Rules and Regulations Review

2024 Draft Telecom Rules on Interception, Temporary Suspension of Services, and Cyber Security

G.S.R. 519(E), G.S.R. 520(E), and G.S.R. 522(E) issued on August 28, 2024 under the Telecommunications Act, 2023

Key Features of the Draft Rules

Procedure for Interception and Temporary Suspension of Services

- Home Secretaries of the central and state governments will have powers to issue orders.
- Committees will be constituted to review the orders. They will be headed by the Cabinet Secretary at the central level, and the Chief Secretary at the state level.
- Intercepted material as well as records pertaining to interception must be deleted every six months, unless required for functional purposes.

Cyber Security

- Telecom entities may be required to share traffic data and any other data for cyber security analysis by the government.
- Telecom entities will have certain obligations such as adopting a cyber security policy, appointing a Chief Telecom Security Officer, and carrying out cyber security audits.
- Identification number of a telecom equipment must be registered with the government.

Key Issues and Analysis

Interception

- The Review Committees consist solely of members from the Executive. This raises the question whether there is sufficient safeguard against misuse by the government.
- Deleting records pertaining to interception orders may lead to a lack of information for any subsequent judicial review, or parliamentary oversight of interception framework.

Temporary Suspension of Services

- The Draft Rules are similar to currently applicable Rules. State governments have issued multiple orders under existing Rules, which may violate the restrictions imposed under the Act. This raises question about the effective implementation of the Rules.
- The Draft Rules do not require publication of findings of Review Committees. This may be in contradiction with the directions of the Supreme Court.

Cyber Security

- Definition of traffic data may cover contents of calls, messages, or chats on instant messaging platforms. This could imply interception for cyber security purposes.

The Telecommunications Act, 2023 was passed by Parliament in December 2023.[1] It replaced the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933.[2] The 2023 Act regulates telecom networks and services in the country. The 2023 Act kept the existing Rules under the 1885 Act in effect. In August 2024, the Department of Telecommunications released Draft Rules under the 2023 Act for public feedback. These seek to replace the existing Rules on: (i) interception, (ii) temporary suspension of services, and (iii) tampering of mobile equipment identifiers.[3,4] They also introduce a framework for telecom cyber security.

Saket Surya
saket@prsindia.org

November 22, 2024

KEY FEATURES

Procedure for Interception and Temporary Suspension of Services

The Telecommunications Act, 2023 allows for communication to be intercepted, or services to be temporarily suspended on specified grounds. Such an action may be undertaken if it is: (i) on occurrence of public emergency or in the interest of public safety, and (ii) necessary or expedient in the interest of specified grounds such as security of the state and public order. The 2024 Draft Rules specify the procedure for these actions. For both interception and suspension of services, the same authorities are empowered to issue orders and review orders. The provisions are similar to the currently applicable Rules (see Table 1). The existing Rules were issued under the Indian Telegraph Act, 1885. While the 2023 Act repealed the 1885 Act, it kept the Rules under it in effect.

Table 1: Comparison of 2024 Draft Rules on Interception and Temporary Suspension of Services with Rules issued under the Indian Telegraph Act, 1885

Rules under the 1885 Act	2024 Draft Rules
The authority who can sanction interception or temporary suspension of services	
▪ Home Secretaries of the central government and state governments ▪ Where not feasible for Home Secretaries under unavoidable circumstances, officer of the rank of Joint Secretary to the central government or above authorised by them ▪ In certain cases of interception where it is not feasible for above authorities to issue orders, Head or the second senior most officer of specified law enforcement or security agencies; the order must be confirmed by the Home Secretary	▪ No change
Details to be specified in an order	
▪ **Interception:** (i) reasons for order, (ii) the authority who will undertake interception, and (iii) use of intercepted messages ▪ **Suspension of services**: reasons for order	▪ **Interception**: No change ▪ **Suspension:** to also include: (i) clearly defined geographical area(s), and (ii) duration
Review of orders	
▪ A committee to be constituted at both the central and state government level, to review the issued orders, and record its findings	▪ The Committees are also empowered to set aside orders
Composition of Review Committees	
▪ At the central level, the Committee will consist of: (i) Cabinet Secretary, (ii) Legal Affairs Secretary, and (iii) Telecom Secretary ▪ At the state level, the Committee will consist of: (i) Chief Secretary, (ii) Law Secretary, and (iii) Secretary other than the Home Secretary	▪ No change
Retention of data in cases of interception	
▪ Records pertaining to interception order and intercepted material must be destroyed every six months, unless required for functional purposes. This is applicable to the order issuing authority and the authority undertaking interception. ▪ The Department of Telecommunications and the telecom entity must delete records pertaining to interception within two months of discontinuance of the order.	▪ No change
Publication of suspension orders	
▪ No such provision	▪ Must be published

Sources: See endnotes 3 and 4; PRS.

Cyber Security

- **Data processing for cyber security:** The central government may require telecom entities to share traffic data and any other data for telecom cyber security. Traffic data has been defined as any data generated, transmitted, received, or stored in telecom networks, and includes type, routing, duration, or time of communication. If necessary for ensuring cyber security, data may be shared with: (i) government entities engaged in law enforcement and security related activities, (ii) other telecom entities, or (iii) users. Data must not be used or disclosed for any other purposes. The government may specify safeguards to prevent unauthorised access.
- **Obligations of telecom entities:** Telecom entities are required to: (i) adopt a cyber security policy which provides for security measures, risk management, and incident response, (ii) identify and address security risks, (iii) carry out periodic cyber security audits, (iv) appoint a Chief Telecommunication Security Officer to coordinate with the government, and (v) establish facilities to monitor and address cyber security incidents.
- **Reporting of security incidents:** A telecom entity must report a security incident to the central government within six hours of such occurrence. A security incident has been defined as an event having actual or

potential adverse effect on telecom cyber security. The government may inform public or direct the telecom entity to do so, if it determines that the disclosure is in public interest.

- **Management of telecom equipment:** A manufacturer or importer of a telecom equipment must register the identification number of the equipment with the government. The government may direct blocking of telecom equipment with tampered identification numbers. The government may suspend or terminate the use of an equipment identifier if it is used to endanger cyber security. This also applies to use for activities such as fraud, cheating, or impersonation. Before deciding such cases, the government must give notice, and also provide an opportunity to be heard.

KEY ISSUES AND ANALYSIS

A. Interception of Communication

Review of Interception Orders

Draft Rules: Rule 5

The Draft Rules constitute Review Committees at the central and state government level to examine interception orders. At the central level, the Committee will consist of: (i) Cabinet Secretary, (ii) Legal Affairs Secretary, and (iii) Telecom Secretary. At the state level, the Committee will consist of: (i) Chief Secretary, (ii) Law Secretary, and (iii) Secretary other than the Home Secretary. We discuss issues with these provisions below.

Need for independent oversight mechanism

The Committees consist solely of members from the Executive, and hence, are not independent of the government. This raises the question whether it is an appropriate safeguard against the actions of the Executive itself. This may go against the principle of separation of powers. In case of interception or monitoring of communication, due to the very nature of such orders, the affected person may never be aware. Hence, he cannot challenge such orders for potential illegality. Thus, it may be argued that in such cases, safeguards must be strict.

The composition of the Committees is in line with the directions of the Supreme Court in PUCL vs Union of India (1996).[5] The Court had then held that in the absence of a just and fair procedure to regulate interception, it is not possible to safeguard the fundamental right of freedom of speech and expression, and the right to privacy as part of the fundamental right to life and liberty.[5] Post this, the Supreme Court (2017) has held that the right to privacy is a fundamental right.[6]

The question whether prior judicial oversight may be necessary for interception was discussed in the PUCL judgement.[5] It was contended that only a prior judicial scrutiny could remove apprehension of arbitrariness or unreasonableness of the action.[5] The Court had observed that judicial scrutiny would have to be provided through the statute.[5] While recommending executive-led oversight, the Court referred to the legal framework in the United Kingdom.[5,7] Since then, a new law has been enacted in the United Kingdom which requires the approval of a Judicial Commissioner for such actions.[8] Similarly, in Australia, judicial authorisation is required.[9]

The volume of orders may be too high for Review Committees to effectively examine them

The Draft Rules require that Review Committees meet every two months to review orders. They must record their findings whether these orders are in accordance with the Act. They will also have powers to set aside orders. As per a response by the Ministry of Home Affairs to a 2014 RTI request, on average, the central government issues 7,500-9,000 interception orders every month.[10] The same Committees are responsible for reviewing orders for blocking of internet resources.[11] In 2022, the central government issued orders for blocking 6,775 URLs.[12] The members of the Review Committees are amongst the highest-ranking officials of respective governments. Such volume of orders may make it difficult for these Committees to apply their mind for detailed case-by-case scrutiny.

Retention of Intercepted Content and Related Information

Draft Rules: Rule 3 (10), 3 (11)

The Draft Rules provide that the order issuing authority and other authorised agencies must delete records pertaining to an interception order and intercepted messages every six months. Data should be deleted within the specified period if not required for functional purposes. Under the Rules, the Department of Telecommunications and the telecom entity will also have records pertaining to an interception order. They must delete the records within two months of the discontinuation of interception. We discuss issues with these provisions below.

Deleting records pertaining to interception orders may lead to a lack of information for further scrutiny

Deletion of intercepted content may be required to protect the privacy of the affected individual. However, the question is whether records pertaining to an interception order should also be deleted. They may cover information

such as reasons and durations of such actions. This could lead to a lack of information for any subsequent judicial review. It may also lead to a lack of data for oversight of the overall interception framework by Parliament. In PUCL vs Union of India (1996), the Supreme Court only required destroying copies of the intercepted material.[5]

Retaining intercepted content longer than necessary may contradict the Supreme Court directions

The Supreme Court (1996) had directed that each copy of the intercepted material must be deleted as soon as its retention is no longer necessary.[5] The Draft Rules instead provide for a retention period of six months regardless of whether such retention is necessary.

Confirmation of orders issued under unavoidable circumstances not required

Draft Interception Rules: Rule 3 (2), 3 (3)

Draft Suspension Rules: Rule 3 (1)

Under the Draft Rules, the Home Secretary of the central government and state governments will issue orders for interception. In certain cases, an officer of the rank of Joint Secretary to the central government or above, may issue orders. These would be instances where it is not feasible for the Home Secretary to issue an order. The Draft Rules on Suspension of Services treat such instances differently. They require that the Home Secretary must confirm such an order within 24 hours. Under the Draft Rules on Interception, confirmation is not required.

B. Temporary Suspension of Services

Certain orders issued under the existing Rules go beyond the permitted grounds

Draft Rules: Rule 3 (1)

The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017: Rule 2

The Draft Rules retain the existing framework for temporary suspension of services. Under the existing Rules, state governments have issued multiple orders which may go beyond the limits imposed under the Act and by Courts. For instance, state governments have ordered district-wide or state-wide internet shutdowns for conducting public examinations (Table 2). This raises the question about the effective implementation of the Rules.

Table 2: Some recent internet shutdowns for public exams across states

State	Occasion	Rationale	Services suspended	Area impacted	Duration
Jharkhand[13]	General Graduate Level Combined Competitive Examination-2023	To prevent cheating to eliminate any doubt in public mind regarding integrity of the recruitment process, which may lead to law and order issues and bear risks to public safety	Mobile Internet	Throughout the state	11 hours over two days in September 2024
Assam[14]	State-level recruitment examination for class-III posts	Similar to above	Mobile Internet	Throughout the state	3.5 hours in September 2024
West Bengal[15]	Teacher's Eligibility Test	To prevent incitement of offence relating to the use of unfair means and leakage of question papers, and to uphold general public interest	All types of Internet Services	Six districts	3 hours in December 2022
Rajasthan[16]	Rajasthan Eligibility Examination for Teachers	Multiple district-wise orders were issued; to prevent fake news and rumours about accidents and paper leaks, which may lead to law and order situation and bear risks to public order	Mobile Internet, Bulk SMS services	Six districts in Jaipur Division, Udaipur	10-12 hours in December 2021

Sources: Refer to endnotes marked in the 'State' column; PRS.

In case of internet shutdowns, the Supreme Court (2020) had observed that freedom of speech and expression, and freedom of trade and profession over internet are protected under the Constitution.[17] It noted that complete suspension of telecom services, internet or otherwise, is a drastic measure. It observed that: (i) such a measure must be proportionate to the situation concerned, (ii) it should be done only if necessary and unavoidable, and (iii) the State must assess the existence of an alternate less intrusive remedy.[17]

The Telecommunications Act, 2023 provides that services may be suspended on the occurrence of public emergency or in the interest of public safety.[1] Such an action must be necessary or expedient in the interest of specified grounds such as security of the state and public order. It may be argued that conduct of free and fair public examination does not meet the threshold of occurrence of public emergency or threat to public safety. The Supreme Court (2020) had observed that public emergency includes events which might involve 'widespread risk' of injury or harm to the public or destruction of property.[17]

To ensure that suspension is done as a last resort, the Parliamentary Standing Committee (2021) recommended: (i) codifying parameters on what constitutes as public emergency or public safety, (ii) creating a mechanism to assess the need for shutdown, and (iii) framing uniform guidelines for states.[18] It noted that in Bihar, government guidelines require: (i) shutdown to be considered as a last resort, (ii) minimising duration of shutdown, and (iii) exempting certain government internet-based services such as banking and railways.[18]

Review of Suspension Orders

Draft Rules: Rule 5

The Draft Rules constitute Review Committees to examine suspension orders. These Committees are the same as those for examining interception orders (see Table 1 on Page 2). We discuss issues with these provisions below.

Review Committees comprise solely of members from the Executive

As discussed earlier, the Committees consist solely of members of the Executive, and hence, are not independent. The Parliamentary Standing Committee (2021) had recommended including non-official members such as retired judges and eminent citizens in these Committees.[18] It noted that this will enable them to: (i) gauge the situation in the broadest possible perspective, and (ii) get a critical and objective assessment of the ground situation.[18]

Publication of the Review Committee findings is not required, this may contradict Supreme Court directions

The Supreme Court (2024) has observed that findings of the Review Committees on internet shutdowns must be published.[19] The Draft Rules do not require publication of the findings of the Review Committees.

Publication of Suspension Orders

Draft Rules: Rule 5

The Draft Rules require that suspension orders must be published. We discuss issues with these provisions below.

Manner of publication of suspension orders has not been specified, this is in contrast with various other laws

The Supreme Court (2020) held that all suspension orders must be made freely available through some suitable mechanism.[17] It observed that publishing an order empowers the aggrieved party to challenge it.[17] Making the orders widely known also helps people prepare for lack of connectivity (such as carrying enough cash as UPI will not work). The Draft Rules do not specify the manner of publication. This is different from certain Acts and Rules which provide for public notices. For instance, the 2013 Act on Land Acquisition requires that the district collector must publish notice on his website and convenient places on or near the land to be acquired.[20] The Companies Act, 2013 specifies that companies seeking registration must publish an advertisement in newspapers.[21]

Lack of provisions regarding publication of data on suspension of services

The Parliamentary Standing Committee (2021) had recommended that the central government should maintain a centralised database on suspension of services, and make it available publicly.[18] It noted that this will help in transparency and course correction in case of deviation from Rules, and will also help in gauging economic impact.[18] Draft Rules have not incorporated this recommendation.

C. Cyber Security

Definition of traffic data may include content of communication

Draft Rules: Rule 2 (1) (h)

The Draft Rules define traffic data to include data transmitted, received, or stored in telecommunication networks. As per the definition, traffic data includes data relating to type, routing, duration, or time of communication. If the term "including" in the definition is interpreted as illustrative, then other data transmitted over the network could also be termed as "traffic data". This could include: (i) contents of a call or message, and (ii) chats exchanged over internet-based instant messaging services. This implies that for cyber security, the government may require the interception of contents of communication. Under the Draft Rules on Interception, an order for interception of content will be subject to certain procedural safeguards. Such procedural safeguards are not applicable under the Draft Rules on Cyber Security.

In the European Union, the Directive on Privacy and Electronic Communications of 2002 defines traffic data as data processed for the purpose of conveyance of communication.[22] As per this Directive, traffic data consist of data referring to the routing, duration, time, volume of communication, or location of the equipment used.[22]

No limit on retention of traffic data processed for cyber security purposes

Draft Rules: Rule 3

Under the Draft Rules, the central government may collect and analyse traffic data for cyber security purposes. Traffic data could contain personal data such as IP addresses to identify the origin and the destination of traffic. For processing of personal data, the Digital Personal Data Protection Act, 2023 provides that data must be deleted once the purpose of processing is met.[23] In contrast, the Rules do not specify any limit on the retention of traffic data. This is different from: (i) Rules on interception which requires deletion of intercepted messages after six months, and (ii) telecom licences which require deletion of call detail records after two years.[24]

Procedure for suspension or termination of use of equipment identifiers

If an equipment is used to endanger telecom cyber security, the Draft Rules specify the procedure for suspending or terminating use of the telecom equipment identifier. This will prohibit that equipment from connecting to the

network. The person using this equipment to endanger cyber security may also be barred from accessing telecom services for up to three years. We discuss issues with these provisions below.

Draft Rules: Rule 5

Act: Section 22, 28, 56 (2)(v), 56(2)(z), Third Schedule

Procedure different from other laws

Officers empowered to decide cases not specified: The Rules do not specify which officers will decide cases. This is different from IT Rules on Blocking of Internet Resources.[25] IT Rules set up a committee to examine blocking. This Committee consists of officers of the rank of Joint Secretary or above.[25]

No mechanism for appeal: The Rules do not provide for appeal against the decision of the government. Under IT Rules on Blocking, while there is no provision for appeal, all blocking directions are subject to scrutiny by a Review Committee. This is the same Review Committee as the one for interception. In several laws, appeals lie with an officer who is higher in the rank than the officer who decides cases.[26]

Penalties under the Draft Rules may go beyond the Act

The Draft Rules provide for: (i) suspension or termination of use of a telecom equipment identifier, and (ii) bar on a person to access services up to three years. These Rules have been framed under Section 22, which empowers the government to specify cyber security measures. The Act does not specify suspension or termination of services as a penalty for violating Section 22. Such penalties are specified in the third Schedule of the Act for violation of Section 28, which covers measures for protection of users. In contrast, IT Rules on blocking have been issued under Section 69A of the IT Act, which specifically empowers the government to block access.[25]

1. The Telecommunications Act, 2023.
2. The Indian Telegraph Act, 1885; The Indian Wireless Telegraphy Act, 1933.
3. Rule 419A, The Indian Telegraph Rules, 1951, The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, The Temporary Suspension of Telecom Services (Amendment) Rules, 2022, The Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017, The Prevention of Tampering of the Mobile Device Equipment Identification Number (Amendment) Rules, 2022, issued under the Indian Telegraph Act, 1885.
4. G.S.R. 519(E), G.S.R. 520(E), G.S.R. 522(E), The Gazette of India, Department of Telecommunications, August 28, 2024.
5. People's Union for Civil Liberties vs the Union of India, Supreme Court of India, December 18, 1996.
6. Justice K. S. Puttaswamy Vs. Union of India, Supreme Court, Writ Petition (Civil) 494 of 2012, August 24, 2017.
7. The Interception of Communications Act, 1985, United Kingdom.
8. Part-2: Lawful Interception of Communications, Investigatory Powers Act, 2016, United Kingdom.
9. The Telecommunications (Interception and Access) Act 1979, Australia, The Telecommunications Act, 1997, Australia.
10. No. II.20034/35/2014-IS.II/M, Ministry of Home Affairs, May 12, 2014.
11. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
12. Unstarred Question No. 1064, Lok Sabha, Ministry of Electronics and Information Technology, February 8, 2023.
13. Memo No. P.S.C./Inter.Cell – 02/2022-105, Department of Home, Prison, and Disaster Management, Government of Jharkhand, September 20, 2024, as reported by ANI.
14. Memo No. eCF No. 551356/6-A, Home and Political Affairs Department, Government of Assam, September 14, 2024.
15. Memo No. 1483 – I.S.S/2M-15/19, Home and Hill Affairs Department, Government of West Bengal, December 10, 2022.
16. F 19 () () RTI/2021/260, Office of the Divisional Commissioner, Jaipur Division, November 2, 2021; 2021/Udaipur/3421, Office of the Divisional Commissioner, Udaipur Division, September 25, 2021.
17. Anuradha Bhasin vs the Union of India, Writ Petition (Civil) No. 1031 of 2019, Supreme Court of India, January 10, 2020.
18. "26th Report: Suspension of Telecom Services/Internet and Its Impact", Standing Committee on Communications and Information Technology, December 2021.
19. Foundation For Media Professionals vs Union Territory Of Jammu and Kashmir, Miscellaneous Application No. 1086/2020, Supreme Court of India, February 23, 2024.
20. Section 21, The Right to Fair Compensation and Transparency in Land Acquisition, Rehabilitation and Resettlement Act, 2013.
21. Section 307 and 374, The Companies Act, 2013.
22. Directive 2002/58/EC of the European Parliament, July 12, 2002.
23. Section 8 (7), The Digital Personal Data Protection Act, 2023.
24. No. 20-271/2010 AS-I (Vol.-III), Department of Telecommunications, December 21, 2021.
25. Rule 3,Rule 7, Rule 8, Rule 14, The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
26, The Jan Vishwas (Amendment of Provisions) Act, 2023.