), https://sabrangindia.in/multipurpose-national-identity-card-recall-2003/ (last visited Apr 20, 2026).
[16] Srinivas Kodali, *Digital India on Steroids: How Aadhaar Infra Enables the NPR and the NRC*, The Wire (2019), https://m.thewire.in/article/tech/aadhaar-infra-npr-nrc (last visited Apr 20, 2026). [19] vasureddy, *NRC the Need of the day.. Implement or Perish*, MyVoice (2020), https://myvoice.opindia.com/2020/02/nrc-the-need-of-the-day-implement-or-perish/?hl=en-IN (last visited Apr 19, 2026).

demographics from 15 to 21 and even introducing an app-based data collection. This phase aimed to collect additional personal information, including parents' date of birth and previous residence, while also allowing voluntary submission of optional data, including Aadhaar number, Pan number, Passport number, voter ID, and driving license number, Mobile number, details of father, mother and spouse.[17] As for the biometrics, NPR itself doesn't directly collect them, but it is linked with the Aadhaar database maintained by the Unique Identification Authority of India (UIDAI), which already stores biometrics such as fingerprints, iris scans, and photographs. Thus, over time, NPR has evolved from a simple population register to a more integrated and frequently updatable resident database.[18]

NPR AND EXCLUSIONISM

NPR is primarily conceived as a neutral and harmless population database, but its operational design reveals concern. For instance, NPR wasn't just a normal database with the records of the citizens of the country: instead, it included information of the usual residents, meaning anyone who was living in a certain area for a certain period of time was required to provide their details as mandated under the statutes.[19] Moreover, the wide discretionary power given to the office, as low as a local sub-registrar for the task of labelling of 'doubtful' individuals, is alarming, as it leaves room for subjectivity in the presence of biases, as well as the abuse of power that can take place in the process of identification. Additionally, the local sub-registrar is required to maintain records of those individuals whom other non-doubtful individuals deem as 'doubtful'. In the absence of clear, uniform, and transparent criteria governing such classification, it introduces ambiguity into the process, thereby potentially opening the door to arbitrariness, often accompanied by officers' biases, leading to further discrepancies and misuse of authority. Consequently, a normal data collection exercise can raise doubt and suspicion among the local population. In addition, "non-doubtful" residents may informally influence or even validate the classification of others as "doubtful". The system risks reinstating pre-existing social hierarchies, allowing prejudice and biases to affect the administrative outcomes.

[17] NPR 2020: What Does It Want to know? | SabrangIndia, SabrangIndia (2020), https://sabrangindia.in/npr2020-what-does-it-want-know/ (last visited Apr 20, 2026).
[18] Kodali, *Digital India on Steroids* https://m.thewire.in/article/tech/aadhaar-infra-npr-nrc (last visited Apr 20, 2026).
[19] Usha Ramanathan, *Implications of registering, tracking, Profiling*, (2010), https://www.ielrc.org/Content/n1001.pdf (last visited Apr 19, 2026).

When viewed in conjunction with the National Register of Citizens (NRC), NPR becomes the first step in the three-step chronology of an exclusionary framework that forces individuals to provide proof for the validation of their citizenship. NPR serves as an effective foundational database from which NRC is derived. Individuals who get authenticated through the NPR are included in the NRC. As for those who remain "doubtful", they are removed from the framework, citing for further verification. In such a situation, the burden of proof falls onto the individuals, requiring them to somehow establish the affirmation of their citizenship. Through such a framework, the conventional presumption of citizenship is reversed and replaced by the conditional recognition of citizens, dependent upon as haphazard as bureaucratic validation. This process for the ones excluded isn't just time-consuming but also resource-intensive, which disproportionately affects the poor and marginalized, who are less likely to possess the required documents to prove their identity, and less likely to be able to sustain prolonged legal battles. Moreover, being put in the doubtful categorization often comes with the consequences of disenfranchisement, exclusion from welfare schemes, and social stigmatization, often further weakening the vulnerable.

A troubling side to all of this is the potential of statelessness that can be caused through the NPR and NRC. The Citizenship laws have considerably narrowed down in their criteria of Citizenship by birth, this is especially the case for individuals born between 1987 and 2003, and after 2004. Anyone born between 1987 and 2003 to immigrant parents is ineligible to avail citizenship by birth, and anyone born after 2004 to one Indian parent and one illegal migrant is also ineligible.[20] Not surprisingly, children born to parents with disputed citizenship status or in the "doubtful" category may themselves have the same when it comes to their own citizenship. This creates a dichotomous situation wherein individuals, despite having lived their whole lives in India, serving the country, having no meaningful connection to any country but India, are rendered outsiders in their own nation. The prospect of inheriting statelessness at birth raises several constitutional as well as humanitarian concerns, for something like this is entirely beyond the control of a person, like the status of a parent.

Unlike its portrayed image, the NPR-NRC framework disproportionately impacts the poor and disadvantaged, often the ones who are also the religious minorities, or even the ones who are historically disadvantaged communities like the Dalits and Adivasis, because these are the

[20] The Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, People's Archive of Rural India (2019), https://ruralindiaonline.org/hi/library/resource/the-citizenship-rules-2003/?hl=en-IN (last visited Apr 19, 2026).

individuals who are less likely to be able to produce the required documents for proof. Thus, the system further risks exacerbating the patterns of marginalization.

Compounded with the Citizenship Amendment Act, there is an additional layer of complexity. Although NPR-NRC renders people as "Doubtful", it provides a pathway for citizenship for specific religious minorities from neighboring countries, but explicitly excludes Muslims from this ambit. These further shed light on the asymmetrical landscape, wherein individuals of similar status are treated differently based on their religious identity. It is clear from the chronology that NPR and NRC function not in isolation, but as broader components of legal and political strategy, within which exclusion and selective inclusion occur simultaneously.

NPR AND SURVEILLANCE

The NPR, after 2011, shifted extensively from a conventional documentation of population to a thorough regime of data collection and state surveillance. Unlike the census, NPR not only includes demographic data but also biometric data of residents above a certain age. While the exercise of biometrics collection is generally framed as a technological advancement and even an administrative necessity, it is worth noting that data collection isn't done in isolation. In fact, such a database is incorporated into a broader ecosystem designed with the intent of surveillance.

The NPR framework crosses paths with the NATGRID and the UID (the Unique Identification Project); The compiled database of NPR is shared with the Unique Identification Authority of India (UIDAI) for de-duplication, the integration of the same has been encouraged by the Union Home Ministry, with the explanation of national security as grounds for tracking and surveillance by the state and its agencies.[21] This integration transforms a static repository of data into a tool that might be considered state-led mass surveillance and interference into the personal lives of the people. NATGRID, for instance, is designed to enable multiple intelligence and security agencies to access data from 21 categories of databases, including railway and air travel, income tax, phone calls, bank account details, credit card transactions, visa and immigration records, property records, and the driving licenses of citizens. When combined with the databases of NPR and Aadhaar, such an integration would enhance the performance of the state in creating detailed profiles of individuals. This is worrying, given

[21] Vajiram Editor, *Vajiram Editor*, Vajiram and Ravi (2026), https://vajiramandravi.com/upsc-exam/nationalpopulation-register-npr/?hl=en-IN (last visited Apr 19, 2026).

what may emerge through this if the state has the technical ability to profile individuals across different walks of life. The Aadhar linkage is particularly significant here, even though it is officially limited to only identity verification, it is capable of linking separate data sets, enabling the compilation of information on a particular individual's profile. With such an integration, the lines of identification and surveillance tend to blur, as the summation of seemingly harmless databases on close surveillance can reveal intimate details of an individual's personal life, including their patterns of behavior, associations, and even their personal history.

Implications of such an integration are severe enough to fundamentally alter the relationship between the state and an individual. In a constitutional democracy such as India, the state derives its power from the consent of those governed and the citizens of this country; the rights possessed by the citizens put limits on the power of the state. However, a system that constantly mandates citizens to disclose personal information, marked by constant visibility and traceability, risks straining the pre-existing relationship between the state and its citizens. Under such a framework, a nation can start resembling an Orwellian state, wherein individuals can resemble "subjects" under constant surveillance and monitoring, rather than being free citizens of a free nation.

Unlike the Census Act of 1948, which contains explicit provisions on maintaining the confidentiality of the information collected from the population and strictly prohibiting the data from being used as evidence, the NPR does not provide any close safeguards; on the contrary, the NPR is designed so that sharing and integration of the collected data is possible. This is, of course, a shift from the conventional data collection with the intent of policy planning to a more invasive data profiling used for broader state purposes.[22]

The aggregation of personal data gives rise to several vulnerabilities in terms of privacy breaches, unauthorized access, and misuse of such a huge repository containing very personal data. Once collected, the information doesn't disperse; instead, it is always accessible, meaning the state has access to records that can endure the test of time. This raises questions not just about the surveillance activities in the present but about the future of the data collected by the state, in ways that weren't even originally consented to.

[22] Ramanathan, *Implications of registering* (2010), https://www.ielrc.org/Content/n1001.pdf (last visited Apr 19, 2026).

Such a concentration of data with the state agencies without proper oversight mechanisms increases the risk of abuse. The proposed functions of NATGRID, that allows multiple intelligence and enforcement agencies access to integrated databases, are already surrounded by concern and controversy due to the inadequacy of safeguards and lack of accountability. Moreover, the absence of any parliamentary or judicial oversight mechanisms further exacerbates these concerns of the data being used beyond the purposes of national security, including political surveillance and state control.

Another impact of such surveillance activities is the fact that they're not evenly distributed. Marginalized communities are already subjected to scrutiny and possess limited resources to seek state action, and are therefore more likely to bear the impact of intrusive practices. The integration of NPR with NATGRID risks reinforcing pre-existing patterns of exclusion and discrimination, particularly alongside mechanisms like the NPR-NRC framework that already create suspicion about a part of the population.

PART III – CULTURAL ETHOS AND THE PUTTASWAMY TEST

The traditional and cultural ethos of the general Indian population has historically framed privacy through a more communal and collective rather than individualistic lens; the familial structure of the 'joint family' has made the physical and emotional boundaries of a private person more fluid. Due to these factors, in the digital era, as the Indian society transitions from a low-tech society to one of the most data-intensive economies in the world, there is an overall lower level of concern about privacy in India compared to Western nations like the United States. The lack of information and a culturally communal approach towards data and information sharing have given rise to a 'privacy paradox' wherein Indians are more likely to portray that they are concerned about privacy in surveys than in actuality. They are more likely to trade off their digital privacy for immediate rewards like social validation and convenience.[23]

This cultural inclination towards trading off personal data for day-to-day convenience, to avail services like UPI, Aadhaar Card, or government subsidies, opens a door for the government and MNCs to hoard an array of metadata left unattended by the population.' To protect its citizen from the realised or unrealised privacy breaches, Retired Justice K. S. Puttaswamy took the matter in his own hands and filed a writ petition in the Apex court of the country challenging

[23] "Nobody Should Control the End user": Exploring Privacy Perspectives of Indian Internet Users in Light of DPDPA, Arxiv.org (2016), https://arxiv.org/html/2508.17962v1 (last visited Apr 19, 2026).

the constitutional validity of the Adhaar Scheme, which established no checks on the power of the government to use the biometric data collected[24] Justice K. S. Puttaswamy demanded 'Right to Privacy' as a fundamental right. The court ruled unanimously on August 24th 2017, recognising privacy as a fundamental right guaranteed by the Constitution.[25]

The judgment also established that privacy, although a fundamental right that every citizen holds, is not absolute. Right to Privacy can be overridden if the state provides compelling evidence to pass the 'Proportionality Test'. If passed, through this test, the state's legitimate interests are duly safeguarded.

The proportionality test is the standard used by the Supreme Court and High Courts to determine if a government action reasonably restricts a citizen's fundamental rights. A government action must satisfy four criteria's: (a) Whether there exists a valid, good law that authorises the state's action, (b) Whether or not the state's action serve a legitimate state interest for the public good, (c) Whether there exists a rational nexus between the means and the end, i.e., the action taken by the state and the ultimate goal it wants to achieve, (d) Whether or not the intended action of the state is the least intrusive method to achieve their ultimate goal.

The first requirement **(PRONG 1)** is the existence of a clear, valid and good statutory law that grants power to the state to take any action. NATGRID was conceptualised, brought into development, and implemented all without a good statutory law that allows it to be established. Although the conceptualisation and establishment are supported by Article 77(3) of the Constitution of India. The act of collecting, linking, or processing the private data of citizens is not supported by any law.[26] Article 77(3) only allows the formation of an agency, it is a substantive law, for the agency to work it requires a procedural law, which does not exist. This absence of a clear procedural law is violative of the fundamental rights of the citizens under Article 21.[27]

NATGRID was established via a Cabinet Committee on Security (CCS) executive order in 2009. Section 24(1) states that the Right to Information Act does not apply to the intelligence

[24] Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2019) 1 SCC 1 (2018). 53 ¶ 531 (India).
[25] *Fundamental right to privacy,* Supreme Court Observer (2025), https://www.scobserver.in/cases/puttaswamyv-union-of-india-fundamental-right-to-privacy-case-background/ (last visited Apr 20, 2026).
[26] "Indian Constitution," § 77(3) (1950).
[27] "Indian Constitution," § 21 (1950).

and security organizations specified in the Second Schedule.[28] On June 9, 2011, the Department of Personnel and Training (DoPT) issued a gazette notification (G.S.R. 442(E)) adding NATGRID to the Second Schedule of the RTI Act which exempted it from transparency requirements and disclosure to the public.[29] Referring to the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 the government justified the "automated access" to data from 21 provider organizations, categorizing NATGRID as a "middleware" platform rather than a data-collector itself. The government argues that that since 10 specific agencies (like IB, RAW, and NIA, etc.) are already authorized to intercept data, NATGRID is simply the technical facility through which they exercise that power. The absence of a dedicated statutory framework for NATGRID means there is no parliamentary oversight, making the state's action of integration legally failed under the standards of first prong test.

The second requirement **(PRONG 2)** is establishment of legitimate state interest for the state to be taking such any action. Prima facie, as a democratic welfare state, it does have a legitimate interest of National Security, yet it is complex to assume and answer this Prong as the protection of the fundamental rights of the people is another legitimate state aim. When the two interests are conflicting with each other the least intrusive method should be preferred over the other and that is Prong 4.

The third requirement **(PRONG 3)** is to establish a rational connection between the state's action (means) and the goal this action tries to achieve (ends). To feed the data of over every person residing in India, regardless of nationality using National Population Register, is the "means" of the state. The government has emphasised that NPR data would be used only for development planning and welfare administration, that is the "end" government wants to achieve. If we broaden out our scope and consider how other the democracies balance out public welfare and rights of the people, it can be observed in the case of USA that National Counterterrorism Center (NCTC) with their tools flag out those who are known or suspected international terrorists and then take an action, that is contrary to how India deals with it. Instead of integrating the data of every single citizen and non-citizen with NATGRID, as the

[28] "Right to Information," § 24(1) (2005), https://rti.dopt.gov.in/Writereaddata/RTI%20Act,%202005%20(Amended)-English%20Version.PDF. (last visited Apr 19, 2026).
[29] Ministry of Personnel, Public Grievances and Pensions (Department of Personnel and Training) Gazette Notification, (2011), https://documents.doptcirculars.nic.in/D2/D02rti/1_3_2011-IR09062011.pdf (last visited Apr 20, 2026).

most rational step for counterterrorism, the government should integrate only the data of those who are known and suspected. Hence, the nexus between the means and ends do not align perfectly, failing the prong.

The final requirement **(PRONG 4)** is a question of the least intrusive method, whether the action taken by the state is least intrusive to those who can or are getting affected by it. The NPR-NATGRID linkage is fundamentally not the least intrusive/restrictive method relative to the goal of either of these systems. Welfare of the people and National Security is achieved not by compromising and keeping a watch on every single person in the register, it is done so by keeping a watch on the known criminals and suspected persons. Before the personal data of persons enter in the NATGRID framework, there should exist a filter which singles out the suspected to the safe persons and then the information of the suspected persons should be feed into the said framework. Integrating every single person all at once makes the framework and attractive target for State sponsored cyber-attack, and the suspicion of mass surveillance becomes an uncomfortable dilemma in the minds of the people.

Without a specific law and rigorous judicial oversight, the NPR-NATGRID integration constitutes an overreach that fails the proportionality test and is violative of the core tenants of the Puttaswamy judgment.

PART IV – COMPARATIVE STUDY OF SURVEILLANCE SYSTEMS ACROSS THE GLOBE

For the comparative study, we shall take the assertion of authoritarianism and how invasive these systems are in different parts of the world as the frame of reference. The group of comparison is India, USA, UK and China. This study looks at the systems encroachment over the private lives of the people.

Every nation-state, be it democratic, dictatorship or where religious fanaticism is prominent, boasts a techno-authoritative approach with their surveillance systems. The main aim of mass surveillance is National Security, Counter-Terrorism, Political Control and Suppressing Dissent, the former two are common justifications given by the countries and the latter two are hidden agendas. NATGRID since the very inception did not have any legislative or statutory framework governing it or having an oversight. NATGRID has a complete executive autonomy as there exists virtually no good laws which keep the system in check and prevent it from

harming the fundamental rights such as the right to privacy. As a welfare state, the people of India should be of utmost importance to the government, the protection of the people should be of paramount concern. When NATGRID was conceptualised, its only purpose revolved around measures and interaction between databases for national security and counter-terror measures, which are, again, the common justification given by any nation-state. As of April, 2026 the scope of NATGRID has expanded its horizons. After integrating with NPR, it can now perform AI-driven behaviour analysis for mass-surveillance and as it is accessible to state police, it can map the "family tree" and identity of nearly 1.2 billion citizens.

Although India claims to maintain an air-gapped segmentation, the government cannot do away with exclusively keeping the system isolated; in order to do analytics and real-time intelligence the crucial supposed air-gapped systems have to be connected with the rest of the network as emphasised by Phil Neray, the vice president of industrial cybersecurity for CyberX[30]. India shall not be keeping its servers disconnected to the rest of the network. And even in the exceptional case scenario if the air-gap is maintained, the use of USB drives or SD cards for software updates, firmware patches, or backups is a primary way for the malware to enter isolated networks. It is one of the most common tactics used by state-sponsored cyberattacks, for example Pegasus[31]. Hence, the personal data of those who are subject to it is always at risk.

In the United States, the infrastructure that primarily analyses and integrates all intelligence possessed by the U.S. government pertaining to terrorism is the National Counterterrorism Center (NCTC). It operates under the Office of the Director of National Intelligence (ODNI), it serves as the centre designed to prevent another intelligence failure like 9/11. It utilises Terrorist Identities Datamart Environment (TIDE) a tool that stores everything from biometrics (fingerprints, facial scans) and DNA to social media handles and travel history.[32] It has a classified database containing the identities of over 2 million known or suspected international terrorists (KSTs). The difference between India's counter terror mechanism and the USA's that the former does not actively classify only the known and suspected international terrorists it takes a general approach of storing every person's personal data, this raises number of red flags

[30] Ericka Chickowski, *Should Trump Tackle Air-Gapped Critical Infrastructure?*, Dark Reading (2017), https://www.darkreading.com/vulnerabilities-threats/should-trump-tackle-air-gapped-critical-infrastructure- (last visited Apr 20, 2026).
[31] Pegasus Spyware, Drishti IAS, https://www.drishtiias.com/daily-updates/daily-news-analysis/pegasusspyware-1 (last visited Apr 20, 2026).
[32] The National Counterterrorism Center, *NCTC*, Dni.gov (2018), https://www.dni.gov/index.php/nctc-home (last visited Apr 20, 2026).

as to what can the stored data be used for.

Another main distinction between NATGRID and the operations within the purview of NCTC is that the latter has a strict legal mandate to adhere to. The general provisions of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the National Counterterrorism Centre (NCTC) to serve as a multiagency centre analysing and integrating all intelligence pertaining to terrorism, including threats to U.S. interests at home and abroad.[33], the likes of which cannot be observed in India.

The United Kingdom's (UK) surveillance system, on the other hand, is widely deemed as one of the most "legally sophisticated" systems out there. It provides the state with immense power to monitor its citizens, yet unlike NATGRID, it operates under a strict "Double Lock" system of judicial and political oversight. It can be said that this system includes elements of both NATGRID and NCTC; it monitors not only all of its citizens but also makes sure that the system is governed by a statutory framework. The Investigatory Powers Act, 2016 (IPA) (a.k.a Snooper's Act) governs the use of surveillance and investigatory powers by public authorities, including intelligence agencies, law enforcement, and various government departments.[34]

GCHQ (Government Communications Headquarters) is the UK's signals intelligence agency. It intercepts millions of digital signals daily, ranging from satellite communications to undersea fiber-optic cables. It has the power to intercept any devices globally to gather intelligence. This is one of the most invasive powers. It allows the government to remotely hack into computers, smartphones, and even "smart home" devices.[35] This system is unique because of its "Double Lock" safeguard. For the most intrusive warrants (like hacking or bulk interception). Firstly, a Secretary of State (a politician) must personally sign the warrant, and secondly, an independent Judicial Commissioner (a senior judge) must then approve it. If the judge disapproves, the politician cannot move forward,[36] whereas in India, oversight is largely internal to the executive

[33] Department of Justice, *The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, Bureau of Justice Assistance (2004), https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1282 (last visited Apr 20, 2026).
[34] What Is the Investigatory Powers Act? | Cyera Glossary, Cyera.com (2016), https://www.cyera.com/glossary/investigatory-powers-act (last visited Apr 20, 2026).
[35] Peter Sommer, *Why the UK Needs to Rethink the Investigatory Powers Act and Allow Intercept Evidence in Court*, ComputerWeekly.com (2026), https://www.computerweekly.com/feature/Why-the-UK-needs-to-rethinkthe-Investigatory-Powers-Act. (last visited Apr !9, 2026)
[36] Meredith Broadbent, *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers*, www.csis.org (2024), https://www.csis.org/analysis/new-investigatory-powers-act-unitedkingdom-enhances-government-surveillance-powers (last visited Apr 20, 2026).

branch, and neither the legislature nor the judiciary has any say on it.

As a dictatorship regime, it would not be too far-fetched to state that China's surveillance state is the most advanced and comprehensive in human history. This system operates on three surveillance systems. SKYNET is a network of over 180 million (as of 2018) AI-powered cameras across cities. It uses "Real-time Pedestrian Tracking" to not just recognize your face, but also identify your gait (the way you walk), your clothing, and even your "emotional state" through micro-expressions.[37] If the system detects a group of people gathering in an "unusual" pattern, it flags it as a "potential mass incident" and alerts local police. SHARPEYES is a grid system for the rural areas where the cameras are fewer Villagers are given "Smart Terminals" or special TV boxes. They can watch live security feeds of their own neighbourhoods from their living rooms[38]. And lastly, the infamous SOCIAL CREDIT SYSTEM (SCS) it is a digital reputation system that rates the "trustworthiness" of every citizen and business. Using the data from SkyNet, SharpEyes, Bank Records, and Internet history as well. If the system detects that a person commits a crime, or fails to pay a debt, or even if they play too many video games, they are placed on a Blacklist.[39] This system closely resembles the Gandiva AI, an advanced Artificial Intelligence (AI) and analytics layer deployed on top of the NATGRID. It creates a single, unified 360-degree profile of an individual, using the data from the above-mentioned 21 databases (including NPR) ensuring that a suspect cannot hide behind a slight misspelling or a different ID card, the person who is being inspected by the said AI will not know if they are being inspected, it is a closed system, unlike the credit system of China. SCS can result in the person being banned from high-speed trains, being blocked from high-end hotels, or their children being denied entry into top schools. China tries to exert control over every possible aspect of the person's presence in their country; the right to life, personal liberty, and privacy is none existent if looked at from the government-to-people point of view. In India, the primary data for investigation is derived from Adhaar and Bank records; China goes way beyond mere investigation. Its primary tool is advanced cameras surveying virtually everything. China is the most invasive, the UK is the most regulated, and India is the most efficient, with less invasion

[37] Skynet | Surveillance Watch, Surveillancewatch.io (2026), https://www.surveillancewatch.io/entities/skynet (last visited Apr 20, 2026).
[38] Dave Gershgorn, *China's "Sharp Eyes" Program Aims to Surveil 100% of Public Space*, Center for Security and Emerging Technology (2021), https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-tosurveil-100-of-public-space/ (last visited Apr 20, 2026).
[39] Drew Donnelly, *China Social Credit System Explained - How It Works [2026]*, Remote People (2026), https://remotepeople.com/china-social-credit-system-explained/ (last visited Apr 20, 2026).

at linking massive population data without requiring the 24/7 video monitoring seen in China.

PART V – RECOMMENDATIONS

1. To meet the proportionality test of the Putt swamy judgment, by creating a formal statutory framework. A dedicated NATGRID Act would, first of all, provide a "procedure established by law" that is clear and accessible, and secondly, prove the legitimacy of the institution instilling confidence in those whose personal data is collected.

2. Establishing a permanent Parliamentary Standing Committee on Intelligence would enable regular review of query logs and compliance, and a mandatory judicial warrant should be required for accessing highly sensitive biometric data, such as personal bank records or the detailed relational household linkages found in the NPR.

3. For national security, the surveillance of the demographic data for 119 crore residents (NPR data must also be revised after the Census, 2027) must be governed by the principles of necessity and proportionality to avoid population-wide profiling of the marginalized.

4. The Gandiva AI is fundamentally an automated bot; it is bound to hallucinate. To mitigate the risks, such as hallucinations or algorithmic bias, the "Gandiva" analytical engine must undergo regular, transparent audits to ensure its "entity resolution" and facial recognition features do not replicate social prejudices, and the algorithm does not churn out wrong data.

5. Finally, the data integrated in NATGRID or solely the National Population Register should be decentralized so that potential cyber-attacks can be avoided, or in the worst-case scenario, if a data breach does take place, it should not compromise all the data. The technological safeguards should be enhanced by adopting advanced cryptographic methods to create immutable records.

6. Additionally, a grievance redressal mechanism must be established to provide citizens with the right to correct inaccurate demographic data and seek a remedy for wrongful surveillance, in strict alignment with the fundamental right to informational self-determination.

PART VI – CONCLUSION

The integration of the National Population Register with NATGRID indicates a transition in

the executive's approach from NATGRID being a targeted counter-terrorism infrastructure to a potential mass surveillance tool. When conceptualised, it was done so to terminate any terrorist activity in the country. National security was the primary concern. Now, it has just become an excuse to keep the system opaque. The framework fails the Puttswamy proportionality test by operating without a dedicated statutory law, lacking a rational nexus, and failing the "least intrusive" standard compared to systems like the US's NCTC. Hence, the state's move is violative of the fundamental right to privacy of those who are subject to it. This integration, combined with the exclusionary risks of the NPR-NRC framework for marginalized groups and the heightened threat of state-sponsored cyber-attacks on databases, speaks of potential ulterior motives against the marginalized communities and overlooks the potential risks, respectively. Without judicial or legislative safeguards, the NPR-NATGRID integration erodes the democratic autonomy of the nation-state in favour of a techno authoritative regime.

BIBLIOGRAPHY

Arxiv.org. "'Nobody Should Control the End User': Exploring Privacy Perspectives of Indian Internet Users in Light of DPDPA," 2016. https://arxiv.org/html/2508.17962v1.

Broadbent, Meredith. "A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers." *www.csis.org*, May 20, 2024.

https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhancesgovernment-surveillance-powers.

Chickowski, Ericka. "Should Trump Tackle Air-Gapped Critical Infrastructure?" Dark Reading, 2017. https://www.darkreading.com/vulnerabilities-threats/should-trump-tackle-airgapped-critical-infrastructure-.

Cyera.com. "What Is the Investigatory Powers Act? | Cyera Glossary," 2016. https://www.cyera.com/glossary/investigatory-powers-act.

D'souza, Shanthie Mariet. "Mumbai Terrorist Attacks of 2008 | Events, Death Toll, & Facts." In *Encyclopædia Britannica*, 2019. https://www.britannica.com/event/Mumbai-terroristattacks-of-2008.

Department of Justice. "The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)." Bureau of Justice Assistance, December 17, 2004. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1282.

Donnelly, Drew. "China Social Credit System Explained - How It Works [2026]." Remote People, February 14, 2026. https://remotepeople.com/china-social-credit-system-explained/.

Drishti IAS. "NATGRID–NPR Integration," 2024. https://www.drishtiias.com/dailyupdates/daily-news-analysis/natgrid-npr-integration.

Drishti IAS. "Pegasus Spyware." Accessed April 20, 2026. https://www.drishtiias.com/dailyupdates/daily-news-analysis/pegasus-spyware-1.

Gershgorn, Dave. "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space." Center for Security and Emerging Technology, March 2, 2021. https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-publicspace/.

Gktoday.in. "NATGRID-NCRB Sign MoU to Link 14,000 Police Stations," July 13, 2020. https://www.gktoday.in/natgrid-ncrb-sign-mou-to-link-14000-police-stations/.

Greenleaf, Graham. "India's National ID System: Danger Grows in a Privacy Vacuum." Berkeley Electronic Press (bepress), July 19, 2011.

https://law.bepress.com/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1315&context=unswwps-flrps11.

Gupta, Apar. "'Natgrid', the Search Engine of Digital Authoritarianism." Internet Freedom Foundation (IFF), January 10, 2026. https://internetfreedom.in/natgrid-the-search-engine-ofdigital-authoritarianism/.

IMI. "State Sponsored Cyber Warfare." Identity Management Institute®, May 9, 2023. https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/.

Indian Constitution, 77(3) § (1950).

Indian constitution, 21 § (1950).

Jayal, Niraja Gopal. "Reinventing the Republic: Faith and Citizenship in India." *Studies in Indian Politics* 10, no. 1 (April 20, 2022): 14–30. https://doi.org/10.1177/23210230221082799.

Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others (Supreme Court of India September 26, 2018).

Kodali, Srinivas. "Digital India on Steroids: How Aadhaar Infra Enables the NPR and the NRC." The Wire, December 24, 2019. https://m.thewire.in/article/tech/aadhaar-infra-npr-nrc. "Ministry of Personnel, Public Grievances and Pensions (Department of Personnel and

Training) Gazette Notification," July 11, 2011. https://documents.doptcirculars.nic.in/D2/D02rti/1_3_2011-IR09062011.pdf.

Mukhopadhyay, Devdutta. "Data Protection and the National Population Register." Internet Freedom Foundation (IFF), February 28, 2020. https://internetfreedom.in/data-protection-andthe-national-population-register/.

Nath, Sujit. "Fitting Mumbai"S Terror Jigsaw." India Today, December 7, 2008. https://www.indiatoday.in/latest-headlines/story/fitting-mumbai-s-terror-jigsaw-34732-200812-07.

People's Archive of Rural India. "The Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003," 2019. https://ruralindiaonline.org/hi/library/resource/the-citizenship-rules-2003/?hl=en-IN.

Pib.gov.in. "Assistance to States to Tackle Cyber Incidents," 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504®=1&lang=1.

Ramanathan, Usha. "Implications of Registering, Tracking, Profiling," April 5, 2010. https://www.ielrc.org/Content/n1001.pdf.

SabrangIndia. "NPR 2020: What Does It Want to Know? | SabrangIndia," January 17, 2020. https://sabrangindia.in/npr-2020-what-does-it-want-know/.

Sabrangindia. "Multipurpose National Identity Card, Recall from 2003," January 25, 2020. https://sabrangindia.in/multipurpose-national-identity-card-recall-2003/.

Satp.org. "Home Ministers Speech at the 22nd Intelligence Bureau Centenary Endowment

Lecture: South Asia Terrorism Portal," 2026. https://www.satp.org/satporgtp/countries/india/document/papers/09dec25pib.htm.

Service, Express News. "MHA Advises States to Use NATGRID Database to Control Crimes, Criminals." The New Indian Express, July 6, 2025. https://www.newindianexpress.com/nation/2025/Jul/06/mha-advises-states-to-use-natgriddatabase-to-control-crimes-criminals.

Singh, Vijaita. "National Intelligence Grid Slowly Gathers Pace, Receives 45k Requests a Month." The Hindu, December 7, 2025. https://www.thehindu.com/news/national/nationalintelligence-grid-slowly-gathers-pace-receives-45k-requests-a-month/article70369184.ece.

Sommer, Peter. "Why the UK Needs to Rethink the Investigatory Powers Act and Allow Intercept Evidence in Court. 2026. https://www.computerweekly.com/feature/Why-the-UK-needs-to-rethink-the-InvestigatoryPowers-Act.

Supreme Court Observer. "Fundamental Right to Privacy," July 16, 2025. https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacycase-background/.

The National Counterterrorism Center. "NCTC." Dni.gov, 2018. https://www.dni.gov/index.php/nctc-home.

The Wire Staff. "Full Text: What the High Level Inquiry Committee on the 26/11 Attacks Had to Say." The Wire, September 26, 2019. https://thewire.in/security/26-11-mumbai-terrorattack-inquiry-committee.

Vajiram Editor. "Vajiram Editor." Vajiram and Ravi, January 7, 2026. https://vajiramandravi.com/upsc-exam/national-population-register-npr/?hl=en-IN.

Vasureddy. "NRC the Need of the Day.. Implement or Perish." MyVoice, February 13, 2020. https://myvoice.opindia.com/2020/02/nrc-the-need-of-the-day-implement-or-perish/?hl=enIN.