
EXECUTIVE WATCHING EXECUTIVE: THE MISSING INDEPENDENT OVERSIGHT BODY IN THE TELECOMMUNICATIONS INTERCEPTION RULES, 2024

Rishabh Sisodiya, Samarth Udasin & Rohit Kadian,
National Law Institute University, Bhopal

ABSTRACT

The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, notified on 6 December 2024 under the Telecommunications Act, 2023, replaced a colonial-era interception framework with a fresh statutory scheme, yet reproduced its most significant institutional defect: the body charged with reviewing interception orders is composed entirely of serving executive officers, appointed by, and answerable to, the very government whose orders it reviews. This paper argues that the Review Committee, as constituted under rule 5 of the 2024 Rules, fails the sufficient safeguards limb of the proportionality standard articulated by the Supreme Court of India in *Justice K S Puttaswamy v Union of India*¹ and subsequently read as the ‘fifth prong’ of proportionality in *Gujarat Mazdoor Sabha v State of Gujarat*² and *Ramesh Chandra Sharma v State of Uttar Pradesh*³. It is tested further against the independent-authorisation standard laid down by the Grand Chamber of the European Court of Human Rights in *Big Brother Watch and Others v United Kingdom*⁴. Drawing on comparative institutional models from the United Kingdom, Germany and South Africa, and on recent judicial engagement with the 2024 Rules including the Chhattisgarh High Court’s 2026 ruling in *Shri Ravi Shankar Ji Maharaj v Central Bureau of India*⁵, the paper proposes a concrete institutional redesign: a statutorily independent Communications Oversight Board, headed by a retired Judge of the Supreme Court or a High Court, empowered with binding ex-post review and, for non-emergency orders, ex-ante concurrence.

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

²Gujarat Mazdoor Sabha v State of Gujarat [2020] 13 SCR 886, [50]–[51].

³Ramesh Chandra Sharma v State of Uttar Pradesh, Civil Appeal No 8819 of 2022 (SC, 20 February 2023) [49]–[51]; see also Rudraksh Lakra, ‘Guest Post: Proportionality’s Fifth Prong – A Reassessment’ (Indian Constitutional Law and Philosophy, 7 March 2023) <<https://indconlawphil.wordpress.com/2023/03/07/guest-post-proportionalitys-fifth-prong-a-reassessment/>> accessed 22 August 2026.

⁴Big Brother Watch and Others v United Kingdom App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).

⁵Shri Ravi Shankar Ji Maharaj v Central Bureau of Investigation, CRMP No 1504 of 2026 (Chhattisgarh HC, 7 August 2026).

Keywords: Administrative Law; telecommunications interception; proportionality; independent oversight; Puttaswamy; Big Brother Watch; Review Committee; surveillance reform.

I. Introduction

On 6 December 2024, the Department of Telecommunications notified the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 ('the 2024 Rules'), under section 20 of the Telecommunications Act, 2023.⁶ The Rules supersede rules 419 and 419A of the Indian Telegraph Rules, 1951, closing a chapter of interception law that had, for nearly two decades, rested on subordinate legislation traceable to the Supreme Court's 1996 intervention in *People's Union for Civil Liberties v Union of India*⁷. The reform was an opportunity: a chance to re-engineer India's interception architecture in the image of the post-2017 constitutional order, in which privacy is a fundamental right and any executive intrusion upon it must satisfy a structured proportionality standard. That opportunity was, in one crucial respect, declined.

The 2024 Rules retain almost verbatim the institutional design of the 1951 Rules they replace. Interception orders are authorised by a 'competent authority' who is, invariably, a serving bureaucrat: the Union Home Secretary at the Centre, or the corresponding State Home Secretary, with a Joint Secretary-rank officer empowered to act in 'unavoidable circumstances'.⁸ Those orders are then reviewed, not by a court, not by Parliament, and not by any person independent of the government, but by a Review Committee whose entire membership is drawn from the executive branch: at the Union level, the Cabinet Secretary as chairperson together with the Secretary of Legal Affairs and the Secretary of Telecommunications; at the State level, the Chief Secretary together with the Law Secretary and one further Secretary.⁹ This is, in substance, the same body reviewing the same government's own orders – executive watching executive.

This paper asks a narrow but consequential question: does a review mechanism composed entirely of executive appointees, reviewing the interception decisions of fellow executive

⁶Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, GSR 754(E), 6 December 2024, made in exercise of powers under s 20(2)(a) and s 20(4) read with s 56(2)(t)–(u) of the Telecommunications Act 2023 (Act 44 of 2023).

⁷*People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301 ('PUCL').

⁸Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 3, r 2(1)(c).

⁹Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 5.

officers, satisfy the constitutional and comparative standards that now govern surveillance law in India? It answers in the negative, and it does so by testing the Review Committee against two independent, mutually reinforcing benchmarks. The first is doctrinal and domestic: the requirement of ‘sufficient safeguards’ against the abuse of a rights-infringing measure, which the Supreme Court has increasingly treated as the fifth and final limb of the proportionality standard first articulated in the privacy judgment, *Justice K S Puttaswamy v Union of India*. The second is comparative and persuasive: the requirement, laid down by the Grand Chamber of the European Court of Human Rights in *Big Brother Watch and Others v United Kingdom*, that any regime of communications surveillance be authorised, at the outset, by a body independent of the executive. Neither benchmark demands a judge; both demand independence. The Review Committee, structurally, has none.

The argument proceeds in six further parts. Part II sets out the architecture of interception under the 2023 Act and the 2024 Rules, including the September 2025 amendment and recent judicial engagement with the Rules. Part III traces the doctrinal evolution of the proportionality standard from *Puttaswamy* through *Gujarat Mazdoor Sabha* to *Ramesh Chandra Sharma*, establishing ‘sufficient safeguards’ as an independent constitutional requirement. Part IV applies that requirement to the Review Committee’s composition, workload, and practice. Part V examines *Big Brother Watch* and the Strasbourg ‘quality of law’ test. Part VI surveys comparative institutional design in the United Kingdom, Germany, and South Africa. Part VII proposes a concrete redesign, and Part VIII concludes.

II. The Architecture of Interception under the 2023 Act and the 2024 Rules

Section 20(2) of the Telecommunications Act, 2023 empowers the Central Government, a State Government, or a specially authorised officer to direct, on the occurrence of a public emergency or in the interest of public safety, that a message or class of messages be intercepted, detained, or disclosed, where necessary or expedient in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or the prevention of incitement to an offence.¹⁰ Neither ‘public emergency’ nor ‘public safety’ is defined in the Act or the Rules, a gap that commentators identified during the consultation on the draft Rules and that persists in the notified text.¹¹

¹⁰Telecommunications Act 2023 (Act 44 of 2023), s 20(2).

¹¹PRS Legislative Research, ‘Draft Telecom Rules on Interception, Temporary Suspension of Services, and

The 2024 Rules operationalise section 20(2). An authorised agency, a law-enforcement or security agency notified by the Central Government, executes an interception order issued by the ‘competent authority’: the Union Home Secretary, or the equivalent State Home Secretary, save that an officer not below the rank of Joint Secretary may issue an order in ‘unavoidable circumstances’, an expression the Rules again leave undefined.¹² In remote areas, or for operational reasons, the head or second-most senior officer of the authorised agency at the Central or State level, not below the rank of Inspector-General of Police may issue an order, subject to confirmation by the competent authority within seven working days; if confirmation does not follow within that period, the intercepted material may not be used for any purpose and copies must be destroyed within two working days.¹³ Orders remain valid for sixty days at a time, extendable to a maximum of one hundred and eighty days.¹⁴

Every confirmed interception order must be placed before the relevant Review Committee within seven working days.¹⁵ Rule 5 constitutes that Committee. At the Union level it consists of the Cabinet Secretary, who chairs it, the Secretary of Legal Affairs, and the Secretary of Telecommunications; at the State level, the Chief Secretary chairs a committee comprising the Secretary of Law or the Legal Remembrancer and a further Secretary other than the Home Secretary.¹⁶ The Committee is required to meet at least once every two months, to record its findings on whether interception orders conform to the Act, and, if it finds a defect, to set the order aside and direct destruction of the intercepted material.¹⁷ Records must ordinarily be destroyed every six months by the authorised agency, the competent authority, and the Review Committee alike, unless retained for functional necessity or under court direction.¹⁸

Two features of this design bear emphasis. First, every actor in the chain, the authorised agency that intercepts, the competent authority that authorises, and the Review Committee that reviews is a serving member of the executive branch of the same government. There is no point in the process at which a person independent of the executive, whether a judge, a parliamentarian, or an appointee insulated from executive control, examines the necessity or proportionality of an

Cyber Security 2024’ (Rules and Regulations Review, 28 December 2025).

¹²Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 2(1)(c), r 3(2)–(3).

¹³Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 3(4)–(6).

¹⁴Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 4.

¹⁵Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 7.

¹⁶Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 5.

¹⁷Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 7(4)–(5).

¹⁸Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 22.

interception order before, or shortly after, it takes effect. Second, the Review Committee's remit is confined to legality review of the order's form as to whether it conforms to the Act rather than a substantive re-assessment of necessity or proportionality on the facts, a limitation that becomes significant when the Committee's composition is tested against the constitutional standard in Part IV below.

The 2024 Rules have since been amended once, by the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Amendment Rules, 2025, notified on 12 September 2025.¹⁹ That amendment relaxed the requirement that an authorised agency appoint exactly two nodal officers, permitting instead 'one or more' nodal officers according to operational need; it left the composition, mandate, and powers of the Review Committee wholly untouched.²⁰ The institutional defect identified in this paper is accordingly not a transitional feature of the 2024 Rules awaiting correction; it is a design choice that the Government reaffirmed at the first available legislative opportunity.

That the defect is not merely theoretical is illustrated by the Chhattisgarh High Court's decision in *Shri Ravi Shankar Ji Maharaj v Central Bureau of Investigation*, decided on 7 August 2026.²¹ A Division Bench of the High Court set aside an interception authorisation, the Ministry of Home Affairs' confirmation of it, and the Review Committee's subsequent proceedings, holding that a competent authority's confirmation is merely confirmatory and cannot retrospectively validate an interception that pre-dated the authorisation, and, crucially, that 'neither the Ministry of Home Affairs nor the Review Committee can retrospectively validate interception for an anterior period' once the jurisdictional fact of a lawful authorisation is absent.²² The case is instructive for a reason distinct from its holding on retrospectivity: the Review Committee itself had, at its scheduled sitting, passed proceedings over an interception that a High Court subsequently found to rest on no lawful authorisation at all. A review body drawn from, and answerable to, the same administrative hierarchy that generated the defect did not catch it; a court did. That is precisely the failure mode this paper anticipates from a wholly

¹⁹Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Amendment Rules 2025, GSR 625(E), 12 September 2025.

²⁰Internet Freedom Foundation, 'IFF's Submission to the DoT on the Proposed Amendments to the Interception Rules & the Cyber Security Rules' (Internet Freedom Foundation, 6 August 2025).

²¹*Shri Ravi Shankar Ji Maharaj v Central Bureau of Investigation*, CRMP No 1504 of 2026 (Chhattisgarh HC, 7 August 2026) (Sinha CJ and Agrawal J).

²²LiveLaw, 'Telephone Interception Cannot Be Retrospectively Validated By MHA Confirmation Order: Chhattisgarh High Court' (LiveLaw, 8 August 2026).

executive review mechanism.

III. The Constitutional Touchstone: Puttaswamy and the Fifth Prong of Proportionality

In *Justice K S Puttaswamy v Union of India*, a nine-judge Bench of the Supreme Court held that the right to privacy is protected under Articles 14, 19, and 21 of the Constitution, and that any invasion of that right by the State must satisfy a structured standard of justification.²³ Justice Chandrachud's plurality opinion described a requirement of legality, a requirement of a legitimate State aim, and a requirement of proportionality between the means adopted and the aim pursued.²⁴ Read together with paragraph 49 of the judgment, in which the Court summarised the standard as requiring that State action be sanctioned by law, be necessary in a democratic society for a legitimate aim, be proportionate to the need for interference, and be attended by 'procedural guarantees against abuse of such interference', *Puttaswamy* is now understood to have laid down a four-limbed test in which safeguards against abuse form a distinct and independent element, not a mere afterthought to necessity.²⁵

That fourth limb was made explicit, and numbered, three years later. In *Gujarat Mazdoor Sabha v State of Gujarat*, a three-judge Bench, examining the Gujarat Government's pandemic-era suspension of statutory working-hour protections, articulated the proportionality standard as a five-condition test: that the interference have a legitimate State purpose; that there be a rational nexus between the interference and that purpose; that the measure be necessary to achieve the purpose; that the restriction go no further than is necessary to protect the legitimate objective; and, fifth, that 'the State should provide sufficient safeguards . . . for the possibility of an abuse of such rights-infringing interference'.²⁶ The Court in *Gujarat Mazdoor Sabha* itself acknowledged that this fifth condition had not been expressly numbered in *Puttaswamy*, but held that Justice Chandrachud had, in substance, already read it in.²⁷

The Supreme Court applied and named this fifth prong most recently in *Ramesh Chandra Sharma v State of Uttar Pradesh*, holding expressly that proportionality in Indian constitutional law has attained the form of a 'five-pronged test', tracing that formulation through *Puttaswamy*

²³ Justice K S Puttaswamy v Union of India (2017) 10 SCC 1 [325]–[326] (Chandrachud J), [637]–[638] (Kaul J).

²⁴ *ibid* [325].

²⁵ Ramesh Chandra Sharma v State of Uttar Pradesh, Civil Appeal No 8819 of 2022 (SC, 20 February 2023) [49], summarising Puttaswamy (2017) 10 SCC 1 [49].

²⁶ Gujarat Mazdoor Sabha v State of Gujarat [2020] 13 SCR 886, [50].

²⁷ *ibid* [51].

and *Gujarat Mazdoor Sabha* to a requirement that the State ‘necessarily . . . factor in’ the risk of abuse when a measure ‘leaves sufficient room for abuse’.²⁸ As commentators have observed, this reasoning locates the inquiry into abuse within the design of the impugned measure itself: abuse, on this account, ‘does not take place outside the law, but is baked into the law’, so that a law which leaves insufficient room to prevent or correct abuse is, for that reason alone, disproportionate.²⁹ The Bombay High Court applied precisely this fifth prong within months, in *Kunal Kamra v Union of India*, where Patel J held that the impugned fact-checking mechanism under the amended Information Technology Rules failed the requirement of sufficient safeguards because its grievance-redressal process operated only after the event, leaving the affected party unable to know, in advance, the basis on which content had been flagged.³⁰

This line of authority is directly transposable to the field of communications interception, indeed, it was born of a case, *Gujarat Mazdoor Sabha*, that itself traced its proportionality analysis back to *PUCL*, the very case that produced the 1951 Rules’ Review Committee in the first place.³¹ The Court’s treatment of internet-shutdown orders in *Anuradha Bhasin v Union of India* confirms the point: there too the Court required orders restricting telecommunications to satisfy necessity and proportionality and to be subject to periodic review by a Review Committee — yet the Court itself later re-delegated review to a committee ‘composed of executive officials, the very same body that imposed the restrictions in the first place’, a design that subsequent litigation, and academic comment, has criticised as having produced only a hollow victory for the proportionality standard it purported to enforce.³² If a wholly executive Review Committee was already found wanting in the internet-shutdown context, there is no principled basis on which an identically composed Review Committee should be thought

²⁸Ramesh Chandra Sharma v State of Uttar Pradesh, Civil Appeal No 8819 of 2022 (SC, 20 February 2023) [51].

²⁹Rudraksh Lakra, ‘Guest Post: Proportionality’s Fifth Prong – A Reassessment’ (Indian Constitutional Law and Philosophy, 7 March 2023), discussing Gautam Bhatia, ‘Proportionality’s Fifth Prong’ (Indian Constitutional Law and Philosophy, 23 February 2023).

³⁰Kunal Kamra v Union of India, Writ Petition (L) No 9792 of 2023 (Bombay HC, 26 September 2024) (Chandurkar J, adopting Patel J’s reasoning) [192]–[193].

³¹PUCL (1997) 1 SCC 301 [35]. The Court in PUCL directed the Central Government to frame procedural safeguards, including periodic review by a committee, in the absence of any rules under s 5(2) of the Indian Telegraph Act 1885.

³²Anuradha Bhasin v Union of India (2020) 3 SCC 637 [140]–[151]; Foundation for Media Professionals v Union Territory of Jammu and Kashmir (2020) 5 SCC 746 (directing constitution of a Special Committee, again composed of government officials, to review continuing restrictions); see also the critique in Gautam Bhatia and others, discussed in ‘Anuradha Bhasin v Union of India: An Examination of the Supreme Court’s Application of the Doctrine of Proportionality’ (Contemporary Asia Law Journal, 12 May 2024).

adequate in the more intrusive context of content interception.

Two further points sharpen the doctrinal force of the fifth prong for present purposes. First, the fifth prong asks not merely whether a redress mechanism exists on paper, but whether the mechanism, as designed, meaningfully reduces the risk of abuse; a nominal safeguard that leaves the abuser and the reviewer effectively coextensive with one another cannot discharge that burden. Second, because the fifth prong is treated as an independent limb rather than a component folded into necessity or balancing, a measure may satisfy legality, legitimate aim, and even proportionality *stricto sensu*, and still fail the constitutional standard for want of sufficient safeguards. It follows that the Review Committee's deficiencies cannot be cured simply by pointing to the existence of a competent-authority confirmation requirement, or a sixty-to-one-hundred-and-eighty-day validity ceiling, elsewhere in the Rules: those provisions answer to necessity and proportionality, not to the distinct question of whether the safeguard against abuse is itself adequate.

IV. Testing the Review Committee Against the Fifth Prong

Applying the fifth prong to the Review Committee constituted under rule 5 exposes at least four independent structural weaknesses.

First, composition. Every member of the Central Review Committee, the Cabinet Secretary, the Secretary of Legal Affairs, and the Secretary of Telecommunications is a serving civil servant of the Government of India, appointed by, and removable at the pleasure of, the Union Executive.³³ The same is true, *mutatis mutandis*, of the State Review Committees. None of these officers enjoys security of tenure comparable to a judge; none is appointed through a process involving the judiciary, Parliament, or any body external to the executive. The Parliamentary Standing Committee on Information Technology recommended, as long ago as 2021, that non-official members including retired judges and eminent citizens be included in these very committees, precisely so that review would not remain an intramural exercise; that recommendation was neither incorporated into the draft Rules of 2024 nor into the notified text.³⁴ Civil-society respondents made the identical recommendation during the public consultation on the draft 2024 Rules, urging the inclusion of retired judges or independent

³³Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024, r 5(1).

³⁴PRS Legislative Research, 'Draft Telecom Rules on Interception, Temporary Suspension of Services, and Cyber Security 2024' (Rules and Regulations Review, 28 December 2025), citing the Standing Committee on Information Technology (2021).

experts, and a mechanism for affected individuals to be heard; the Department of Telecommunications did not incorporate it, and the Internet Freedom Foundation's analysis of the consultation record confirms that the rule was notified unchanged.³⁵

Second, functional capacity. The Justice B N Srikrishna Committee, in its 2018 report on data protection, observed that the Review Committee is tasked with examining between fifteen and eighteen thousand interception orders at each bi-monthly sitting, a volume that renders anything beyond the most cursory box-ticking exercise practically impossible.³⁶ Nothing in the 2024 Rules, or in the 2025 amendment, addresses that structural overload: the Committee's bi-monthly sitting frequency is unchanged, its membership unchanged, and its resourcing left unstated. A safeguard that cannot, as a matter of arithmetic, be meaningfully exercised over the volume of decisions entrusted to it is not a sufficient safeguard within the meaning the Supreme Court has given that phrase; it is a formality.

Third, absence of participation and publication. The 2024 Rules make no provision for the individual whose communications have been intercepted to be heard by, or even to be notified of the existence of, the Review Committee's proceedings concerning that interception, whether before or after the fact. Nor do the Rules require the Committee's findings to be published, even in a redacted or aggregated form, save where a court subsequently compels disclosure in the course of litigation, as occurred in the *Shri Ravi Shankar Ji Maharaj* proceedings. This absence of adversarial or public accountability contrasts with the Supreme Court's own direction, in the internet-shutdown context, that Review Committee orders under the parallel telecom-suspension Rules be published, precisely so that the safeguard is not confined to an internal administrative record.³⁷ No equivalent direction, and no equivalent rule, governs the interception Review Committee.

Fourth, the absence of a complementary data-protection check. The Digital Personal Data

³⁵Internet Freedom Foundation, 'Analysis of the Public Comments on the Draft Interception Rules, 2024' (Internet Freedom Foundation, 2026); see also Software Freedom Law Centre, 'Comments on the Draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024' (SFLC.in, 2024).

³⁶Justice B N Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Report, Ministry of Electronics and Information Technology, 2018), discussed in Saikrishna & Associates, 'The Department of Telecommunication Has Released Four Draft Rules for Public Consultation Under the Telecom Act' (Saikrishna & Associates, 13 September 2024).

³⁷PRS Legislative Research, 'Draft Telecom Rules on Interception, Temporary Suspension of Services, and Cyber Security 2024' (Rules and Regulations Review, 28 December 2025), citing the Supreme Court's 2024 direction that findings of Review Committees on internet shutdowns be published.

Protection Act, 2023 will, once its substantive provisions are in force, permit the Central Government to exempt by notification any instrumentality of the State from the whole of the Act where personal data is processed in the interests of the sovereignty and integrity of India, security of the State, or public order.³⁸ That power is not yet operative: the Central Government's commencement notification of 13 November 2025 brought into force only the provisions establishing the Data Protection Board of India (sections 18 to 26) and a handful of miscellaneous provisions, deferring sections 3 to 17, including the exemption power itself, to 13 May 2027. The point made here is accordingly prospective rather than a description of the present institutional landscape. Once section 17 commences, interception activity conducted under the Telecommunications Act and the 2024 Rules will fall squarely within the exemption's natural scope, so that the one general-purpose oversight body Indian law is creating with a mandate to examine the lawfulness of government processing of personal data will be excluded from interception decisions at the very moment its jurisdiction over government processing generally comes into being. On the Act's own timetable, the Review Committee is set to remain, even after the Board becomes operative, the sole institutional check in this architecture.

Taken together, these four features demonstrate that the Review Committee is not merely an imperfect safeguard but a safeguard that is, on the Supreme Court's own articulation of the fifth prong, insufficient: it is staffed exclusively by persons subject to the same chain of executive command that authorised the interception; it lacks the numerical capacity to scrutinise the volume of orders placed before it; it affords no opportunity for the affected individual, or the public, to test its findings; and no independent data-protection authority stands behind it as a check of last resort. A measure that *leaves sufficient room for abuse*, in the words of *Ramesh Chandra Sharma*, is disproportionate regardless of how carefully its necessity and legitimate-aim requirements have otherwise been drafted.

V. The Strasbourg Standard: *Big Brother Watch v United Kingdom* and Independent Oversight

The Grand Chamber of the European Court of Human Rights confronted a structurally similar

³⁸Digital Personal Data Protection Act 2023 (Act 22 of 2023), s 17(2)(a); Ministry of Electronics and Information Technology, Notification GSR 843(E), 13 November 2025, issued under s 1(2) of the Act (bringing sections 18 to 26 and certain miscellaneous provisions into force with effect from 13 November 2025, section 6(9) and section 27(1)(d) with effect from 13 November 2026, and all other provisions, including section 17, with effect from 13 May 2027).

question in *Big Brother Watch and Others v United Kingdom*, a case triggered by Edward Snowden's 2013 disclosures concerning the bulk-interception programme operated under the United Kingdom's Regulation of Investigatory Powers Act 2000.³⁹ The Court did not hold that bulk interception is, in itself, incompatible with Article 8 of the European Convention on Human Rights; it accepted that such regimes serve a vital security function in the face of contemporary threats.⁴⁰ What the Convention requires, instead, is that any interference of this kind be attended by 'end-to-end safeguards' sufficient to guard against arbitrariness and abuse, assessed globally across the different stages of the interception process.⁴¹

Among those end-to-end safeguards, the Grand Chamber identified authorisation by a body independent of the executive as 'one of the fundamental safeguards' that a compliant regime must possess.⁴² Independence from the executive did not, on the Court's reasoning, require that the authorising body be a court: judicial authorisation was described as best practice, but not a categorical requirement, provided that whatever body performed the function was genuinely independent of the branch of government whose surveillance activity it was reviewing, was informed of both the purpose of the interception and the scope of the material likely to be intercepted, and was capable of assessing necessity and proportionality on the merits rather than applying purely formal criteria.⁴³ The Court found that the United Kingdom's regime, as it then stood, lacked precisely this safeguard: authorisation rested with the Secretary of State who is a member of the executive rather than with any body independent of it, and that deficiency, combined with the absence of independent oversight of selectors used to filter intercepted communications, contributed to the Court's finding of a violation of Article 8.⁴⁴ Notably, the Court reached this conclusion notwithstanding that the United Kingdom regime already possessed features considerably more robust than India's: an Interception of Communications Commissioner providing independent oversight of the system as a whole, and an Investigatory Powers Tribunal offering individuals a judicial remedy, features the Court held were, without more, insufficient to counterbalance the absence of independent authorisation at the point of decision.⁴⁵

³⁹*Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) [1]–[10].

⁴⁰*ibid* [340], [386].

⁴¹*ibid* [350].

⁴²*ibid* [377].

⁴³*ibid* [351].

⁴⁴*ibid* [377]–[382], [416].

⁴⁵*ibid* [377].

The Court's companion jurisprudence sharpens the point that independence must be substantive rather than titular. In *Roman Zakharov v Russia*, the Grand Chamber found a violation of Article 8 notwithstanding that Russian law formally required prior judicial authorisation for interception, because the evidence before the Court showed that Russian judges, in practice, applied only formal criteria to authorisation requests without independently verifying necessity or proportionality.⁴⁶ The lesson generalises beyond judicial authorisation to any oversight body, however labelled: a reviewing body that lacks either the institutional distance or the practical incentive to scrutinise the executive's own decisions on the merits fails the safeguard requirement, whatever its formal designation.

Measured against this standard, the Review Committee under rule 5 of the 2024 Rules fails on every element the Grand Chamber identified. It is not independent of the executive: its members are drawn exclusively from the executive hierarchy that issues and executes interception orders, and its chairperson, the Cabinet Secretary, or the Chief Secretary at the State level, sits at the apex of that very hierarchy. It does not authorise at the outset: its function under rule 7 is retrospective review, occurring after an order has already been executed and, given the bi-monthly sitting cycle, potentially months after the interception has run its course. And, as demonstrated in Part IV, there is no reliable evidence that its review descends to a substantive assessment of necessity and proportionality on the facts of each of the fifteen to eighteen thousand orders it is expected to consider at each sitting, rather than a formal check of paperwork, precisely the failure mode the Grand Chamber condemned in *Zakharov*. India is not, of course, bound by the European Convention on Human Rights, and *Big Brother Watch* has no binding force in Indian law. Its value here is persuasive and comparative: it demonstrates that a mature human-rights court, applying a standard closely analogous to India's own proportionality doctrine, and dealing with a country whose interception architecture was in most other respects markedly stronger than India's, still found the presence of independent authorisation to be indispensable. If the United Kingdom's more elaborate safeguards did not suffice without independent authorisation, India's considerably thinner ones cannot.

VI. Comparative Institutional Design

The Srikrishna Committee's own comparative survey in 2018 noted that democratic jurisdictions typically supply one, or both, of two forms of independence absent from the Indian

⁴⁶*Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) [267]–[275].

scheme: legislative oversight, or judicial approval.⁴⁷ Three illustrations sharpen the point. Germany's framework for restricting the secrecy of correspondence, posts, and telecommunications rests on Article 10 of the Basic Law and its implementing legislation. Under this framework, a specially constituted G-10 Commission, comprising members appointed by but not drawn from the executive and chaired by a person qualified to hold judicial office, authorises and reviews strategic and individual interception measures while reporting to a Parliamentary Control Panel, combining legislative accountability with a quasi-judicial authorising function external to the intelligence services themselves. South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 vests the power to authorise interception directions in a judge designated for that purpose, who sits outside the ordinary judicial hierarchy specifically to perform this function, giving that jurisdiction both judicial approval and, through parliamentary reporting obligations, a measure of legislative accountability. The United Kingdom's post-*Big Brother Watch* architecture, under the Investigatory Powers Act 2016, employs a 'double-lock': a warrant is issued by the Secretary of State but must additionally be approved by a Judicial Commissioner, drawn from serving or former holders of high judicial office, applying judicial review principles to the necessity and proportionality of the warrant before it takes effect.⁴⁸

What unites these three models, despite their considerable differences, is that in each the body performing the safeguard function is institutionally distinct from the executive department whose surveillance activity it reviews, is appointed through a process that does not run solely through that department, and possesses either the power to prevent an unlawful interception before it occurs or a standing, resourced mandate to detect and correct one promptly after. None of these features is present in India's Review Committee. India need not adopt any one of these models wholesale. Part VII proposes a design suited to India's constitutional structure but the comparative survey confirms that independence from the executive, in some institutional form, is the international norm rather than an exceptional demand.

VII. A Concrete Institutional Redesign

The deficiencies identified above are not incurable by judicial interpretation alone; they call

⁴⁷Justice B N Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report, Ministry of Electronics and Information Technology, 2018), noting comparative models in Germany, the United Kingdom, and South Africa.

⁴⁸Information Law & Policy Centre, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber Judgment' (Information Law & Policy Centre, 28 May 2021), describing the Investigatory Powers Commissioner's Office and the role of Judicial Commissioners.

for legislative and regulatory redesign. This paper proposes a five-element reform, capable of being implemented by amendment to section 20 of the Telecommunications Act, 2023 and to rules 5 and 7 of the 2024 Rules, without requiring wholesale reconstruction of the interception framework.

1. An independent Communications Oversight Board. Rule 5's Review Committee should be replaced by a statutory Communications Oversight Board, chaired by a retired Judge of the Supreme Court or of a High Court, appointed by a committee comprising the Chief Justice of India or a nominee Judge, the Union Home Minister, and the Leader of the Opposition in the Lok Sabha, a composition modelled on existing Indian appointment mechanisms for constitutional and quasi-constitutional bodies, adapted to insulate the appointment from unilateral executive control. The Board should further include one member with technical expertise in telecommunications and cybersecurity, and one member drawn from outside government service, nominated through a transparent public process. Serving civil servants should be excluded from membership altogether; a security-liaison officer may attend sittings to provide operational context but should not vote.

2. Ex-ante concurrence for non-emergency orders. For interception orders issued otherwise than under the 'unavoidable circumstances' exception, the competent authority's order should require the concurrence of at least one member of the Board, sitting individually if necessary to preserve speed, before the order takes effect, mirroring the double-lock adopted in the United Kingdom, and answering directly to the Grand Chamber's requirement in *Big Brother Watch* that independent authorisation occur 'at the outset' rather than only in retrospect. For orders issued under the emergency exception, the existing seventy-two-hour and seven-day confirmation timelines should be retained, but the confirmation itself should run to the Board rather than solely to the competent authority, converting today's single-layer executive confirmation into a genuine second check.

3. Binding ex-post review with real powers. Whether or not ex-ante concurrence was obtained, the Board should conduct a substantive ex-post review of every interception order within a fixed period, with the power already nominally present in rule 7, but exercised by the wrong body to set aside a non-compliant order, direct destruction of intercepted material, and additionally to direct that the affected individual be notified once the underlying investigation or operational necessity has concluded, subject only to a further, time-bound extension of

secrecy where the Board is itself satisfied that notification would compromise an ongoing operation. This restores an adversarial or quasi-adversarial dimension to the safeguard that rule 7, as it stands, entirely lacks.

4. Structural capacity commensurate with volume. Reflecting the Srikrishna Committee's finding on caseload, the Board should sit in benches, be permitted to delegate preliminary scrutiny to a secretariat of legally and technically qualified staff, and report publicly, at least annually, on the volume of orders reviewed, the proportion set aside, and the average time to review, without disclosing operational particulars that would compromise security. Parliament's Standing Committee on Communications and Information Technology should receive an unredacted version of that report in closed session, restoring the legislative-oversight dimension that the Standing Committee itself recommended in 2021 and that the 2024 Rules did not adopt.

5. Alignment with the data-protection framework. Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, due to commence on 13 May 2027, should itself be drafted, or any notification issued under it framed, so that any exemption granted to interception-related processing is expressly conditioned upon the existence and functioning of the Communications Oversight Board proposed above, giving the Data Protection Board of India a residual jurisdiction to examine systemic non-compliance even where individual interception decisions remain outside its day-to-day purview.

This design does not require India to adopt judicial pre-authorisation for every interception order, a step some commentators favour but which risks either overwhelming the ordinary judiciary or creating a specialised surveillance court whose own independence would then require separate safeguarding.⁴⁹ Nor does it dispense with executive competence in matters of national security, which the Board's technical and security-liaison arrangements are designed to preserve. What it does is convert a nominal safeguard of executive officers reviewing fellow executive officers, on paper, twice a year, over tens of thousands of orders into a safeguard that is structurally capable of performing the function the Constitution, on the Supreme Court's own articulation of the fifth prong, requires it to perform.

⁴⁹Big Brother Watch and Others v United Kingdom App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) [351], confirming that judicial authorisation, while best practice, is not indispensable provided the authorising body is genuinely independent of the executive.

VIII. Conclusion

The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 modernised the language of India's interception law without modernising its institutions. The Review Committee constituted under rule 5 is unchanged in substance since 1951, and left untouched by the 2025 amendment remained a body of executive officers reviewing the orders of fellow executive officers, sitting bi-monthly over a caseload the Government's own 2018 expert committee described as unmanageable, without power to hear the affected individual, and without any obligation to publish its findings absent litigation. Tested against the Supreme Court's fifth prong of proportionality, the requirement of sufficient safeguards against abuse, read into *Puttaswamy* by *Gujarat Mazdoor Sabha* and named by *Ramesh Chandra Sharma* and against the European Court of Human Rights' requirement in *Big Brother Watch* of authorisation by a body independent of the executive, the Review Committee fails on every measure that matters: independence, timing, capacity, and accountability. The Chhattisgarh High Court's 2026 decision in *Shri Ravi Shankar Ji Maharaj* shows what this failure looks like in practice is a defect that the Review Committee's own proceedings did not catch, and that only a court, applying an entirely different institutional logic, was able to correct.

The remedy is not to abandon executive judgment in matters of national security, a domain in which courts and legislatures alike must accord genuine deference. It is to ensure that the safeguard interposed between that judgment and the citizen's constitutional right to privacy is one capable of functioning as a safeguard at all. A Communications Oversight Board of the kind proposed in Part VII, independent in appointment, empowered to concur before interception where operational urgency permits, and possessed of a real ex-post remedial power would bring India's interception law into alignment with both its own constitutional doctrine and the comparative practice of the democracies it has long claimed to emulate. Until such a body exists, the Rules will continue to ask the executive to watch itself, and the Constitution's fifth prong of proportionality will remain, in this one but consequential field, unsatisfied.