Date: 27 September, 2024

To:
Shri Devendra Kumar Rai,
Joint Secretary (Telecom),
Department of Telecommunications,
Ministry of Communications,
Government of India

Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110001
jst-dot@gov.in

Access Now's Suggestions on the Draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024

We thank the Department of Telecommunications ("DoT") for the opportunity to submit suggestions with respect to the draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 ("the Rules") under the Telecommunications Act, 2023 ("the Act"). We welcome this initiative to update the existing procedure for surveillance of telecommunications in Rule 419A of the Indian Telegraph Rules, 1951 ("Rule 419A").

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence and expertise based in over 20 countries across six continents, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.

Access Now engages with a global community of individuals from over 162 countries in our annual RightsCon summit series, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We have special consultative status at the United Nations.[1]

In India and globally, Access Now has consistently engaged with stakeholders including governments and regulatory authorities on matters pertaining to digital rights,[2] including

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, *No liberty, no safety: Sri Lanka must withdraw the Online Safety Bill*, https://www.accessnow.org/press-release/sri-lanka-must-withdraw-the-online-safety-bill/.

data protection,[3] cybersecurity,[4] content governance,[5] internet shutdowns,[6] surveillance and digital security.

The need to update surveillance law in India

There has been a pressing need to update the framework for surveillance and interception in India for many years. Privacy of communications affects an overwhelming majority of people in India as the "overall tele density (number of telephones per 100 population) in India increased from 75.2 per cent in March 2014 to 85.7 per cent in March 2024."[7] The leading judgement examining the government's telephone tapping powers under Section 5(2) of the Indian Telegraph Act, 1885 (Section 5(2)) — *PUCL v. Union of India* — was delivered in December 1996.[8] The Supreme Court saved the provision only by reading in safeguards which were later incorporated into the Telegraph Rules as Rule 419A. The Supreme Court's assertion of the right to privacy in *PUCL* and other cases was reaffirmed and expanded by a Constitution Bench of the same court in the landmark judgement of *Puttaswamy* (2017).[9] *Puttaswamy* and subsequent pronouncements on the right to privacy have given rise to a need to reform and review surveillance in India, to ensure that any restrictions on the right to privacy satisfy the proportionality standard under the law as it now stands.

General recommendations

Even in 1996, the Supreme Court in *PUCL* had no doubt that it was important to protect people's privacy from abuse of surveillance powers. At that time there were no procedural

---

[3] Access Now, *Joint submission on the Bangladesh Draft Data Protection Act 2023,* https://www.accessnow.org/wp-content/uploads/2023/10/Submission-on-the-Bangladesh-Data-Protection-Act-2023-Access-Now-and-Tech-Global-Institute.pdf.

[4] Access Now, *Discussion Paper on International Cybersecurity Norms* for the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, https://www.accessnow.org/to-keep-us-safe-global-cybersecurity-norms-must-be-human-centered-and-protect-rights/.

[5] Access Now, *Submission on the draft Broadcasting Services (Regulation) Bill, 2023,* https://www.accessnow.org/wp-content/uploads/2024/01/Access-Now-Submission_Broadcasting-Services-Bill_January-2024.pdf.

[6] Access Now, *Shrinking democracy, growing violence: Internet shutdowns in 2023*, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf.

[7] Ministry of Finance, *India's Services Landscape Witnesses Rapid Technology Driven Transformation in Domestic Services Delivery and Diversification of Exports,* https://pib.gov.in/PressReleasePage.aspx?PRID=2034919.

[8] *People's Union for Civil Liberties (PUCL) v. The Union of India & Anr.* (1997) 1 SCC 301, available at https://main.sci.gov.in/judgment/judis/14584.pdf.

[9] *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* (2017) 10 SCC 1, available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

safeguards against the misuse of Section 5(2), a colonial-era provision meant for the imperial government to surveil and control its subjects. Such a provision has no place in a modern democratic state founded on progressive principles like universal adult franchise and a representative and accountable government, and which recognizes the right to privacy as a fundamental right under the Constitution. It is therefore essential to undertake a comprehensive reform of the surveillance framework in India, understand its impact on the lives of people, and put in place stronger institutional safeguards to respect people's rights as we understand them today.

International standards

India is committed to protecting the right to privacy under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. To help states fulfil these commitments, in December 2022 the United Nations General Assembly unanimously adopted a resolution on "The right to privacy in the digital age" urging member states to adopt a range of practical measures to protect and improve people's privacy particularly with respect to surveillance.[10]

Specifically, the resolution calls upon all states to:

- Regularly review their "procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data … with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;" (paragraph 7(d));
- Establish "independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;" (paragraph 7(e)); and
- Provide "individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations;" (paragraph 7(f)).

At present, there is no regularly scheduled mandatory review of the surveillance framework in India. The existing mechanisms for review of state surveillance have not been shown to be adequately independent, effective, or impartial, and there is no transparency

[10] United Nations General Assembly, *The right to privacy in the digital age* A/RES/77/211, https://documents.un.org/doc/undoc/gen/n22/762/14/pdf/n2276214.pdf.

of these proceedings and limited accountability for unlawful surveillance. There is also no established legal remedy for any person whose right to privacy has been violated by unlawful interception as there is rarely sufficient material to support a cause of action in a court of law, nor is there any statutory right to seek remedy.

Prior judicial sanction

Prior judicial approval of an interception order is one of the most essential, achievable ways to balance the requirements of investigation and public safety with individual privacy. In *PUCL*, the Supreme Court refrained from imposing an obligation to obtain prior judicial sanction in the form of a warrant for telephone tapping. The Court recorded that alternative measures were available based on the United Kingdom's *Interception of Communications Act 1985*.[11] It is therefore pertinent to note that the law in the UK has progressed significantly since then. The said Act was repealed and replaced by the *Regulation of Investigatory Powers Act 2000* and since then the UK has also enacted the *Investigatory Powers Act 2016* to provide further safeguards for privacy. These safeguards include the introduction of prior judicial approval for the issuance of a warrant for interception. To this end, we recommend the inclusion of a procedure for prior judicial sanction for interception in the Act along with a direct right of remedy or complaint to the high courts or other independent judicial mechanism.

Legislative oversight

Parliamentary processes provide an important check on the executive's exercise of powers. We recommend regular reporting by the competent authority to Parliament and the State Legislatures, which can constitute committees to monitor and evaluate the use of interception powers, their usefulness and efficiency, and their effect on personal liberty, privacy and freedom of speech. The present rules should also be laid before Parliament in keeping with the requirements of the Act.

We recommend that Section 56(3) of the Act be strictly followed and any rules be laid before each House of Parliament for thirty days so that Members of Parliament have the opportunity to debate and discuss the rules and make any modifications required.

Legal remedies

[11] *People's Union for Civil Liberties (PUCL) v. The Union of India & Anr.* at page 15, available at https://main.sci.gov.in/judgment/judis/14584.pdf.

Although privacy was recognised as a fundamental right under the Constitution in 2017 and has been recognised as an important human right in international law, people in India remain relatively powerless when their privacy is violated through unlawful surveillance or interception because of the absence of clear legal remedies. Without consequences and compensation for violations of privacy enshrined in a statute, the right to privacy is not actionable and remains an illusion.

We recommend that the Rules include a direct right of remedy or complaint to the High Courts or other independent judicial mechanism.

Maintaining and strengthening online privacy and security

In our digital world, end-to-end encrypted services enable people to actually exercise their rights to privacy and free speech, and to remain safe online and offline.[12] The Rules must clearly prohibit the application of interception orders to services offering end-to-end encryption, in recognition of the fact that it is not technically feasible for them to enable interception in any manner without ceasing to provide end-to-end encryption.[13] This is explained in Access Now's publication 'Encryption - Frequently Asked Questions':[14]

> "Since the provider of an E2EE system does not have decryption keys for the exchanged content by design, the provider can't access this content even if it wants to, or is compelled to. This also means that if malicious actors hack an E2EE platform's systems, the hackers can't get access to the content of the messages, either. This information simply does not exist in decrypted form on the servers."

Any application of the interception rules which might require service providers to create a systemic vulnerability, weakness, or backdoor of any sort would hurt privacy and cause damage to individuals, governments, businesses and institutions, and negatively impact the country's cybersecurity.[15] Section 20(2)(a) of the Act, which authorises the making of

---

[12] Access Now, *Why encryption is important: 10 facts to counter the myths*, https://www.accessnow.org/why-encryption-is-important/.
[13] Access Now, *Who we hurt when we attack encryption*, https://www.accessnow.org/who-we-hurt-when-we-attack-encryption/.
[14] Access Now, *Encryption FAQ: encrypted messaging, AI, content moderation, and more*, https://www.accessnow.org/encryption-faq/.
[15] Namrata Maheshwari, Greg Nojeim, *Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth*, 17 Indian J. L. & Tech. 1 (2021); George Robert Barker, William Lehr, Mark Loney and Douglas Sicker, *The Economic Impact of Laws that Weaken Encryption*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866902.

these rules, provides that the authority issuing an order may direct the disclosure of messages or a class of messages "in intelligible format." This provision should not be misused against services which provide end-to-end encryption, the strongest online security tool available today.

We recommend that the Rules explicitly prohibit the use of interception or other government powers to mandate that end-to-end encrypted services develop an ability to access and disclose data in a plaintext format, or to mandate any technological change that would amount to a systemic vulnerability, weakness or workaround.

Rule-wise suggestions

1. **Scope of the Rules and the Act — Rule 2(g): must be limited to the scope of the Telecommunications Act, 2023 and the ambit of the Department of Telecommunications.**

When Parliament passed the Act in December 2023, the Hon'ble Minister of Telecommunications at that time assured Parliament and the people of India that internet-based communication services, popularly referred to as "Over-The-Top" or "OTT" communication services, were not within the ambit of the Act.[16] The DoT also affirmed this position in January 2024.[17] This position is in line with international standards and recommendations, and furthers the interests of people in India by enabling their access to multiple modes of safe and secure communication for individual and business needs.[18]

Despite this clarity and consistency from the Government in favour of better access to services for people, telecommunication service providers continue to claim that OTT communication services should be included within the scope of the Act, raising concerns that this issue may be reopened and that the impact of the Act may be far beyond what

[16] Economic Times, *OTT not under ambit of Telecom Bill: Ashwini Vaishnaw*, https://economictimes.indiatimes.com/industry/telecom/telecom-news/ott-not-under-ambit-of-telecom-bill-ashwini-vaishnaw/articleshow/106224226.cms.
[17] Medianama, *Conscious decision to indicate that OTTs are excluded from the telecom act: DoT*, https://www.medianama.com/2024/01/223-dot-conscious-decision-ott-exclusion-telecom-act/.
[18] Access Now, *Submission on the TRAI Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*, https://www.accessnow.org/wp-content/uploads/2023/09/Submission-on-TRAI-Consultation-Paper_Access-Now_Sep-2023.pdf; Access Now, *Submission of Counter-Comments on the TRAI Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services* https://www.accessnow.org/wp-content/uploads/2023/09/Counter-Comments-on-TRAI-Consultation-Paper_Access-Now_Sep-2023.pdf.

Parliament was made aware of at the time when it approved the Act.[19] Such speculation must be ended for the sake of regulatory certainty and clarity and in favour of promoting free, secure speech.

We recommend that Department of Telecommunications (including in its role in coordinating the Digital Communications Commission) and the Telecom Regulatory Authority of India (TRAI) reaffirm that the scope and impact of the Act excludes OTT communication services, and if necessary, an amendment to the text of the Act may be introduced so that the legislative intent is unambiguous.

2. **Authorised agencies — Rule 3(1): Authorisation of agencies should be done after Parliamentary scrutiny and not left to be notified.**

Any law enforcement or security agency which is authorised to intercept communications should have been specifically named by Parliament in the text of the Act, rather than left to the executive. People's representatives in Parliament must have the opportunity to debate and determine how many authorities may be permitted to wield these extraordinary powers, the need to authorise an agency, and the reasons for which an agency has been chosen. Parliamentary committees should have the power to inquire into the use of interception powers by agencies and their adherence to the law. For example, an agency which has been found to have misused its emergency interception powers by issuing unnecessary and unjustified orders should not be re-authorised. Leaving the agencies to be notified without any oversight from Parliament or opportunity for feedback from the public eliminates a crucial pre-interception check and balance.

We recommend that the Act be amended with a schedule to include the names of agencies who may intercept communications, and until such amendment is made, that Rule 3(1) specify the names of the agencies.

3. **Ordering interception — Rule 3(2): Prior judicial sanction should be required for any interception order.**

The most practical way to ensure independent oversight and prevent abuse of powers is by instituting a pre-interception check and requiring a court order, or warrant, before any individual's privacy is infringed. In making an application to a court, the competent

[19] Indian Express, *OTTs under Telecom Act: Despite govt's denial, telcos have a different view*, https://indianexpress.com/article/business/ott-telecom-act-centre-9525168/.

authority must provide the following information and the court must consider the case in light of the principle of proportionality among other conditions for infringement of fundamental rights.

The application should state:

(1) The facts of the case,
(2) The period of time, in hours, for which interception is sought,
(3) The objective of issuing the order, that is, the nature of communications sought to be intercepted, which must be lawful,
(4) The ground(s) under Section 20(2) which are being invoked, which must be connected with the facts set out and the objective,
(5) The reasons why the objective could not be secured through any other less intrusive means, demonstrating that other means have been considered, and
(6) Whether previous interception orders have been issued in respect of the same individual or the same facts, and if so, the extent and validity of such orders, and the justification for further interception in this regard.

We recommend that rule 3(2) be subject to an application made by the competent authority to the High Court of Delhi in the case of the Central Government and the High Court of the state in the case of a State Government and an affirmative order permitting interception by such court.

4. Emergent cases — Rule 3: The exercise of emergency interception powers must be limited by stricter safeguards and narrow reading of the Rule.

4.1. Grounds for issuing an emergency order — Rule 3(3): Grounds must be narrow.

In Rule 419A, an emergency order could be issued in "emergent cases" in (1) remote areas, or (2) for operational reasons, where in either situation it was not feasible to obtain prior directions of the competent authority. Rule 3(3) has rearranged this to read "in emergent cases, in remote areas, or for operational reasons, where it is not feasible for the competent authority … to issue an interception order". This must be read as requiring "emergent" circumstances to be present in either (i) a remote area or (ii) a case where operational reasons exist for infeasibility of prior permission. Additionally, guidelines must be laid down to determine what constitutes an "emergent" circumstance. Without clarity

as to the nature of circumstances, orders are liable to be passed in a range of scenarios on the basis of a subjective understanding of an emergency.

We recommend that Rule 3(3) be clarified to ensure that "emergent" circumstances are a requirement for any order passed under it and to specify exhaustively what constitutes an emergent circumstance.

4.2. Timeline of orders in emergent cases — Rule 3(5): The Review Committee must consider an order issued under Rule 3(3) within seven days of issuance of the order.

As the rule presently reads, emergency orders are submitted to the relevant review committee only within seven days from the date of confirmation — which could be within seven days from the date of issuance of the order. Emergency orders not issued by the competent authority require stricter safeguards and should have a shorter timeline for operation rather than longer.

Illustration of the timeline under the proposed rules:

Order	Date of issuance of order	Date of confirmation by competent authority	Date of submission to the Committee
Under 3(2)	01.01.2024	N/A	By 09.01.2024
Under 3(3)	01.01.2024	By 09.01.2024	By 17.01.2024

We recommend that Rule 3(5) require that emergency orders be reviewed within seven (7) days of their issuance and not confirmation.

5. Contents of an interception order — Rule 3(8): More information is required to ensure lawfulness, transparency and accountability.

5.1. Limiting who can access intercepted information — Rule 3(8)(a).

The Rules omit a requirement included in Rule 419A to record the name and designation of the officer(s) to whom the intercepted messages shall be disclosed. Instead, Rule 3(8)(a) simply requires that the order specify the "agency that will undertake the interception". This appears to overlook a requirement mentioned in the Act itself since Section 20(2)(a)

provides that messages may be "disclosed in intelligible format to the officer mentioned in such order."

Intercepted information cannot be shared with any and all officers of an authorised agency, or all authorised agencies. It would constitute a grave violation of an individual's privacy if the law does not provide any limitation as to who can see the intercepted information, whether or not such information is actually shared.

The danger that the information will be used, directly or indirectly, for a purpose beyond the reason to be specified in Rule 3(8)(b) is magnified by such omission. The existence of an obligation to specify a reason under Rule 3(8)(b) implies that there is a need for an identifiable officer to have access to such information for an identifiable purpose.

The rules must make this explicit and retain the requirement for an interception order to include the name and designation of the officer to whom such messages shall be disclosed as was present in Rule 419A. Intercepted messages must be disclosed only to the named officer of an authorised agency; such officer must have a clear link to the reason for the order; and disclosure within the agency, beyond the specified officer or beyond the agency is prohibited and punishable.

We recommend that Rule 3(8)(a) require that an interception order must state the name and designation of the officer to whom such messages shall be disclosed; that such officer must have a clear link to the reason for the order; and that disclosure within the agency, beyond the specified officer or beyond the agency is prohibited and punishable.

5.2. Requiring greater specificity as to the reasons for which an order may be issued — Rule 3(8)(b).

In specifying the reasons for an order, the competent authority must not simply refer to one of the grounds for an order and assert it as a reason. This is insufficient to understand the reasons for the order and for its evaluation under the proportionality test.

We recommend that Rule 3(8)(b) require that the order must record:

(1) The facts of the case,
(2) The period of time, in hours, for which interception is sought,

(3) **The objective of issuing the order, that is, the nature of communications sought to be intercepted, which must be lawful,**
(4) **The ground(s) under Section 20(2) which are being invoked, which must be connected with the facts set out and the objective,**
(5) **The reasons why the objective could not be secured through any other less intrusive means, demonstrating that other means have been considered, and**
(6) **Whether previous interception orders have been issued in respect of the same individual or the same facts, and if so, the extent and validity of such orders, and the justification for further interception in this regard.**

6. Limiting the duration of an interception order — Rule 3(8)(c).

The Rules propose that an order may continue for 60 days and may be extended up to 180 days with no interim review. This is the same structure as was permitted by Rule 419A, reflecting no review of the standard in light of the principles of necessity and proportionality. This is an extremely long period of time during which an individual may meet and converse with multiple people and will likely engage in every normal activity of their life. An order of interception for such a long period is an inherently disproportionate violation of the right to privacy.

We recommend that Rule 3(8)(c) require that interception orders should be permitted to operate for only as long as they are necessary and required in terms of the facts of the case, and in no case should they be permitted to operate for longer than a maximum period to be specified in the Rules, after which they must lapse. There should be no option to extend an order and if further interception is sought, it must be applied for through a fresh process with reasons for the extension request.

7. Destruction of records — Rules 3(10) and 3(11): Records must be preserved for transparency and accountability.

It is not possible to have any review of the exercise of surveillance powers, and to prevent abuse, without examining interception orders and the relevant records. The problem of proper maintenance and keeping of records by the agencies was also noted by the Supreme Court in *PUCL*. The justification of the government that records must be destroyed in order to maintain "secrecy" and "confidentiality" does not take into account the requirements of review, accountability, and transparency.

The rules conflate confidentiality of the intercepted communications with confidentiality of the records relating to such interception. The former affects the privacy of an individual, but the latter protects only the government and the authorised agency from accountability for placing people under surveillance. In other words, keeping interception orders "confidential" and destroying them violates the right of the individual to know how and when their privacy has been invaded.

We recommend that the Rules must require that records pertaining to an interception order, not including the intercepted messages themselves, must be maintained in perpetuity.

8. Blanket exemption for demonstration and testing — Rule 3(12): There is no justification for this exemption.

Installation and demonstration of interception systems must be documented under the Rules in order to ensure that the systems are in fact lawful. Any testing of systems would involve interception which must not be carried out except by following the procedure under the Rules. There is no explanation as to what exactly constitutes "demonstration" or "testing", the permitted scope, time and so on, and no justification to exempt these activities from the requirement of being authorised by a lawful order from the competent authority, and being reviewed by the Review Committee. If retained, this could be misused to order interception and conduct surveillance without following the procedure required.

We recommend that Rule 3(12) be omitted.

9. Safeguards against unauthorised interception — Rule 4(4): Safeguards must be clear and must not obstruct scrutiny.

9.1. Internal safeguards must be clear and public — Rule 4(4)(b)

Without clearly laid out and publicised safeguards, there is no way to determine whether the obligation has been satisfied. **We recommend that the rules must specify at least the minimum "internal safeguards" which are implemented.**

9.2. Standard of confidentiality must be clear and have an exemption for necessary public disclosure — Rule 4(4)(c)

The rules omit the reference in Rule 419A to the privacy of citizens which is affected by the interception of messages. The provision requires that "confidentiality and secrecy" be maintained in the matter of interception. It may be noted that "confidentiality" and "secrecy" are vague and subjective terms, and are not specific conditions which can be tested. This is particularly important in light of the absence of any other provision in the rules for specifying who can access intercepted information (see our recommendation in paragraph 5.1 on Rule 3(8)(a) and the need to include the name of the officer who will have access to intercepted information).

Confidentiality to protect the privacy of an individual is necessary to make sure that intercepted messages are not disclosed to any person unauthorised by the specific interception order through which they have been obtained. Determining what is unauthorised access can be done only if there is a positive obligation to only disclose information to a specific person.

However, this confidentiality provision must not be a weapon to shield the state or agencies from scrutiny of their activities. The Rules must require disclosure of details of an interception order and its operation to the individual who is the subject of the interception order or any other individual whose communications have been intercepted by operation of the order, or to a court of law where an inquiry has been filed to test the legality and validity of an interception order or the exercise of powers under these rules. This provision must operate in tandem with preservation of records (see our recommendation in paragraph 7 on Rule 3(10) and Rule 3(11)).

We recommend that Rule 4(4)(c) permit access to interception orders and records to an individual whose communications have been intercepted by such order and to a court of law inquiring into the validity of such interception.

10. Means of communication of an interception order — Rule 4(5)

It is unclear why the Central Government would have to notify modes of communication of an interception order which could be an acceptable alternative to "in writing". Interception orders communicated in any mode other than "in writing" would imply that there would be no written record of such communication, which would hamper the ability of courts and individuals to examine the legality of any interception order and its operation.

To illustrate, without the details of the written communication by which an interception order was communicated by an authorised agency to the DoT or to a telecommunication entity such as the time at which the order was received, it is impossible to know whether interception commenced under authority of a valid order or not. Further, the absence of a written order makes it extremely onerous, if not practically impossible, for the order to be challenged and for any remedy to be sought.

In *PUCL*, the Supreme Court referred to the CBI's report on telephone tapping which noted that the telecom service provider, MTNL, could not provide records for the authorisation of interception, highlighting the need to ensure that written records are maintained by the telecommunication entity.[20]

We recommend that any mode of communication to be prescribed under Rule 4(5) must require a written record of the details of such communication, which is preserved and accessible for scrutiny.

11. Responsibility for violation of the rules — Rule 4(7): Penalties and their imposition must be clear and transparently applied.

The Rules omit the specific reference in Rule 419A to the penalties for violation of the rules or for permitting unauthorised interception, imposing a mandatory fine and suspension/ revocation of the license of the telecommunication authority.

Section 42(2)(b) of the Act under Chapter IX (Offences) prescribes that any person who "intercepts a message unlawfully" shall be punishable. There is no minimum fine or minimum term of imprisonment prescribed but either or both may be imposed. A fine may be a maximum of Rs.2 crores, and imprisonment may be up to three years.

It appears that there is no specific penalty or punishment prescribed for any other violation of the rules, such as not complying with the confidentiality requirements. Under the Act, a residual punishment is prescribed in the Third Schedule at serial number 4. There is no minimum fine prescribed for a violation. For a first offence, a violator may be fined up to Rs.25,000/-. This is a relatively low amount keeping in mind the gravity of the offence (violation of a fundamental right) and the relative position of the entity (a telecommunications service provider or network provider).

[20] *People's Union for Civil Liberties (PUCL) v. The Union of India & Anr.* at page 1-2, available at https://main.sci.gov.in/judgment/judis/14584.pdf.

We recommend that the Rules include clear penalties for contravention of the procedure for interception or unauthorised access to intercepted messages.

11.1. Responsibility of, and application of penalties to, the Department of Telecommunications, an authorised agency, or any other Government official for violation of the Rules.

Rule 4(7) applies only to the telecommunication entity and its employees or vendors. There is nothing in the Rules asserting that officials of the Department of Telecommunications, an authorised agency, or any other Government official involved in interception shall be punished for unlawful interception or other violation of the Rules. The Rules must contain a positive assertion to this effect so that there is no ambiguity in determining the consequences of unlawful interception. State officials ordering unlawful interception, or otherwise misusing their powers or violating rules, must be subject to the strictest punishment including a minimum penalty.

We recommend that the Rules specify that penalties will be applicable to the Department of Telecommunications, an authorised agency, or any other Government official for violation of the Rules.

12. The Review Committees and their functioning — Rule 5: Interception orders must be reviewed independently and transparently.

12.1. Composition — Rules 5(1) and 5(2): Committees must be independent.

The Rules reproduce the same structure of review committees at the central and state levels as were present in Rule 419A. There is no change to this structure despite the clear lack of independence of the Review Committee from the competent authority and the government ordering interception. Review of interception orders can only be done impartially by an office which is not directly controlled by the authorities issuing such an order.

Instead of a three-member Review Committee, interception orders issued by the Central Government should be reviewed by a single-member committee of a Judge of the High Court of Delhi, and orders issued by a State Government should be reviewed by a Judge of the High Court of that state.

We recommend that interception orders be reviewed by a single-member committee of a Judge of the High Court of Delhi, and orders issued by a State Government should be reviewed by a Judge of the High Court of that state, under Rule 5(1) and 5(2).

12.2. Powers, duties and functions of the Review Committees — Rule 5(3): Committees must be empowered to stop unlawful interception.

Independent Review Committees must be obligated and have binding authority to set aside any interception order which does violate either the Act, the Rules, or the Constitution. If an order is illegal, the Committee must also notify the subject of such an order and make available the records of the case, including the messages intercepted to the subject of such interception if they so choose, with necessary safeguards to prevent wide dissemination. This is essential for people to have a meaningful opportunity to seek legal remedies including compensation for the unlawful invasion of their privacy. Unless the Review Committee is empowered to stop unlawful interception and enable redressal for individuals whose privacy has been violated, there can be no accountability for any misuse or abuse of the Act. An interception order — whether issued through the emergency process or by the competent authority — must not be permitted to recur if it has been set aside by the Review Committee on any ground.

We recommend that Rule 5(3) empower Review Committees to set aside interception orders, notify the subject of such unlawful interception, make the records of the case available to the subject or to a court, and order compensation to be paid to the subject.

We recommend that an interception order must not be permitted to recur if it has been set aside by the Review Committee.

12.3. Procedure: Committee proceedings should be recorded.

Review Committee proceedings, including the deliberations and the final determination of the committee, should be recorded and records maintained in perpetuity. The records should be made available when requested, for example, to a court for judicial review, or in response to requests under the Right to Information Act, 2005.

We recommend that Review Committee proceedings be recorded and preserved.

12.4. Procedure: Committee meetings must be frequent.

Under Rule 419A the Review Committee was required to meet "at least" once every two months. Under the present rules, the obligation is lowered to meet only every two months. A meeting every two months is insufficient to meaningfully review all the interception orders and evaluate them on the basis of necessity and proportionality.

In 2011 the Central Government told Parliament that on average, it issued between 7,500 to 9,000 telephone interception orders every month.[21] The Review Committee would therefore have to examine between 15,000 to 18,000 orders in its meeting every two months which is impractical and likely to result in rubber-stamping of interception orders.

Infrequent meetings of the Review Committee also means that potentially unlawful interception may continue for up to two months until reviewed and set aside by the Committee. It is therefore essential that Committees meet at least every week to review orders on a timely basis and curb any unlawful interception.

We recommend that the Review Committee meet at least once a week to review interception orders.

Summary of all suggestions

S. No.	Rule/ Provision	Recommendation
1.	General recommendation	We recommend that Section 56(3) of the Act be strictly followed and any rules be laid before each House of Parliament for thirty days so that Members of Parliament have the opportunity to debate and discuss the rules and make any modifications required.
2.	General recommendation	We recommend that the Rules include a direct right of remedy or complaint to the High Courts or other independent judicial mechanism.

[21] Rajya Sabha, Starred Question No.292 answered on 16.03.2011, *Tapping of MPs Telephones,* https://sansad.in/getFile/annex/222/As292.pdf?source=pqars.

S. No.	Rule/ Provision	Recommendation
3.	General recommendation	We recommend that the Rules explicitly prohibit the use of interception or other government powers to mandate that end-to-end encrypted services develop an ability to access and disclose data in a plaintext format, or to mandate any technological change that would amount to a systemic vulnerability, weakness or workaround.
4.	General recommendation	We recommend that the Department of Telecommunications (including in its role in coordinating the Digital Communications Commission) and the Telecom Regulatory Authority of India reaffirm that the scope and impact of the Act excludes OTT communication services, and if necessary, that an amendment to the text of the Act may be introduced so that the legislative intent is unambiguous.
5.	General recommendation	We recommend that the Act be amended with a schedule to include the names of agencies who may intercept communications, and until such amendment is made, that Rule 3(1) specify the names of the agencies.
6.	Rule 3(2) - ordering interception.	We recommend that rule 3(2) be subject to an application made by the competent authority to the High Court of Delhi in the case of the Central Government and the High Court of the state in the case of a State Government and an affirmative order permitting interception by such court.
7.	Rule 3(3) - grounds for emergency orders.	We recommend that Rule 3(3) be clarified to ensure that “emergent” circumstances are a requirement for any order passed under it and to specify exhaustively what constitutes an emergent circumstance.
8.	Rule 3(5) - timeline for emergency orders.	We recommend that Rule 3(5) require that emergency orders be reviewed within seven (7) days of their issuance and not confirmation.

S. No.	Rule/ Provision	Recommendation
9.	Rule 3(8) - disclosure of intercepted messages.	We recommend that Rule 3(8)(a) require that an interception order must state the name and designation of the officer to whom such messages shall be disclosed; that such officer must have a clear link to the reason for the order; and that disclosure within the agency, beyond the specified officer or beyond the agency is prohibited and punishable.
10.	Rule 3(8)(b) - reasons for issuing an interception order.	We recommend that Rule 3(8)(b) require that the order must record: (1) The facts of the case, (2) The period of time, in hours, for which interception is sought, (3) The objective of issuing the order, that is, the nature of communications sought to be intercepted, which must be lawful, (4) The ground(s) under Section 20(2) which are being invoked, which must be connected with the facts set out and the objective, (5) The reasons why the objective could not be secured through any other less intrusive means, demonstrating that other means have been considered, and (6) Whether previous interception orders have been issued in respect of the same individual or the same facts, and if so, the extent and validity of such orders, and the justification for further interception in this regard.
11.	Rule 3(8)(c) - duration of an interception order.	We recommend that Rule 3(8)(c) require that interception orders should be permitted to operate for only as long as they are necessary and required in terms of the facts of the case, and in no case should they be permitted to operate for longer than a maximum period to be specified in the Rules, after which they must lapse. There should be no option to extend an order and if further interception is sought, it must be applied for through a fresh process with

S. No.	Rule/ Provision	Recommendation
		reasons for the extension request.
12.	Rules 3(10) and 3(11) - destruction of records.	We recommend that the Rules must require that records pertaining to an interception order, not including the intercepted messages themselves, must be maintained in perpetuity.
13.	Rule 3(12) - exemption for test.	We recommend that Rule 3(12) be omitted.
14.	Rule 4(4)(b) - internal safeguards.	We recommend that the rules must specify at least the minimum "internal safeguards" which are implemented.
15.	Rule 4(4)(c) - confidentiality of records.	We recommend that Rule 4(4)(c) permit access to interception orders and records to an individual whose communications have been intercepted by such order and to a court of law inquiring into the validity of such interception.
16.	Rule 4(5) - communication of an interception order.	We recommend that any mode of communication to be prescribed under Rule 4(5) must require a written record of the details of such communication, which is preserved and accessible for scrutiny.
17.	Rule 4(7) - penalties.	We recommend that the Rules include clear references to penalties for contravention of the procedure for interception or unauthorised access to intercepted messages.
18.	Rule 4(7) - penalties.	We recommend that the Rules specify that penalties will be applicable to the Department of Telecommunications, an authorised agency, or any other Government official for violation of the Rules.
19.	Rules 5(1) and 5(2) - Review Committee composition.	We recommend that interception orders be reviewed by a single-member committee of a Judge of the High Court of Delhi, and orders issued by a State Government should be reviewed by a Judge of the High Court of that state, under Rule 5(1) and 5(2).
20.	Rule 5(3) - Review	We recommend that Rule 5(3) empower Review

S. No.	Rule/ Provision	Recommendation
	Committee powers.	Committees to set aside interception orders, notify the subject of such unlawful interception, make the records of the case available to the subject or to a court, and order compensation to be paid to the subject.
21.	Rule 5(3) - Review Committee powers.	We recommend that an interception order must not be permitted to recur if it has been set aside by the Review Committee.
22.	Rule 5(3) - Review Committee procedure.	We recommend that Review Committee proceedings be recorded and preserved.
23.	Rule 5(3) - Review Committee procedure.	We recommend that the Review Committee meet at least once a week to review interception orders.

We thank you for the opportunity to participate in this consultation. We hope that the Ministry will undertake further public consultation after review of initial comments from all stakeholders, including through public meetings. We remain available for any clarification or queries in relation to this feedback, and any other further assistance.

Yours sincerely,

Namrata Maheshwari
Senior Policy Counsel and Encryption Policy Lead
namrata@accessnow.org

Shruti Narayan
Asia Pacific Policy Counsel
shruti@accessnow.org

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | **https://www.accessnow.org**