PRIVACY, PROPORTIONALITY, AND THE TELECOM ACT, 2023: A CONSTITUTIONAL ANALYSIS OF SURVEILLANCE POWERS

Ayushi Singh, Gujarat National Law University, Gandhinagar

ABSTRACT

The Telecommunications Act, 2023 marks a significant shift in India's legal framework for regulating communication services. While the Act replaces colonial-era legislation with a more contemporary structure, it also introduces expansive executive powers for intercepting messages, blocking communication, and suspending telecom services. These powers, framed in broad terms and lacking institutional safeguards, raise serious concerns about their compatibility with the constitutional right to privacy.

This article examines the surveillance-related provisions of the Telecom Act through the lens of key Supreme Court decisions, including *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *People's Union for Civil Liberties v. Union of India*, and *Anuradha Bhasin v. Union of India*. These cases collectively establish that any intrusion on fundamental rights must satisfy the tests of legality, necessity, and proportionality.

The article argues that the Telecom Act, in its current form, fails to incorporate the procedural and institutional safeguards required under constitutional jurisprudence. It concludes by recommending legal reforms that would align the Act with constitutional principles while maintaining the state's ability to ensure national security.

Introduction

In December 2023, the Indian Parliament passed the Telecommunications Act, 2023 (**'Telecom Act'**), repealing the colonial-era Indian Telegraph Act, 1885.[1] The new law was introduced to match the pace of technological development and improve the way telecommunication services are regulated in the country. While it does modernise the legal framework for telecom, the Act also gives the government broad powers to intercept messages, block communication, and suspend telecom services.[2] These provisions raise important questions about individual privacy and the potential for state overreach.

India has seen a rapid digital transformation in the last decade. More people now use mobile phones, the internet, and online services than ever before. In this environment, laws that govern communication are not just about infrastructure. They also affect personal freedom and constitutional rights. The Telecom Act claims to protect national security and public safety, but the way it gives these powers to the executive without clear checks and balances has drawn criticism.

This article looks at the surveillance-related provisions of the Telecom Act in light of recent constitutional developments. The Supreme Court of India has laid down important principles on the right to privacy and state surveillance in cases like *Justice K.S. Puttaswamy v. Union of India* (2017), *People's Union for Civil Liberties v. Union of India* (1997), and *Anuradha Bhasin v. Union of India* (2020). These decisions form the legal background against which new laws like the Telecom Act must be tested.

The article argues that while national security is an important concern, it cannot come at the cost of basic constitutional rights. Any surveillance power must follow the principles of legality, necessity, and proportionality.

Key Provisions of the Telecom Act, 2023

The Telecom Act introduces a new regulatory structure for telecommunication services in India. One of the most significant parts of the Act relates to how the government can intercept, block, or suspend communication services. These powers are often justified in the name of

[1] The Telecommunications Act, § 2(1), No. 44, Acts of Parliament, 2023 (India).
[2] *Id.* §§ 20, 21.

national security, public order, or during times of emergency. However, some of these provisions have raised legal and constitutional concerns.

1. Interception and Disclosure of Messages

Section 20 of the Act allows the central government, or any state government, to intercept or detain messages if it is in the interest of India's sovereignty, security, or public order.[3] The government can also direct telecommunication service providers to assist in this process. While similar powers existed under the Indian Telegraph Act, 1885, the new law retains the same vague language. The section does not set out specific procedural safeguards or independent oversight mechanisms.

This is important because surveillance without accountability may lead to misuse. There is no provision in the Act that requires prior judicial approval for interception. Nor does it provide for any post-facto review by an independent authority. This creates the risk of secret and unchecked surveillance, which goes against the constitutional principle of limited government.

2. Blocking of Messages and Suspension of Services

Section 20(2) also empowers the government to block the transmission or reception of messages under similar grounds.[4] This means that messages on platforms such as messaging apps or social media may be blocked if the government believes they pose a risk to public order or national security.

In addition, Section 20(3) allows for the temporary suspension of telecommunication services, which includes phone and internet services. This can be done in the event of a public emergency or in the interest of public safety.[5] Again, the law does not define what qualifies as a public emergency. Nor does it prescribe any limit on how long such a suspension can last. This gives the executive wide discretion to shut down networks without accountability.

3. Definition of Telecommunication Services

Section 3(7) of the Act gives a very broad definition of telecommunication services.[6] It includes

[3] The Telecommunications Act, § 20(1), No. 44, Acts of Parliament, 2023 (India).
[4] *Id.* § 20(2).
[5] *Id.* § 20(3).
[6] *Id.* § 3(7).

services like broadcasting, machine-to-machine communication, and over-the-top (OTT) communication services. This means that apps like WhatsApp, Signal, and Zoom could also fall within the scope of the Act. Including these services under telecom regulation may have a chilling effect on digital communication and free speech.

These provisions suggest that while the law updates the licensing and operational framework for telecom providers, it also expands state power in ways that may affect constitutional rights. The next section will examine whether these powers meet the legal standards set by the Supreme Court in key privacy and surveillance cases.

Surveillance and the Constitutional Right to Privacy

The Telecom Act allows the government to intercept messages and suspend telecommunication services for a range of reasons. These include protecting the sovereignty of India, ensuring public order, and responding to public emergencies.[7] However, such powers must be tested against the constitutional right to privacy, which the Supreme Court of India recognised as a fundamental right in 2017.

1. The Right to Privacy as a Fundamental Right

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court held that the right to privacy is protected under Article 21 of the Constitution.[8] The Court laid down a three-part test to assess whether any restriction on this right is valid. The test requires that any restriction must be based on a law (legality), must pursue a legitimate state interest (necessity), and must be the least intrusive means available (proportionality).[9]

This test is relevant when examining the surveillance powers under the Telecom Act. Section 20 of the Act permits interception and service suspension on grounds such as national security and public safety.[10] While these are legitimate concerns, the Act does not contain detailed procedures to ensure necessity or proportionality. There is also no requirement for independent oversight or prior judicial approval.

[7] The Telecommunications Act, § 20, No. 44, Acts of Parliament, 2023 (India).
[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[9] *Id*. at 180.
[10] The Telecommunications Act, § 20, No. 44, Acts of Parliament, 2023 (India).

2. Lack of Procedural Safeguards

The Supreme Court has consistently held that fundamental rights cannot be overridden by vague or discretionary state powers. In *Puttaswamy*, the Court emphasised that laws affecting privacy must not only serve a legitimate aim but also be proportionate in scope and effect.[11] However, the Telecom Act does not define the threshold for what qualifies as a public emergency or public safety concern. Nor does it explain how such decisions are to be reviewed or challenged.

This lack of clarity opens the door to arbitrary decision-making. Without procedural safeguards, interception powers may be used in a way that discourages free speech, stifles dissent, or targets specific groups.

3. No Provision for Judicial or Independent Oversight

A key issue with the Telecom Act is the absence of independent or judicial oversight over interception decisions. Under Section 20, the power to approve interception rests entirely with the central or state government.[12] There is no requirement for judicial authorisation or post-facto review by an independent authority.

This is particularly concerning given India's past experience with surveillance systems like the Central Monitoring System (CMS), which allowed the government to directly access call and data records without transparency.[13] The *Puttaswamy* judgment warned against "excessive state surveillance" and stressed the need for legal safeguards and institutional accountability.[14]

In contrast, many democratic jurisdictions have included oversight mechanisms. For example, the United Kingdom's Investigatory Powers Act requires judicial commissioners to authorise interception warrants.[15] Similarly, the United States' Foreign Intelligence Surveillance Act (**'FISA'**) established a special court to oversee surveillance related to national security.[16] The

[11] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at 201.
[12] The Telecommunications Act, § 20(1), No. 44, Acts of Parliament, 2023 (India).
[13] Vikas Bajaj, *India's Surveillance State*, THE NEW YORK TIMES (July 10, 2014), https://www.nytimes.com/2014/07/11/opinion/indias-surveillance-state.html (accessed 16 June 2025).
[14] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at 247.
[15] Investigatory Powers Act 2016, c. 25, § 23 (UK).
[16] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (USA).

Telecom Act does not include any such oversight model, making it inconsistent with international best practices and constitutional norms.

4. Impact on Individual Liberty

The absence of oversight and safeguards has a direct impact on the liberty and dignity of individuals. Without a legal process that allows users to challenge surveillance, there is no check on how or why an individual may be monitored. The chilling effect on expression, dissent, and association is difficult to measure, but it is significant.

In the *Puttaswamy* case, the Court recognised that privacy includes not only personal autonomy but also the freedom to think and communicate without fear.[17] This makes it clear that any law permitting surveillance must not be vague, overbroad, or devoid of accountability.

In the current form, the Telecom Act fails to meet the standards laid down in *Puttaswamy*. While it may serve important state interests, it does so at the risk of weakening individual rights. A surveillance regime that operates without transparency or checks is inconsistent with a constitutional democracy.

The power to intercept communication under Indian law has existed since the colonial era. One of the most important decisions on this issue is *People's Union for Civil Liberties v. Union of India* ('PUCL'), which dealt with telephone tapping under the Indian Telegraph Act, 1885.[1] In that case, the Supreme Court held that although the state may intercept communications in the interest of public safety or national security, such powers must be exercised within a framework of legal safeguards. The judgment continues to guide the interpretation of surveillance laws and their relationship to constitutional rights.

Institutionalising State Control – A Look Back at PUCL

The power to intercept communication under Indian law has existed since the colonial era. One of the most important decisions on this issue is *People's Union for Civil Liberties v. Union of India* ('PUCL'), which dealt with telephone tapping under the Indian Telegraph Act, 1885.[18] In that case, the Supreme Court held that although the state may intercept communications in the

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at 234.
[18] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

interest of public safety or national security, such powers must be exercised within a framework of legal safeguards. The judgment continues to guide the interpretation of surveillance laws and their relationship to constitutional rights.

1. The Origins of Procedural Safeguards

In *PUCL*, the petitioners challenged the constitutionality of Section 5(2) of the Telegraph Act, which allowed the government to intercept communications under certain conditions.[19] The Court upheld the provision but introduced a set of procedural requirements to ensure it was not misused. It held that interception must be approved by a senior official, specifically the Home Secretary at the central or state level. The government's decision must be based on actual material that justifies such an intrusion into private communication, and a review committee must examine the order within a prescribed period.[20]

These safeguards were intended to ensure that the exercise of surveillance powers did not become arbitrary. The Court acknowledged that while the state may need to intercept messages in some cases, such authority must be balanced against the individual's right to privacy and dignity under Article 21 of the Constitution.

2. How the Telecom Act Measures Up

Section 20 of the Telecommunications Act, 2023 retains the government's power to intercept communications or suspend telecommunication services under similar grounds such as public order and national security.[21] However, unlike the judgment in *PUCL*, the new Act does not lay down any detailed safeguards in its text. It does not clarify who within the government must authorise an interception order. Nor does it require the reasons to be recorded in writing, or mandate any kind of independent or time-bound review. The omission of these basic checks is notable, especially since the Supreme Court in *PUCL* had expressly required them to prevent the misuse of state power.[22]

[19] *Id.*
[20] *Id.* at 308–309.
[21] The Telecommunications Act, § 20, No. 44, Acts of Parliament, 2023 (India).
[22] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, at 312.

3. Increased Discretion and Centralisation

The structure of the Act also raises concerns about increasing centralisation and executive discretion. Section 20 grants interception authority to both the central and state governments but does not require them to consult an independent authority or involve technical experts in the decision-making process. There is no institutional mechanism to scrutinise or review whether the decision was proportionate or even necessary. In *PUCL*, the Court recognised that unchecked powers of interception could be used to monitor political dissidents, journalists, and activists.[23] The danger of such misuse is even greater today, as modern surveillance tools allow for real-time tracking, keyword detection, and bulk data collection.

In addition, the Act defines telecommunication services broadly under Section 3(7), covering not only traditional telephone and radio services but also digital platforms and internet-based communication.[24] This expansive scope widens the net of potential surveillance without introducing parallel safeguards to constrain abuse.

4. The Need for Legislative Safeguards

The judgment in *PUCL* made clear that surveillance powers, even when lawfully granted, must be exercised within a protective constitutional framework. While the Court's reading of procedural safeguards into Section 5(2) was an important step, relying solely on judicial interpretation is not enough. Surveillance laws must incorporate these safeguards into the legislative text to ensure consistency, predictability, and accountability.

The Telecom Act, in its current form, does not reflect the balanced approach mandated in *PUCL*. Instead, it creates a framework that enables executive surveillance without procedural control. This departs from the spirit of constitutionalism and undermines the citizen's ability to enjoy rights without undue intrusion.

Access, Shutdowns, and the Public's Right to Know

Alongside interception powers, the Telecommunications Act, 2023 also grants the government authority to suspend telecom services, including the internet. This is provided under Section

[23] *Id.*
[24] The Telecommunications Act, § 3(7), No. 44, Acts of Parliament, 2023 (India).

20(3), which states that services may be suspended on the occurrence of a public emergency or in the interest of public safety.[25] However, like the interception provisions, this section does not include clear procedures, definitions, or oversight mechanisms. This absence is concerning, particularly given India's recent history with prolonged internet shutdowns, and must be assessed against the standards set by the Supreme Court in *Anuradha Bhasin v. Union of India*.

1. The Legal Standard for Internet Shutdowns

The *Anuradha Bhasin* case was filed in response to the internet restrictions imposed in Jammu and Kashmir in August 2019, following the abrogation of Article 370. The petitioners challenged the constitutionality of the restrictions, arguing that indefinite suspension of the internet violated the rights to freedom of expression and trade under Article 19 of the Constitution.[26] The Supreme Court, while not ordering immediate restoration of services, laid down important principles that apply to any suspension of internet access by the state.

The Court held that the freedom of speech and expression and the right to carry on trade or business through the internet are protected under Article 19.[27] It ruled that any restriction on these rights must be reasonable, and satisfy the test of legality, necessity, and proportionality. Crucially, the Court observed that indefinite suspension of internet services is not permissible, and that such orders must be reviewed periodically by a competent authority.[28]

2. Comparing the Telecom Act with Anuradha Bhasin

Despite the Supreme Court's clear guidance, Section 20(3) of the Telecom Act does not include any provision requiring the government to periodically review suspension orders. It also does not define what qualifies as a public emergency or public safety issue. This gives the executive significant discretion to impose network shutdowns, even for extended periods. The absence of statutory safeguards becomes problematic when such powers are used during protests, elections, or in politically sensitive regions.

The Court in *Anuradha Bhasin* emphasised that any restriction must be backed by a reasoned order, and that orders affecting fundamental rights must be made publicly available to ensure

[25] The Telecommunications Act, § 20(3), No. 44, Acts of Parliament, 2023 (India).
[26] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[27] Id. at 664.
[28] Id. at 672.

accountability.[29] The Telecom Act does not require such transparency. In practice, this means that telecom shutdowns may be ordered without public justification, and affected persons may have no avenue to challenge or even access the basis of the decision.

3. The Consequences of Unchecked Suspension Powers

In recent years, India has led the world in the number of internet shutdowns imposed by a single country.[30] These shutdowns have disrupted access to education, healthcare, banking, and emergency services. They also prevent journalists, lawyers, and citizens from communicating or documenting events. When such measures are imposed without procedural safeguards, they do not merely inconvenience users but infringe on constitutional rights.

The Supreme Court's ruling in *Anuradha Bhasin* made clear that digital access is not a privilege but a medium through which fundamental rights are exercised. The Telecom Act's failure to incorporate the standards laid down in that case reflects a larger trend of prioritising executive power over constitutional accountability.

The "Security" Justification – Can Privacy and National Security Coexist?

A common argument in defence of expansive surveillance powers is that they are necessary to protect national security. Governments across the world have relied on this rationale to justify extraordinary state control over communication networks. In India, the justification of national security is repeatedly invoked in the Telecom Act, particularly in provisions dealing with interception, blocking, and suspension of services.[31] However, a closer look reveals that invoking security cannot be a blanket justification for bypassing constitutional rights.

1. The False Binary Between Privacy and Security

The idea that privacy and national security are in conflict creates a false binary. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court expressly rejected the notion that privacy must always give way to state interests.[32] Instead, the Court laid down a structured approach through the three-fold test: the state must show that its interference with privacy is

[29] Id. at 669.
[30] Software Freedom Law Center, *Internet Shutdowns in India*, https://sflc.in/internet-shutdowns (accessed 16 June 2025).
[31] The Telecommunications Act, § 20, No. 44, Acts of Parliament, 2023 (India).
[32] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

authorised by law, is necessary for a legitimate aim, and is proportionate to that aim.[33] This means that even national security measures must be designed and implemented in a way that minimises harm to individual rights.

The Court also stressed that privacy is essential to the enjoyment of life and liberty. If a security measure undermines the foundational principles of the Constitution, then it does not serve national security in the long term. The risk is that vague or unchecked powers may be used not only against terrorists or criminals but also against civil society actors, political dissenters, or journalists.

2. The Need for Institutional Safeguards

What distinguishes legitimate state action from overreach is the presence of institutional safeguards. In jurisdictions such as the United Kingdom, the United States, and Germany, national security surveillance is subject to judicial or parliamentary oversight.[34] The United Kingdom's Investigatory Powers Act, for instance, requires a special judicial body to review surveillance orders.[35] Similarly, the United States' FISA established a special court to authorise surveillance in national security cases.[36] These frameworks aim to ensure that the security agencies are accountable, even if the details of their operations remain classified.

In contrast, the Telecom Act does not introduce any oversight mechanism for its surveillance-related provisions. There is no requirement for prior judicial authorisation, post-facto review, or parliamentary scrutiny. The power to monitor, block, or shut down communications is entirely concentrated in the executive, without checks from other branches of government.

3. Constitutional Security Must Include Rights

National security, as a constitutional value, cannot be separated from the values of liberty, dignity, and democratic accountability. A model of security that disregards rights is not merely unjust but also unsustainable. The Supreme Court in *Puttaswamy* acknowledged this by holding that privacy is not an elitist concern but a necessary condition for free thought, personal

[33] Id. at 180.
[34] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 91 (2010).
[35] Investigatory Powers Act 2016, c. 25, § 23 (UK).
[36] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (USA).

autonomy, and democratic participation.[37]

The Telecom Act, by omitting any framework for balancing privacy with state interests, reflects an outdated understanding of security. It assumes that giving the state more control will automatically produce safety. But a truly secure society is one in which both the state and the individual are protected through law. Surveillance laws that fail to observe this balance do more harm than good.

Conclusion and Recommendations

The Telecom Act, 2023 represents a major shift in India's regulatory framework for communication services. It modernises several aspects of licensing and infrastructure management, but it also introduces or retains broad surveillance powers without clear legal safeguards. The Act allows the government to intercept, block, and suspend telecom services on vaguely defined grounds such as public order, national security, or public safety. While these powers are not new, their formal recognition in a modern statute without updated safeguards raises serious concerns.

India's constitutional framework, particularly as developed through judicial interpretation, requires that any restriction on fundamental rights must be legal, necessary, and proportionate. The Telecom Act, in its present form, does not meet these standards. It does not mandate judicial authorisation, fails to provide for independent review, and offers no clear mechanism for transparency or accountability.

If the state's interest in national security is to be pursued within a constitutional democracy, it must be balanced against the individual's right to privacy, dignity, and freedom of expression. Surveillance powers must operate within a framework of law that ensures oversight, prevents abuse, and enables challenge.

To move toward this balance, Parliament should consider amending the Act to include specific safeguards. These could include requiring judicial or parliamentary approval for interception orders, mandating that reasons be recorded in writing, introducing a statutory review committee, and ensuring public access to the rationale behind service suspensions. Such steps

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at 236.

would not only bring the Act in line with constitutional standards but also improve public trust in state institutions.

In a democracy, surveillance cannot be an unchecked executive function. It must be lawful, accountable, and proportionate. The Telecom Act, if left as it is, risks shifting India toward a surveillance state where individual rights are subordinated to opaque claims of public interest. A truly secure society must protect both the nation and its people through laws that are both effective and just.