MULTIDIMENSIONAL SURVEILLANCE AND PUBLIC WI-FI IN INDIAN RAILWAYS: DATA PROTECTION, CYBER-SECURITY VULNERABILITIES, AND STATE LIABILITY UNDER ARTICLE 21

Roshan Kumar Giri, Campus Law Centre, Faculty of Law, University of Delhi.

ABSTRACT

Indian Railways operates one of the world' s largest public Wi-Fi deployments, covering 6117[1] railway stations under the Rail-wire initiative facilitated through Rail-Tel Corporation of India. While this infrastructure has rapidly expanded digital access for millions of computers, it simultaneously creates a formidable architecture of multidimensional surveillance, metadata collection, behavioural tracking, facial recognition integration and real-time data aggregation that intersects extensively with fundamental rights jurisprudence. This paper critically analysis the intersection of public Wi-Fi surveillance in Indian railways with the constitutional guarantee of the right to privacy under article 21[2] of the constitution of India, as established and crystallized by the nine judges bench of the Supreme Court in Justice K.S Puttaswamy (Retd.) v. Union of India (2017). The paper analyses the Cybersecurity vulnerabilities inherent in mass public Wi-Fi infrastructure, the adequacy and lacunae of the existing data protection framework in India, including the Digital Personal Data Protection Act, 2023 (DPDPA),[3] and the outline of state liability for data breaches and surveillance overreach. It further engages with comparative jurisprudence from the European Union, the United States and Canada to situate India's evolving framework within the global discourse on privacy, surveillance, and state accountability The paper argues that the present surveillance architecture of Indian Railways' public Wi-Fi lacks adequate constitutional legitimacy under the tripartite Puttaswamy test of legality, necessity, and proportionality, and proposes a rights-compliant framework for reform.

Keywords- Article 21- Right to Privacy, Cybersecurity, Mass Surveillance, State Liability, Digital Rights

[1] https://infra.economictimes.indiatimes.com/news/railways/indian-railways-rolls-out-free-wi-fi-at-over-6100-stations-expands-cctv-coverage/126037488
[2]https://indiankanoon.org/doc/1199182/
[3]https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

I. INTRODUCTION

The Indian railway network transcends its function as mere transportation infrastructure, serving as the nation's circulatory system by transporting approximately 23 million [4]passengers daily across 68,000 kilometers of track. Since 2016, this physical network has been integrated with an expansive digital layer: the Rail-wire public Wi-Fi service, implemented by Rail-Tel Corporation of India Limited, a public sector undertaking under the Ministry of Railways. By 2024, Rail-wire operated across more than 6,117 railway stations, establishing it as one of the most significant public Wi-Fi deployments globally.While this initiative represents a substantial expansion of digital access—consistent with India's "Digital India" vision and constitutional commitments to equality in the information age—it simultaneously facilitates a pervasive surveillance architecture. Users connecting to the Rail-wire network are required to authenticate via mobile number, establishing a definitive link between government-verified identifiers and individual digital behavior. The infrastructure systematically collects, aggregates, and potentially analyzes browsing metadata, geolocation, device identifiers, and temporal usage patterns. When considered alongside the deployment of Integrated Security Systems featuring facial recognition technology at major railway stations, Indian Railways emerges as a locus of multifaceted state surveillance. This paper operates on the premise that the right to privacy, as constitutionally affirmed in Justice K.S. Puttaswamy v. Union of India[5],is not a privilege reserved for the affluent or the technologically proficient. Rather, it is a fundamental right that must be upheld in spaces where the state centralizes populations and provides services, including railway stations and their associated digital infrastructure. Accordingly, this paper addresses three research questions:

1-Does the surveillance architecture inherent in Indian Railways' public Wi-Fi satisfy the constitutional tripartite test established in Puttaswamy?

2-What cybersecurity vulnerabilities does the Rail-wire infrastructure introduce, and what is the extent of state liability for resulting harm?

3-Is the Digital Personal Data Protection Act, 2023, sufficient to mitigate the data protection

[4]https://en.wikipedia.org/wiki/Indian_Railways
https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1595411&reg=48&lang=2
https://www.pib.gov.in/newsite/printrelease.aspx?relid=149088&reg=48&lang=2
https://www.twingate.com/blog/tips/indian-railways-data-breach
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 [Puttaswamy I].

concerns emerging from state-operated public Wi-Fi surveillance,

The paper is organized as follows: Part II provides a technical and institutional analysis of the Rail-wire Wi-Fi infrastructure and its surveillance dimensions; Part III examines the constitutional framework of privacy under Article 21 and the Puttaswamy doctrine; Part IV applies the tripartite test to the Rail-wire surveillance ecosystem; Part V analyzes cybersecurity vulnerabilities and state liability; Part VI evaluates the adequacy of the DPDPA 2023 framework; Part VII offers comparative perspectives; and Part VIII proposes a rights-compliant reform framework, followed by the conclusion in Part IX.

II. THE RAILWIRE INFRASTRUCTURE: ARCHITECTURE OF CONNECTIVITY AND SURVEILLANCE

A. Institutional Background: Rail-Tel and the Rail-wire Initiative-

Rail-tel Corporation of India Limited is a Navratna (2024)[6]Public Sector Undertaking established under the Companies Act, wholly owned by the Government of India through the Ministry of Railways. Rail-tel owns and operates one of India's largest neutral telecom infrastructure providers, with an extensive optic fibre network along railway tracks that spans over 60,000 route kilometers. The Rail-wire initiative was launched in February 2016 at Patna [7] Junction, with Google as the initial technology partner under its 'Google Station' programme a collaboration that itself raises questions about public-private data sharing arrangements and the commodification of citizen data.

B. The Authentication Mechanism as Primary Surveillance Vector-

The compulsory authentication process for Rail-wire Wi-Fi compose up the first and most foundational layer of surveillance. Users are required to authenticate their identity through a mobile phone number, to which a One-Time Password (OTP) is sent via SMS. This authentication requirement has many significant implications:

First, it creates a compulsory linkage between a government-traceable identifier the mobile number, which under the Telecom Regulatory Authority of India (TRAI) regulations and the

[6] https://indianexpress.com/article/explained/explained-economics/navratna-status-irctc-irfc-9868272/
[7] https://indianexpress.com/article/technology/tech-news-technology/google-wifi-free-internet-suresh-prabhu-indian-railways-2811832/

Prevention of Money Laundering Act, 2002 (PMLA) must be linked to an Aadhaar number or other verified identity document and the user's digital activity on the network.

Second, the authentication process generates a purposeful record in RailTel's servers that links a specific individual to a specific device (through the device's Media Access Control or MAC address[8]), at a specific location (the railway station), at a specific time. When aggregated across multiple sessions and multiple stations, this data creates what scholars of surveillance studies would recognise as a comprehensive movement profile — far more revealing than the simple fact of railway travel, since it captures not merely that a person was at Station A on Date X, but that they were actively using the internet and the digital content they accessed.

Third, OTP - based authentication creates retrievable metadata that may be retained and shared with authorities, thereby expanding the surveillance architecture .

C. **Data Collection Beyond Authentication:**

The Surveillance Ecosystem Rail-wire operates within the broader Integrated Security system developed by the Ministry of railways, RPF, and state police that incorporate Closed-Circuit Television (CCTV) cameras with facial recognition capabilities at major stations.The convergence of biometric surveillance through facial recognition with behavioral surveillance through Wi-Fi usage data creates what the philosopher Shoshana Zuboff[9] has termed 'surveillance capitalism' in the private sector context but which, in the public sector context of Indian Railways, constitutes a surveillance state. A user identified through facial recognition at a railway station, whose mobile number is also authenticated on the Rail-wire network, becomes the subject of a comprehensive file their physical presence, their movement through the station, and their digital behaviour are all captured, correlated, and retained.The legal basis for this integrated surveillance architecture is entirely unclear. No comprehensive statutory framework governing the deployment and use of facial recognition technology exists in India. The Puttaswamy judgment expressly identifies the absence of a surveillance law as a constitutional lacuna that must be filled. The deployment of FRT by the RPF and Rail Tel, without clear statutory authorization, explicit consent, or judicial oversight, raises acute Article 21 concerns.

[8] https://study-ccna.com/mac-ip-addresses/
[9] https://en.wikipedia.org/wiki/Surveillance_capitalism

III. THE CONSTITUTIONAL FRAMEWORK: PRIVACY AS A FUNDAMENTAL RIGHT

A. The Puttaswamy Revolution: From Minority View to Constitutional Cornerstone

The ambit of privacy jurisprudence in India before 2017 was marked by ambiguity and constitutional subordination. In M.P. Sharma v. Satish Chandra[10] (1954), an eight-judge bench of the Supreme Court had held, in the context of search and seizure, that no fundamental right to privacy existed in the Indian Constitution. This position was reiterated, though with somewhat less clarity, in Kharak Singh v. State of U.P[11]. (1963), where a six-judge bench struck down domiciliary visits by police as violating Article 21 but was divided on whether privacy per se was constitutionally protected.

The doctrinal uncertainty was definitively resolved by the nine-judge constitutional bench in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The case arose in the context of challenges to the Aadhaar biometric identification programme but its significance go beyond that context. The bench unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution, particularly under Article 21 which guarantees the right to life and personal liberty.

The six separate but concurring opinions produced by the bench persuasive different but complementary understandings of privacy. Justice D.Y. Chandrachud's lead opinion, which has attracted the most scholarly attention, situates privacy as foundational to autonomy, dignity, and liberty as a 'meta-right' that enables the exercise of all other fundamental rights. Justice S.A. Bobde emphasises privacy as a natural right preceding constitutional recognition. Justice Sanjay Kishan Kaul articulates a concept of 'informational privacy' that has particular relevance to digital surveillance.

B. The Tripartite Test: Legality, Necessity, and Proportionality

The Puttaswamy judgment does not recognise privacy as an absolute right but subjects any state-imposed limitation to a tripartite test, the satisfaction of which is constitutionally mandatory:

[10]M.P. Sharma v. Satish Chandra AIR 1954 SC 300.
[11] Kharak Singh v. State of U.P. AIR 1963 SC 1295.

The first prong requires that any interference with the right to privacy must have the sanction of law ('the existence of a law'). This is not merely the requirement that some executive action has been taken, but that a validly enacted law of Parliament or a state legislature authorises the specific interference.

The second prong requires that the law sanctioning the interference must serve a legitimate state aim. The Court indicates that 'national security, prevention of crime, protection of health and morals, and protection of rights and freedoms of others' may constitute legitimate aims, but these must not be merely asserted — they must be demonstrably connected to the interference in question.

The third and most demanding prong requires that the interference be necessary and proportionate to the legitimate aim sought to be achieved that 'the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled.' This requires a genuine analysis of whether less intrusive means could achieve the same legitimate aim, and whether the privacy cost of the measure is outweighed by the benefit conferred.

The Puttaswamy framework was further developed in subsequent decisions. In Anuradha Bhasin v. Union of India[12] (2020), the Supreme Court applied proportionality analysis to the suspension of internet services in Jammu & Kashmir, articulating a four-part proportionality test: legitimate aim, suitability, necessity (least restrictive measure), and proportionality strict sense . In Maneka Gandhi v. Union of India[13] (1978), the foundational case establishing the 'procedure established by law' standard for Article 21, the Court had held that any procedure limiting Article 21 rights must be 'right, just and fair' — not arbitrary, fanciful, or oppressive. The Puttaswamy judgment builds upon and enriches this foundation.

C. Informational Privacy and the Reasonable Expectation Doctrine

Justice Kaul's opinion in Puttaswamy is of particular relevance to the present analysis for its clear recognition of informational privacy as a distinct dimension of the constitutional right. The opinion holds that 'the right to privacy includes the right to control the distribution of personal information' and that an individual retains a constitutionally protected interest in

[12] Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[13] Maneka Gandhi v. Union of India AIR 1978 SC 597.

information that reveals patterns of behaviour, associations, and preferences even where individual data points may seem safe.

The concept of a 'reasonable expectation of privacy' (REP), derived from American Fourth Amendment jurisprudence following Katz v. United States (1967)[14], has been progressively incorporated into Indian constitutional discourse. Applied to the railway station context, the question is whether a citizen who uses a public Wi-Fi network at a railway station can be said to have voluntarily surrendered all reasonable expectations of privacy in their digital activity simply by virtue of using the network.

The answer under a rights-protective interpretation of Puttaswamy must be in the negative. The 'voluntary' nature of consent to the terms of a mandatory authentication process where the alternative is exclusion from digital access in an increasingly digital society is constitutionally suspect. The Supreme Court in S. Ramesh Naidu v. Union of India [15]has recognised that consent obtained under conditions of unequal bargaining power or structural compulsion cannot constitute genuine waiver of fundamental rights. A person at a railway station who needs to access digital services, particularly in the era of digital ticketing, digital payments, and digital communications, cannot meaningfully be said to 'choose' to submit to surveillance as a condition of network access.

D. The Third Party Doctrine and its Constitutional Incompatibility

The 'third party doctrine,' developed by the U.S. Supreme Court in Smith v. Maryland[16] (1979) holds that individuals have no reasonable expectation of privacy in information voluntarily shared with third parties. This doctrine has been criticised as doctrinally inadequate in the digital age and was significantly curtailed by the U.S. Supreme Court in Carpenter v. United States (2018)[17] in the context of Cell Site Location Information.

The third party doctrine has no constitutional foothold in India. The Puttaswamy judgment's recognition of informational privacy as a fundamental right is inconsistent with any proposition that citizens forfeit constitutional protection in their data merely by sharing it with a service provider. The right to control the dissemination of personal information, as articulated by

[14]Katz v. United States 389 U.S. 347 (1967).
[15]S. Ramesh Naidu v. Union of India(Feb.2026)
[16] Smith v. Maryland 442 U.S. 735 (1979).
[17] Carpenter v. United States 585 U.S. 296 (2018)

Justice Kaul, necessarily implies that the state cannot circumvent constitutional protections by routing its surveillance through the instrumentality of a service that citizens must use.

IV. APPLYING THE PUTTASWAMY TEST TO RAILWIRE SURVEILLANCE

A. The Legality Prong: Absence of Adequate Statutory Authorisation

The very important question in any Puttaswamy analysis is whether the privacy invasive practice is sanctioned by law. The surveillance architecture of Indian Railways encompassing mandatory OTP authentication, metadata retention, MAC[18] address collection, and integration with facial recognition systems lacks a comprehensive or specific statutory foundation.

The Indian Telegraph Act, 1885, as amended, governs telecom infrastructure but was not designed to regulate the data practices of a public Wi-Fi network operator. The Information Technology Act, 2000 (IT Act)[19] and its associated rules provide some framework but do not specifically authorise the surveillance practices in question. Section 69 of the IT Act authorises interception, monitoring, and decryption of information in the interests of national security and public order, but the sweeping and indiscriminate collection of metadata from millions of railway Wi-Fi users is not the targeted interception contemplated by Section 69.

V. CYBERSECURITY VULNERABILITIES AND STATE LIABILITY

A. Technical Vulnerabilities in Public Wi-Fi Infrastructure

Public Wi-Fi networks, by their nature and design, present a substantially different security profile compared to private or enterprise networks. The RailWire infrastructure, operating at scale across thousands of geographically dispersed stations with varying levels of technical maintenance, is particularly susceptible to a range of well-documented cybersecurity vulnerabilities.

1. Man-in-the-Middle Attacks

Man-in-the-Middle (MitM) attacks represent perhaps the most significant threat to users of public Wi-Fi networks. In a MitM attack, a malicious actor positions themselves between a

[18] https://study-ccna.com/mac-ip-addresses/
[19] Information Technology Act, 2000 (IT Act-2000),section 69,

user and the network, intercepting and potentially modifying communications. In the railway station environment, the deployment of 'evil twin' access points rogue Wi-Fi hot spots with the same Service Set Identifier (SSID) as legitimate Rail-wire networks enables attackers to intercept the communications of unsuspecting users who connect to the fraudulent network. Given the large footfall at railway stations and the limited ability of users to verify the authenticity of the network they connect to, the risk of MitM attacks on the RailWire network is substantial and has been documented in cybersecurity research contexts.

2. Authentication System Vulnerabilities

The OTP-based authentication mechanism, while providing a layer of user identification, also creates a dedicated attack surface. SMS-based OTP delivery is vulnerable to SIM swap attacks, in which a malicious actor fraudulently obtains a duplicate SIM card for a victim's mobile number, thereby gaining the ability to receive OTPs and authenticate as the victim on the RailWire network. SIM swap attacks have been used to compromise banking authentication systems in India and represent a realistic threat in the railway Wi-Fi context. Furthermore, the centralised authentication server that processes OTP requests constitutes a high-value target: a successful attack on this server could expose the authentication records and potentially the browsing histories of millions of users.

3. Data Retention and Storage Security

The cybersecurity risk is not confined to the transmission phase. The substantial repositories of user data collected and retained by RailTel — including authentication records, MAC addresses, session logs, and potentially browsing metadata — represent concentrated targets for malicious actors. India has experienced significant data breaches involving government databases, including the reported leakage of Aadhaar data and the breach of AIIMS Delhi's digital infrastructure in 2022.[20] A breach of the RailWire database could expose the travel patterns, device information, and digital behaviour of tens of millions of citizens, with profound

[20] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2227410&reg=3&lang=1, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.aiims.edu/images/pdf/notice/AIIMS%2520-%2520THE%2520FIRST%2520DIGITAL%2520REVOLUTION%2520IN%2520HEALTH%2520CARE%2520(1).pdf&ved=2ahUKEwjXm6yo75-VAxUtUGwGHWzhL9IQFnoECBkQAQ&usg=AOvVaw0gpusoqoOTVRC5UarAaZ2U

implications for individual privacy and potential for misuse in targeted harassment, corporate espionage, or political surveillance.

4. Inadequate Encryption Standards

Security audits and journalistic investigations have raised concerns about the encryption standards employed by RailWire networks at various stations, particularly at smaller stations where technical infrastructure may be less current. Networks operating on WPA2 protocols, while more secure than their predecessors, are vulnerable to the KRACK (Key Reinstallation Attack) [21]vulnerability disclosed in 2017 and the PMKID attack [22]method. The absence of mandated security standards, published security audits, and independent vulnerability testing for the RailWire infrastructure represents a significant regulatory gap.

B. State Liability for Data Breaches and Surveillance Harms

The state's liability for harms arising from cybersecurity failures and surveillance overreach in the RailWire context requires analysis across three dimensions: constitutional tort liability, statutory liability, and liability under emerging data protection law.

1. Constitutional Tort: The Nilabati Behera Doctrine

The Supreme Court in Nilabati Behera v. State of Orissa[23] (1993) established that the violation of a fundamental right by the state gives rise to a public law remedy under Article 32 and Article 226 of the Constitution, including the award of compensation. The Court held that the principle of sovereign immunity does not shield the state from liability for fundamental rights violations, departing from the private law principle that precludes tort claims against the Crown in certain contexts.

Applied to the RailWire context, a citizen who suffers demonstrable harm as a result of a data breach from the RailWire database — such as the use of their data to facilitate stalking, identity theft, or targeted harassment — would have a constitutional tort claim against RailTel and, by extension, the Union of India. The more complex question, and one that remains substantially

[21]https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.fortinet.com/resources/cyberglossary/krack-attack&ved=2ahUKEwjloZGh8J-VAxUqV3ADHRDKNawQFnoECBsQAQ&usg=AOvVaw2HfnGVW8o12SvkCysZvHyq
[22] https://www.nccgroup.com/research/pmkid-attacks-debunking-the-80211r-myth/
[23] Nilabati Behera v. State of Orissa (1993) 2 SCC 746.

unsettled in Indian jurisprudence, is whether the mere collection and retention of data without consent and without adequate statutory authority constitutes a continuous violation of Article 21 for which compensation may be sought even in the absence of specific downstream harm.

2. Statutory Liability under the IT Act

Section 43A of the Information Technology Act, 2000[24] (as inserted by the IT (Amendment) Act, 2008) provides that a body corporate that possesses, deals, or handles any sensitive personal data and is negligent in implementing and maintaining reasonable security practices, thereby causing wrongful loss or wrongful gain to any person, shall be liable to pay damages. Section 72A provides for criminal liability for disclosure of information in breach of lawful contract.

RailTel, as a body corporate under the Companies Act that handles sensitive personal data including mobile numbers, usage patterns, and potentially financial information of railway passengers, is subject to Section 43A. The threshold question is whether the security practices implemented by RailTel constitute 'reasonable security practices' [25]within the meaning of the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Given the documented vulnerabilities in public Wi-Fi infrastructure and the absence of published security audits for the RailWire system, there are substantial grounds to conclude that the current practices may not satisfy this standard.

3. Liability under the DPDPA 2023

The Digital Personal Data Protection Act, 2023[26] establishes a framework for the protection of digital personal data and creates obligations for 'Data Fiduciaries' entities that determine the purpose and means of processing personal data. RailTel is plainly a Data Fiduciary under the DPDPA 2023 with respect to the data collected from RailWire users. The Act establishes obligations relating to purpose limitation, data minimisation, storage limitation, and security safeguards.

[24] Information Technology Act, 2000 Amendment Act 2008,section 43A.
[25] (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[26] Digital Personal Data Protection Act, 2023

VI. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: ADEQUACY AND LACUNAE

A. Overview of the DPDPA Framework

The Digital Personal Data Protection Act, 2023 received the assent of the President of India on 11 August 2023, becoming the first comprehensive data protection legislation in India after nearly a decade of effort following the Justice B.N. Srikrishna Committee's recommendations in 2018. The Act establishes a framework based on the core principles of lawful and fair processing, purpose limitation, data minimisation, accuracy, storage limitation, and reasonable security safeguards, broadly aligned with international data protection standards.

The DPDP Act, 2023 established the Data protection board of India, requires Data Fiduciaries to provide notice, obtain consent where necessary, and ensure the accuracy and security of personal data, while imposing penalties of up to 250 crore for specified violations.

B. The Consent Framework and its Application to RailWire

The DPDPA 2023 requires that processing of personal data be based on consent of the Data Principal or on one of the specified 'legitimate uses' listed in Section 7[27]. Consent, under the Act, must be free, specific, informed, unconditional, and unambiguous, and must indicate agreement to the processing of personal data for a specified purpose. The clickwrap consent mechanism employed by RailWire where users tap 'Accept' on a terms of service screen as a condition of network access is unlikely to satisfy this standard.

The problem is not merely one of form. The substantive consent to the collection of browsing metadata, device identifiers, and usage patterns is buried within lengthy terms of service that the majority of users do not read, cannot meaningfully understand, and cannot meaningfully negotiate. Consent obtained in this manner, from individuals who have no practical alternative to acceptance if they wish to use digital services at the railway station, is structurally coerced and therefore legally ineffective as a justification for data processing under a rights-respecting interpretation of the DPDPA.

[27] The DPDP Act, 2023, Section-7, section-17,17(2)

C. The State Exemption Problem

Section 17 of the DPDPA 2023 grants the Central Government the power to exempt the application of the Act's provisions to any Data Fiduciary or class of Data Fiduciaries by notification. Section 17(2) specifically provides that the Central Government may, by notification in the Official Gazette, exempt from the provisions of the Act the processing of personal data by the Central Government, a state government, or any instrumentality of either, for the purposes of security of the State, public order, sovereignty and integrity of India, or friendly relations with foreign states.

This exemption, if applied to RailTel and its railway Wi-Fi operations, would effectively remove the most significant public Wi-Fi surveillance operation in the country from the ambit of data protection law. The breadth of the exemption which requires only a governmental notification rather than judicial authorisation or legislative specification is constitutionally problematic. In S.G. Vombatkere v. Union of India[28] (2022), the Supreme Court struck down Section 66A of the IT Act as unconstitutionally vague. A similarly vague, executive-controlled exemption from data protection obligations fails the 'existence of a law' prong of the Puttaswamy test because a law that grants unlimited executive discretion to suspend constitutional protections is not a 'law' in the constitutional sense but an abdication of parliamentary responsibility.

D. Absence of Provisions for Algorithmic Accountability

The DPDPA 2023 is entirely silent on the use of automated decision-making, profiling, and algorithmic processing of personal data a significant gap given the contemporary reality of AI-driven surveillance systems. The RailWire surveillance ecosystem, if it incorporates machine learning algorithms for anomaly detection or behavioural profiling (as security rationales may suggest), constitutes automated processing that affects individuals' interests without any transparency, explainability, or right to human review.

E. Data Localisation and Cross-Border Transfer Concerns

The RailWire infrastructure was initially deployed with the involvement of Google, raising questions about the extent to which user data was transferred to Google's servers outside India.

[28] S.G. Vombatkere v. Union of India (2022) 7 SCC 433

Following Google's exit from the programme, the data architecture may have changed, but the question of cross-border data transfer remains relevant in the context of RailTel's cloud service providers and technology partners.

The DPDPA 2023 adopts a 'whitelist' approach to cross-border data transfers, permitting transfers to countries notified by the Central Government. However, the provisions are drafted with significant executive flexibility and limited parliamentary oversight, raising concerns about the adequacy of protection for data transferred to third countries and the transparency of transfer decisions.

VII. COMPARATIVE PERSPECTIVES:

GLOBAL APPROACHES TO PUBLIC WI-FI SURVEILLANCE

Canada: The Privacy Act and the Charter Framework Canada regulated government surveillance through the privacy act,1985 section 8 of the candian charter of Rights and freedoms, In 2014 the office of the Privacy Commissioner of Canada found that the collection of Wi- Fi probe data from transportation users constituted personal information collection and therefore required legal authority, proportionality and transparency.The findings affirm that passive collection of data from public transportation users must satisfy privacy and constitutional safeguards.

Lessons for India: A Synthesis

The comparative analysis reveals several converging principles that should inform India's approach to public Wi-Fi surveillance:

First, the consensus in mature constitutional democracies is that the state cannot claim immunity from data protection obligations merely because it is the state. The EU, the US post-Carpenter, and Canada all recognise that state surveillance of citizens must satisfy constitutional requirements of legality, necessity, and proportionality, and that the structural power asymmetry between the state and the individual demands heightened rather than reduced scrutiny.

Second, mass retention of communications metadata without individualised suspicion, independent oversight, or meaningful storage limitation is constitutionally disproportionate.

The CJEU's Digital Rights Ireland decision and the U.S. Supreme Court's Carpenter decision converge on this principle, as does the Puttaswamy judgment's own proportionality framework.

Third, effective data protection requires institutional infrastructure: independent oversight bodies with genuine investigative and enforcement powers, transparent reporting requirements, and effective remedies for individuals. India's Data Protection Board, as constituted under the DPDPA 2023 with significant executive influence over appointments and procedure, falls short of the institutional independence required to perform this function effectively.

VIII. TOWARDS A RIGHTS-COMPLIANT FRAMEWORK: PROPOSALS FOR REFORM

A. Legislative Reform: A Surveillance Law for India

The most foundational reform required is the enactment of a comprehensive surveillance law in India legislation that explicitly authorises, defines the limits of, and provides oversight mechanisms for state surveillance activities, including digital surveillance through public infrastructure. The absence of such legislation is both a constitutional failure (since it means that existing surveillance practices lack the legal foundation required by Puttaswamy) and a democratic failure (since it means that the legislature has not made the fundamental policy choices about the balance between security and privacy that a democratic society requires).

The proposed surveillance law should, at minimum: enumerate the specific categories of surveillance that may be employed by state agencies; establish strict necessity requirements and require that surveillance be targeted rather than mass; provide for prior independent judicial authorisation for surveillance activities above specified levels of intrusiveness; establish data retention limits tied to specific and justified purposes; require regular reporting to Parliament on surveillance activities; and provide effective judicial and quasi-judicial remedies for individuals.

B. Reform of RailWire's Data Architecture

Independently of broader legislative reform, RailTel should be required to reform the data architecture of the RailWire network in accordance with privacy-by-design principles.Authentication should be decoupled from tracking: network access authentication should use ephemeral identifiers that do not link to permanent mobile numbers in retained

records. Technical solutions such as zero-knowledge authentication protocols, while more complex to implement, enable network security without creating permanent identity-behaviour linkages.Browsing metadata should not be collected or retained: session-level data sufficient for network management purposes (connection duration, data volume, basic technical parameters) should be the maximum retained. Content-level or domain-level metadata about individual browsing behaviour should not be retained absent a specific, individualised legal authorisation.

Data retention limits should be clearly specified and publicly disclosed: where some authentication-linked data must be retained for legitimate purposes, clear time-bound retention limits should be established and enforced, with automatic deletion protocols.Security standards should be mandated and independently audited: minimum encryption standards, penetration testing requirements, and independent security audits should be required for all nodes of the RailWire network, with results published in accessible form.

C. Regulation of Facial Recognition Technology in Railways

The deployment of facial recognition technology at railway stations requires, as a matter of constitutional necessity, specific statutory authorisation. In the absence of comprehensive FRT legislation — which India has thus far failed to enact despite multiple calls from civil society, parliamentary committees, and legal scholars — the deployment of FRT by the Railway Protection Force and other railway authorities is constitutionally impermissible.

A statutory framework for FRT in public spaces should provide, at minimum: a complete prohibition on real-time mass facial recognition in public spaces (as distinct from targeted FRT based on individualised warrants); requirements for algorithmic transparency including accuracy rates disaggregated by demographic characteristics; independent testing and certification of FRT systems; and prohibition on the sharing of FRT-derived data with private entities or foreign governments.

D. Amendment of the DPDPA 2023

The Digital Personal Data Protection Act, 2023 requires significant amendment to address the specific concerns identified in this paper:

• The state exemption under Section 17(2) should be significantly narrowed, eliminating the broad executive discretion to exempt government data fiduciaries from the Act's requirements,

and replacing it with specific, Parliament-specified exemptions subject to sunset clauses and independent review.

• Provisions for algorithmic accountability should be inserted, including a right to explanation for automated decisions and a right to human review of algorithmically-generated security assessments.

• The Data Protection Board should be reconstituted as a genuinely independent body with membership drawn from the judiciary, civil society, and technical experts, with security of tenure and freedom from executive direction in individual cases.

• Specific provisions addressing the data protection obligations of government-operated public Wi-Fi networks should be included, providing clarity on the legal basis for data processing and the minimum standards required.

E. Judicial Intervention: The Role of PIL Jurisdiction

In the absence of legislative action, the judicial system particularly through the Public Interest Litigation (PIL) jurisdiction under Articles 32 and 226 of the Constitution — has a significant role to play in enforcing constitutional standards against the surveillance architecture of Indian Railways. The Puttaswamy judgment itself arose from a PIL challenging Aadhaar, illustrating the transformative potential of judicial review in the digital rights context.

Courts adjudicating PILs challenging RailWire surveillance should be guided by the principle that the burden of demonstrating constitutional justification rests with the state. It is insufficient for the Union of India or RailTel to assert security justifications, they must demonstrate, with evidence, that the specific surveillance practices employed are proportionate to demonstrated security benefits that could not be achieved through less intrusive means. Courts should appoint independent technical experts to assess the privacy and security dimensions of the RailWire architecture, rather than deferring entirely to government submissions.

IX. CONCLUSION

Public Wi-Fi in India railway stations has evlved into an underexamine surveillance mechanism that collect citizen's behavioural data without adequate legal safegaurds, oversight, or compliance with the privacy standards established in puttaswamy. When integrated with the deployment of facial recognition technology and the aggregation of location, device, and

behavioural data, the railway station has become a paradigmatic site of the surveillance state.

This paper has argued, through a rigorous application of the Puttaswamy tripartite test of legality, necessity, and proportionality, that the current RailWire surveillance architecture fails constitutional scrutiny at each stage. The absence of a comprehensive surveillance law means that the legality requirement is not satisfied. The vague and shifting rationales advanced for mass data collection mean that a clear legitimate aim cannot be identified. And the indiscriminate, mass character of the surveillance, without individualised justification or independent oversight, fails the necessity and proportionality requirements.

The cybersecurity dimension compounds the constitutional analysis. The concentrated repositories of personal data created by mass public Wi-Fi surveillance create high-value targets for malicious actors, and the state's liability for breaches — under both constitutional tort principles and emerging statutory frameworks — is substantial. The Digital Personal Data Protection Act, 2023, while representing India's first serious attempt at comprehensive data protection legislation, fails to adequately address the specific challenges of government-operated surveillance infrastructure through its broad state exemptions, absence of algorithmic accountability provisions, and structurally constrained oversight body.

The reforms proposed in this paper a comprehensive surveillance law, reform of RailWire's data architecture on privacy-by-design principles, specific regulation of facial recognition technology, amendment of the DPDPA 2023, and active use of judicial PIL jurisdiction represent the minimum required to bring India's railway surveillance practices into constitutional compliance. The promise of Puttaswamy that privacy is a foundational constitutional value, not an elite prerogative can only be redeemed if it is applied with full force to the spaces where the state and its citizens most intimately interact: the platforms, concourses, and waiting rooms of the Indian railway network.

Privacy is not the enemy of security. It is the condition under which genuine security security from an overreaching state as much as security from external threats — becomes possible. A surveillance architecture that treats every railway passenger as a potential suspect, collecting and aggregating their most intimate digital behaviour without consent or oversight, does not make India more secure. It makes India less free.

BIBLIOGRAPHY

Table of Cases

India

Anuradha Bhasin v. Union of India (2020) 3 SCC 637

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1

Justice K.S. Puttaswamy (Retd.) v. Union of India (2019) 1 SCC 1 [Puttaswamy II — Aadhaar]

Kharak Singh v. State of U.P. AIR 1963 SC 1295

Maneka Gandhi v. Union of India AIR 1978 SC 597

M.P. Sharma v. Satish Chandra AIR 1954 SC 300

Nilabati Behera v. State of Orissa (1993) 2 SCC 746

S.G. Vombatkere v. Union of India (2022) 7 SCC 433

Cellular Operators Association of India v. TRAI (2016) 7 SCC 703

United States

Carpenter v. United States 585 U.S. 296 (2018)

Katz v. United States 389 U.S. 347 (1967)

Smith v. Maryland 442 U.S. 735 (1979)

Legislation and Instruments

Constitution of India, 1950

Digital Personal Data Protection Act, 2023

Information Technology Act, 2000

Information Technology (Amendment) Act, 2008

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Railway Protection Force Act, 1957

Railways Act, 1989

Indian Telegraph Act, 1885

Prevention of Money Laundering Act, 2002

General Data Protection Regulation (EU) 2016/679

Privacy Act 1985 (Canada)

Secondary Literature

Bhatia G, 'The Transformative Constitution: A Radical Biography in Nine Acts' (HarperCollins 2019)

Chandrachud DY, 'Privacy, Surveillance and the (Un)constitutionality of the Post-Puttaswamy State' (2019) 31 National Law School of India Review 1

Clarke R, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Xamax Consultancy 2016) <http://www.rogerclarke.com/DV/Intro.html>

Deibert RJ, 'Reset: Reclaiming the Internet for Civil Society' (House of Anansi Press 2020)

Dinesh BM and Narender A, 'Public Wi-Fi Networks and Privacy: Regulatory Imperatives in Developing Economies' (2022) 14 Journal of Internet Law 1

Lyon D, 'Surveillance Society: Monitoring Everyday Life' (Open University Press 2001)

Parsheera S, 'Data Governance in India: Evolving Frameworks and Emerging Challenges' (NIPFP Working Paper No 253, 2019)

Rajagopal A, 'Puttaswamy and the Contours of Informational Privacy' (2018) 30 National Law School of India Review 88

Schwartz PM, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harvard Law Review 1966

Srikrishna BN (chair), 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology 2018)

Suresh M, 'Facial Recognition Technology and Fundamental Rights in India' (2022) 4(1) Indian Constitutional Law Review 45

Zuboff S, 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (PublicAffairs 2019).