THE ARCHITECTURE OF CONTROL: TRACING THE EVOLUTION OF INDIA'S DIGITAL SURVEILLANCE LAWS FROM THE TELEGRAPH ACT TO THE TELECOMMUNICATIONS ACT, 2023

Jisa Jos, LLB, Government Law College, Thiruvananthapuram

ABSTRACT

This paper traces the historical and legal evolution of India's surveillance framework, examining its journey from the colonial-era Indian Telegraph Act of 1885 to the modern Telecommunications Act of 2023. It analyses how the foundational principles of state interception, established under the Telegraph Act, have been adapted, expanded, and embedded into the digital age through subsequent legislation, such as the Information Technology Act, 2000, and its associated rules. The paper argues that India's surveillance jurisprudence is characterized by a persistent legal path dependency, where colonial-era imperatives of control have been systematically digitized and strengthened, often at the expense of the fundamental right to privacy. It critically examines the key provisions of the new Telecommunications Act, 2023, assessing it not as a break from the past but as a culmination of this evolutionary process, which grants the state expansive, centralized powers with insufficient judicial oversight. The paper concludes by discussing the profound implications of this architecture of control for democracy and civil liberties in India.

Keywords: Surveillance Laws (India), Telecommunications Act 2023, Indian Telegraph Act 1885, Digital Privacy, National Security, Interception & Monitoring, Information Technology Act 2000, Right to Privacy

1. Introduction

The rapid digitization of the Indian economy and society has been paralleled by an equally rapid expansion of the state's surveillance capabilities. At the heart of this expansion lies a complex legal architecture, the foundations of which were laid in the 19th century. The journey from the Indian Telegraph Act of 1885 to the Telecommunications Act of 2023 represents more than a mere technological update; it is a story of legal continuity, where frameworks designed for a colonial state have been recalibrated for a digital republic.[1]India's surveillance laws have evolved through a process of *legal osmosis,* where the expansive powers granted under the archaic Telegraph Act have permeated and shaped every subsequent piece of legislation, including the new Telecommunications Act.

The landmark recognition of the right to privacy as a fundamental right in *Justice K.S. Puttuswamy v.Union of India* (2017)[2] created a constitutional imperative for proportionality and oversight. However, the subsequent legislative response, particularly the Telecommunications Act of 2023, appears to sidestep these rigorous standards, instead cementing a framework of executive-centric control. **This legislative evolution demands critical scrutiny for three primary reasons. First, the technological context has undergone a transformation beyond recognition. The colonial state intercepted telegraphs, a limited and slow form of communication. The modern Indian state seeks to monitor a vast, interconnected digital ecosystem encompassing everything from personal messaging and financial transactions to social networks and IoT devices. The potential for a chilling effect on free speech, association, and the right to be let alone is therefore exponentially greater.**[3]

Second, a fundamental tension exists between the state's legitimate interest in national security and its duty to protect citizens' fundamental rights. The persistent use of vague and overarching terms like "public safety" and "public emergency" without stringent, legally enshrined checks and balances tilts this balance overwhelmingly in favour of state power. **Third, the method of this expansion—often through executive-made rules rather than open parliamentary debate—raises serious concerns about democratic accountability and transparency in the process of crafting the state's surveillance powers.**[4]

This research paper is structured in four parts. Part 2 delves into the colonial origins of surveillance under the Telegraph Act, 1885 and its foundational principles. Part 3 examines the expansion of this framework into the digital realm via the Information Technology Act, 2000, and its controversial subordinate rules. Part 4 provides a critical analysis of the surveillance

[1] Ujwala Uppaluri, From Telegraph to Internet: The Colonial Roots of India's Digital Surveillance State, 12 Indian J.L. & Tech. 45, 47 (2019).
[2] Justice K.S. Puttuswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[3] Chinmayi Arun, The Case for Privacy in India, 52 Cornell Int'l L.J. 399, 415 (2019).
[4] Ujwala Uppaluri, *Rule by Rules: The Problem of Executive Law-Making in India's Digital Policy*(2022).

provisions within the new Telecommunications Act, 2023, evaluating them against constitutional benchmarks. The paper concludes by summarizing the trajectory of India's surveillance state and its implications for democratic governance.

2. The Colonial Blueprint: The Indian Telegraph Act, 1885

The Indian Telegraph Act of 1885 was a product of its time—an era of colonial administration concerned with control, public order, and the suppression of dissent. Section 5(2) of the Act granted the central or state government the power to intercept messages on the occurrence of any "public emergency" or in the interest of "public safety".This provision was deliberately crafted with ambiguous and broad terms. The Act did not define "public emergency," leaving it to the subjective satisfaction of the executive. This granted the state sweeping discretionary power with minimal checks and balances. The only procedural safeguard was a review committee to examine the legality of interceptions post-facto, a mechanism established not by the statute itself but by the Supreme Court decades later in People's Union for Civil Liberties (PUCL) v. Union of India.[5]

The colonial intent behind this legal architecture was not to balance state power with individual liberty, but to preserve the sovereignty of the state apparatus itself. The "telegraph" was a strategic technology of empire, crucial for administrative control, military mobilization, and intelligence gathering. The power to control information flow was, therefore, a paramount sovereign function,vesting absolute discretion in the hands of the government.[6]This established a foundational paradigm where surveillance was treated as an inherent executive privilege, rather than a power requiring strict legislative justification and judicial oversight. For over a century, this framework operated with little challenge. It was only in the aftermath of the telecommunications boom of the 1990s and a public interest litigation alleging widespread wiretapping for political purposes that the Supreme Court was compelled to intervene.

In the landmark ***PUCL*** judgment, the Court recognized the severe threat to privacy and free speech posed by the unfettered power under Section 5(2). The Court read down the wide ambit of the provision and laid down procedural safeguards to prevent its abuse. It mandated that interception orders could only be issued by the Home Secretary of the central or state government (with limited exceptions), that the order must specify the reason, and that the interception must be destroyed after its purpose was met.

In the *PUCL* judgment, the Court read down the wide ambit of Section 5(2) and laid down procedural safeguards to prevent its abuse. It mandated that interception orders could only be issued by the Home Secretary of the central or state government (with limited exceptions), that

[5] People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568 (India).
[6] Ravi Sundaram, Pirate Modernity: Delhi's Media Urbanism 44 (Routledge 2010).

the order must specify the reason, and that the interception must be destroyed after its purpose was met.However, these safeguards remained judicial guidelines, not codified statutory law, making them vulnerable to executive override. The Telegraph Act established the foundational logic of Indian surveillance: a power rooted in state sovereignty, triggered by vague and overarching exceptions, and initially lacking robust, independent oversight. This logic would prove remarkably durable.

4. Digitizing Surveillance: The Information Technology Act, 2000 and Beyond

With the advent of the internet, the Telegraph Act's scope became limited. The Information Technology Act, 2000, was introduced to provide a legal framework for electronic commerce and digital communication. However, it also became the vehicle for transferring the interception powers of the telegraph era into the digital age. Section 69 of the IT Act, 2000, mirrored Section 5(2) of the Telegraph Act but expanded its scope significantly. It granted the government the power to intercept, monitor, or decrypt any information transmitted through, stored in, or generated by any computer resource.The grounds for interception were also expanded beyond "public emergency" and "public safety" to include "preventing incitement to the commission of any cognizable offence" or for "investigation of any offence."

Unlike a telegraph message, a "computer resource" is all-encompassing. It includes personal computers, smartphones, servers, cloud storage, and any connected device. The data it encompasses is equally vast: emails, instant messages, social media posts, browsing history, documents, photos, and location data. Furthermore, lowering the threshold from "public emergency" to "investigation of any offence" meant that this powerful surveillance tool could potentially be used for routine law enforcement, vastly increasing the scale of possible interception. The law now allowed for the monitoring of a citizen's entire digital life, not just a specific communication channel. This expansion was exacerbated by the creation of subordinate legislation. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, framed under Section 69, created a multi-layered bureaucratic process for authorization.

While introducing some procedure, the rules concentrated power within the executive branch, with the competent authority being a senior official within the Ministry of Home Affairs. A further significant expansion came with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules mandated "significant social media intermediaries" (platforms with large user bases) to enable traceability of messages—effectively breaking end-to-end encryption upon government demand—and to proactively monitor and remove content based on executive orders.[7]This

[7] Prasanna S., PUCL Case: A Half-Won Battle for Privacy, 32 Econ. & Pol. Wkly.(1997).

shifted the burden of surveillance onto private companies, creating a system of *privatized censorship and monitoring.*

4. Cementing the Framework: The Telecommunications Act, 2023

The Telecommunications Act, 2023, which seeks to replace the Indian Telegraph Act, 1885, and the Indian Wireless Telegraphy Act, 1933, was presented as a forward-looking reform for the digital era. However, its provisions on surveillance, particularly Section 20(2), demonstrate a regression to the broad, colonial-era standard rather than an evolution towards privacy-centric governance. According to Section 20(2), in the event of a "public emergency" or in the interest of "public safety," the government may "temporarily possess any telecommunication service or network." It's telling that the exact, ambiguous terms from the 1885 Act are being used. It disregards the Puttuswamy judgment's jurisprudential advancement and the demand for more precise and limited privacy restrictions.

Most critically, the 2023 Act fails to codify the procedural safeguards mandated by the Supreme Court in the PUCL case. There is no mention of the rank of the authorizing officer, the need to specify the reason, the duration of interception, or the process for destruction of data. By remaining silent, the Act delegates the creation of these critical safeguards to the executive through rule-making power, effectively allowing the government to write its own rules for surveillance.[8]This deliberate omission is the Act's most significant flaw. It represents a conscious choice to avoid subjecting state surveillance power to transparent, parliamentary scrutiny and to instead retain its administration within the opaque realm of executive rule-making. This structure fundamentally violates the proportionality standard laid down in *Puttuswamy*, which requires that any invasion of privacy must be done through a law that is both procedurally and substantively just, fair, and reasonable.

A law that grants the state the power to take possession of entire networks—effectively enabling mass surveillance—while outsourcing the creation of its checks and balances to the very entity that wields the power, cannot be considered a reasonable or just law. It creates a predictable and severe risk of abuse, as the rules can be amended without legislative debate to further expand executive discretion.[9]Furthermore, the Act’s scope now includes the entire modern telecommunication ecosystem, from ISPs and mobile networks to app-based calling services, meaning the power to "take possession" is more expansive and intrusive than ever before.

By cementing this framework into law, the Telecommunications Act, 2023, normalizes extraordinary powers, effectively placing the foundational infrastructure of India's digital society under a perpetual

[8] Suhrith Parthasarathy, *The Telecommunications Bill, 2023 and the Problem of Executive Overreach*, The Hindu (Dec.2023)
[9] Internet Freedom Found*., Analysis of the Telecommunications Bill, 2023: A Deep Dive into the Surveillance State* (Dec. 2023)

shadow of state control. This creates a dangerous scenario where the core legislative provision grants power, while the crucial checks and balances are left to the discretion of the same entity that wields the power. This structure is antithetical to the principle of proportionality and judicial oversight required for the infringement of a fundamental right.

5. Conclusion: An Unchecked Trajectory

The evolution of India's surveillance laws reveals a clear and concerning trajectory. The architecture designed for a colonial state has not been dismantled but has been meticulously digitized and fortified. The transition from the Telegraph Act to the IT Act to the Telecommunications Act represents a process of normalization and expansion, where exceptional powers have become the default toolkit of governance. The Supreme Court's jurisprudence in PUCL and Puttuswamy provided moments of constitutional correction, insisting that privacy is not a gift from the state but a right against it. However, the legislative response, culminating in the Telecommunications Act, 2023, has been to pay lip service to this right while constructing a legal framework that empowers the executive to suspend it with ease.

The absence of strong, independent judicial oversight, the reliance on vague and overarching terms, and the delegation of safeguard creation to the executive branch create a system ripe for abuse. For a vibrant democracy like India, navigating the complexities of national security and individual liberty in the digital age requires a legal framework built on transparency, proportionality, and trust. The current architecture, with its roots in control and its eyes on pervasive monitoring, leans dangerously towards the former at the irreversible expense of the latter. This trajectory remains unchecked because the legal framework systematically avoids building meaningful, external accountability into its design.

The future it portends is one of normalized surveillance, where the mere possibility of being monitored could have a profound chilling effect on freedom of speech, dissent, and association—the very bedrock of a democratic society. The promise of digital India, founded on empowerment and inclusion, is undermined by a parallel architecture of control and suspicion. Ultimately, the question posed by this legal evolution is not merely about privacy, but about what kind of democracy India seeks to be: one that trusts its citizens and is trusted by them, or one that views them as subjects to be managed. Reversing this trajectory will require a future legislative intervention courageous enough to break from its colonial legacy and unequivocally place fundamental rights at the heart of India's digital future.