Date: 23 July 2025

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 inputs on the June 2025 draft rules to amend the Telecommunications (Telecom Cyber Security) Rules, 2024

We are grateful for the opportunity to provide our suggestions and objections to the Department of Telecommunications (DoT) and the Ministry of Communications (the Ministry) on the draft rules to amend the Telecommunications (Telecom Cyber Security) Rules, 2024 under the Telecommunications Act, 2023 (the Act) as published in the Gazette of India on 24 June 2025.

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.[1]

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 helped found the Computer Incident Response Center for Civil Society (CiviCERT) network and are a member of the Forum for Incident Response (FIRST).[2] We have special consultative status

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] CiviCERT, *About CiviCERT*, https://www.civicert.org/about/; Forum for Incident Response, *Vision and Mission Statement*, https://www.first.org/about/mission.

at the United Nations.

In India and globally, Access Now has consistently engaged with stakeholders including governments and regulatory authorities on matters pertaining to digital rights,[3] including data protection,[4] cybersecurity,[5] content governance,[6] internet shutdowns,[7] surveillance and digital security.

Objections and suggestions on the draft amendments

Last year, we provided our expertise and suggestions to the DoT and the Ministry on the various draft rules published for consultation, including the Telecom Cyber Security Rules. Given that the DoT and the Ministry have indicated their willingness to amend those rules and the continued relevance of several of our previous recommendations on how to resolve the issues contained in original rules in addition to our concerns with the present draft amendments, we have attached an extract of those submissions as an annexure to this document.

We are concerned that the **overbroad definitions and scope** in the original text of the Telecom Cyber Security rules not only continues to be an issue - but that the current proposed amendments in fact widen the scope of the problem. This is **particularly so with regards the new definitional category of "telecommunication identifier user entity"** and proposed regulations. Given that the draft amendments themselves note that this proposed entity category "means a person, other than a licensee or authorised entity", it is clear that it is outside the scope of Section 3 of the Telecommunications Act 2023. Irrespective of the considerations of the DoT in proposing these measures, we respectfully submit that they are outside the legally permissible scope for rulemaking under the parent statute. **Clause 2(b) of the draft amendments**]

Additionally, key issues relating to **absence of sufficient safeguards required to govern**

[3] 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/.
[4] 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.
[5] 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/.
[6] 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.
[7] Access Now, *Shrinking democracy, growing violence: Internet shutdowns in 2023*, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf.

significant regulatory powers such as disconnection from telecom networks and access to data still remain unaddressed - and the proposed amendments propose to increase the scope of such powers, increasing the urgency in fixing these gaps. The amendments would allow the government to direct the suspension of the use of telecommunications identifiers, even without issuing notice - let alone requiring independent oversight and judicially required avenues for appeal, review, and remedy. Permanent disconnection of telecom identifiers has also been provided for without requiring clear notice and other safeguards. Additionally, the draft amendments would extend the existing problematic powers of the government to require disclosure of personal information and access to data impacting the privacy of individuals without sufficient safeguards [**Clauses 5(a), 5(b) and 5(c) of the draft amendments**].

We also remain **concerned that the DoT and Ministry have not acted on the statutory obligation to have table these rules before Parliament**, allowing MPs the opportunity to review and make any modifications which might be required. Indeed, the present amendments have been proposed right as Parliament has begun its 2025 Monsoon session - this provides an easy opportunity for the Ministry to satisfy the legal requirement and best practice of parliamentary review by tabling the Telecom Cyber Security rules and the other rules issued under the Telecom Act 2024 before MPs in both houses of parliament.

Conclusion

We thank you for the opportunity to provide our views. We hope that the Ministry will only issue further amendments to these already problematic rules after undertaking 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,

Raman Jit Singh Chima
Global Cybersecurity Lead
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org
Access Now | **https://www.accessnow.org**

ANNEXURE 1: Extract from 27 September 2024 Access Now suggestions on the Telecommunications (Telecom Cyber Security) Rules, 2024

Introduction

Strong, rights-respecting cyber security frameworks are essential to protect people's privacy. They affect every aspect of people's lives, from their interpersonal communications to financial security. We welcome the initiative to create a legal framework to guide cyber security practices in tandem with data protection measures which will ensure that people in India are better protected against cyber attacks and have access to secure and stable communications networks.

These draft Rules are being made under Section 22 of the Act entitled "Protection of telecommunication network and telecommunication services." The Act does not explicitly provide safeguards for people's privacy and freedom of expression, making it necessary to incorporate such provisions in the Rules. This approach aligns with the DoT's goal of protecting people's privacy as set out in the National Digital Communications Policy, 2018.[8] Certain key principles of necessity, proportionality, transparency, and accountability should be kept in mind to achieve the goals set out in the 2018 Policy, and ensure that cyber security policies are designed to address cyber threats without undue infringement of privacy and personal security.

The International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles") provide comprehensive guidance for ensuring that any rules affecting people's privacy of communications are balanced and rights-respecting.[9] The principle of proportionality is also well-recognised in Indian law as a multi-pronged test developed by the Supreme Court of India over successive judgements on fundamental rights. The principle was recognized notably by a seven-judge bench of the Court in *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* wherein the Court held that restrictions on fundamental rights must satisfy the proportionality principle.[10]

[8] Department of Telecommunication, *National Digital Communications Policy 2018,* https://dot.gov.in/sites/default/files/National%20Digital%20Communications%20Policy-2018.pdf?download=1.
[9] https://necessaryandproportionate.org/13-principles/
[10] Supreme Court of India, *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

Specific conditions for proportionality were enumerated by the Court in *Gujarat Mazdoor Sabha & Anr. v. State of Gujarat* as follows:[11]

> "9. … The principle of proportionality envisages an analysis of the following conditions in order to determine the validity of state action that could impinge on fundamental rights:
> (i) A law interfering with fundamental rights must be in pursuance of a legitimate state aim;
> (ii) The justification for rights-infringing measures that interfere with or limit the exercise of fundamental rights and liberties must be based on the existence of a *rational connection* between those measures, the situation in fact and the object sought to be achieved;
> (iii) The measures must be *necessary* to achieve the object and *must not infringe rights to an extent greater than is necessary* to fulfil the aim;
> (iv) Restrictions must not only serve legitimate purposes; they must also be *necessary* to protect them; and
> (v) The State should provide *sufficient safeguards* against the abuse of such interference."(Emphasis supplied.)

All measures notified or ordered under the Rules must be strictly limited to what is necessary and proportionate to "protect and ensure cyber security of telecommunication networks and telecommunication services" as prescribed in Section 22(1) of the Act.

Transparency, participation, and accountability are also key principles to be followed. People should have a clear understanding of the measures being put in place to monitor and restrict their communications. To this end, we welcome the present opportunity for public feedback by which the draft Rules have been published and are open for comments.

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.

Rule-wise comments

[11] Supreme Court of India, *Gujarat Mazdoor Sabha & Anr. v. State of Gujarat*, https://api.sci.gov.in/supremecourt/2020/11439/11439_2020_34_1501_24245_Judgement_01-Oct-2020.pdf.

1. Definition of cybersecurity — Rule 2(1)(c)

The rules currently define telecom cyber security as:

> "cyber security of telecommunication networks and telecommunication services" or "telecom cyber security" refers to tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services, as well as assets of persons, including connected telecommunication equipment, telecommunication services, personnel, infrastructure, applications, and the totality of transmitted and/or stored information, against relevant security risks in the cyber environment;"

Access Now supports an approach to cyber security policy which promotes human rights, including the protection of privacy and personal data, centres users and impacted individuals, and enables systemic change, anchored in pluralistic, democratic processes.[12] The contours of a human rights-based approach are explained here:

> "A human rights-based approach to cybersecurity means putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Such an approach is systematic, meaning that it addresses the technological, social and legal aspects together, and does not differentiate between national security interests and the security of the global internet."[13]

A human rights-aligned approach to cybersecurity in telecommunications would fit well in India's policy-making, which needs to take into account the impact of policies on multiple diverse stakeholders and their rights in a participatory democratic set-up.[14]

The Freedom Online Coalition (FOC), a partnership of 41 governments from around the world working to advance people's freedoms of free expression, association, assembly,

---

[12] Access Now, *Let's not trample upon human rights in the name of "cyber"*, https://www.accessnow.org/lets-not-trample-upon-human-rights-in-the-name-of-cyber/.
[13] Association for Progressive Communications, *A Human Rights-Based Approach to Cybersecurity*, https://www.apc.org/sites/default/files/APCExplainers_cybersecurity.pdf.
[14] See, Association for Progressive Communications, *Why cybersecurity is a human rights issue, and it is time to start treating it like one*, https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one.

and privacy online, has a similar human rights approach to internet standards and cyber security.[15] The FOC's Working Group 1 defines cyber security as:[16]

> "PREAMBLE: International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.
>
> DEFINITION: Cybersecurity is the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline."

The FOC's *Joint Statement on the Human Rights Impact of Cybersecurity Laws* is a useful reference to guide the formulation of rights-respecting cyber security policy.[17] The Statement declares that "human rights and cybersecurity are complementary, interdependent and mutually reinforcing, and that cybersecurity policies and practices should be rights respecting by design." The Statement recognizes the risks of States "asserting excessive control over the Internet under the pretence of ensuring national security while disregarding international human rights law." It also highlights that technology-driven risks to human rights are amplified when "governments seek to compel the suppliers of such technologies to cooperate with their security and intelligence agencies without any democratic or independent checks or balances on these authorities." The Statement warns that the creation of such opaque intelligence gathering capacities "threatens the principles of an open, free, secure, interoperable and reliable Internet, and the rule of law."

We recommend that the Rules include a specific reference to human rights under the Constitution of India as well as international human rights law, and affirm the approach to cybersecurity as based in protection and promotion of human rights online and offline, as also envisaged by the Freedom Online Coalition (FOC), a partnership of 41 governments from around the world.

---

[15] Freedom Online Coalition, https://freedomonlinecoalition.com/.
[16] Freedom Online Coalition, "
https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity/.
[17] Freedom Online Coalition, *Joint Statement on the Human Rights Impact of Cybersecurity Laws*, https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

2. Data collection and dissemination powers should be qualified and narrowed to protect privacy — Rule 3.

Rule 3 prescribes general, broad powers for data collection, processing, and dissemination by the Central Government.

At the outset, it may be noted that the Explanation to Section 22(2) exhaustively defines the "traffic data" which may be collected, analysed, or disseminated through rules made under Section 22(1). The same definition is reproduced in Rule 2(1)(h) of the Rules. Therefore it is clear that in Rule 3(1)(a) the phrase "traffic data and any other data" must be limited to traffic data, as defined in the Act, without inclusion of any other kind of data.

We recommend that the words "and any other data" be removed from Rule 3(1)(a) to avoid any ambiguity or misinterpretation requiring judicial intervention.

2.1. The scope of traffic data sought to be collected and used must be limited.

The term "traffic data" is very broad and requires limitation. Traffic data (sometimes called metadata) includes personal data which is protected by the Digital Personal Data Protection Act, 2023 (DPDPA). Traffic data also includes "protected information" which is defined as information that "includes, reflects, arises from, or is about a person's communications and that is not readily available and easily accessible to the general public."[18] The general distinction between "content" and "traffic" data is therefore insufficient to prevent unauthorised surveillance and collection of personal data.

The increase in telecommunications usage means that traffic data can now be used to not merely identify an individual but to "allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[19] The former head of the United States's

[18] International Principles on the Application of Human Rights to Communication Surveillance, https://necessaryandproportionate.org/principles/.
[19] Court of Justice of the European Union, *Digital Rights Ireland Ltd v. Minister for Communication, Marine and Natural Resources*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293.

National Security Agency once stated that the NSA takes decisions to kill people based on metadata.[20]

The subject of collecting telecommunications data, the effect on individual privacy, and the requirements of proportionality was noted by the Supreme Court in *Puttaswamy* (2018) wherein the Court referred with approval to the line of judgements in Europe applying the principle of proportionality to laws requiring data retention and use.[21]

Specifically, the Supreme Court referred to the judgement of the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland Ltd v. Minister for Communication, Marine and Natural Resources* which dealt with communications data and which was followed in several cases. There, the CJEU held that a provision requiring retention of traffic data for the general purpose of fighting "serious crime" was not valid and did not meet the proportionality standard because of the absence of:

> (i) limitation of data retention to a particular time period, particular geographical zone, and circle of particular persons — in other words, data related to a specific incident;
> (ii) prior review by a court or independent body of the request for access to data;
> (iii) distinction between categories of data collected based on their usefulness;
> (iv) limitation on how long the data could be retained; and
> (v) protection against risk of abuse and unlawful access.

India has incorporated many of the principles underlying data protection and privacy in Europe in the DPDPA, including:[22]

- The principle of consented, lawful and transparent use of personal data;
- The principle of purpose limitation;
- The principle of data minimisation (collection of only as much personal data as is necessary to serve the specified purpose);
- The principle of storage limitation (storing data only till it is needed for the specified purpose);
- The principle of reasonable security safeguards; and
- The principle of accountability.

---

[20] ABC News, "*Ex-NSA Chief: 'We Kill People Based on Metadata'*", https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata.
[21] Supreme Court of India, *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.
[22] Ministry of Electronics and Information Technology, *Salient Features of the Digital Personal Data Protection Bill, 2023*, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264.

In order to comply with the principles of proportionality and the requirements to protect personal data under the DPDPA, measures must be taken to avoid collecting large amounts of personal data, limiting collection requests to such data as is necessary in a specific instance, and ensuring transparency and accountability. For example, in the UK, communications service providers are required to erase or anonymise traffic data after it is no longer needed to prevent its misuse.[23]

Rule 3(1) provides that the Central Government may:

> (i) Notify the "form and manner" in which traffic data must be provided by telecommunication entities; and
> (ii) Direct telecommunication entities "to establish necessary infrastructure and equipment for collection and provision of such data from designated points to enable its processing and storage."

Without adequate safeguards, these provisions could permit creation of infrastructure and installation of equipment enabling mass surveillance. This amplifies concerns around the opacity, lack of accountability or proportionality, and centralisation of power in India's surveillance regime.[24] The Rules must clearly set out what kind of infrastructural changes can be mandated, the grounds that must be satisfied, the checks and balances in place to ensure that the power is not misused, the procedure for an entity to conduct an impact assessment of the requested changes and to submit and publish feedback, and the requirements of notifying the public at large, and facilitating multi-stakeholder consultations with experts and the public to ensure balance between security, innovation and privacy. It is essential that Rule 3(1) be limited not only by the purpose-limitation in Rule 3(4), but also by specific prohibitions against its misuse.

We recommend that clear limitations be incorporated in Rule 3(1) in respect of collection of traffic data. The type of traffic data collected and accessed, the specific purpose for access, the period for which it is being accessed, and the duration of its retention must be specified in a request for data by the Central Government and such a request must require prior judicial approval.

---

[23] Information Commissioner's Office, *Guide to Privacy and Electronic Communications Regulations*, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/communications-networks-and-services/traffic-data/.
[24] The Financial Times, *India's communications 'backdoor' attracts surveillance companies*, available at https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4.

2.2. Access to data collected must be limited.

Further, Rule 3(2) provides that the Central Government may be shared with:

(i) Any agency of the Central Government engaged in "law enforcement and security related activities";
(ii) Telecommunication entities; and
(iii) Users.

A broad permission to share communications data with any law enforcement agency or "related" agency is not justified by the limited purpose of "protecting and ensuring telecom cyber security." There are multiple law enforcement and security related agencies of the Central Government and a generalised data access provision could be easily misused by any party involved which would compromise the security of the data and people's privacy.

It is important not to conflate general law enforcement activities with cybersecurity-related enforcement. Cyber security, which has as its objective the assurance of availability, integrity, and confidentiality as defined by the ITU, must not be subsumed by the demands for information from law enforcement.[25] This would undermine the security objectives of cyber security policy.

A "security incident" is defined under the Rules as "an event having actual or potential adverse effect on telecom cyber security". The US's National Institute of Standards and Technology (NIST) defines a cyber incident as:

> "An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

Reading the definition of a "security incident" in the Rules in the context of the meaning of cyber security, it is clear that the focus of the Rules, and of cyber-focused incident response teams, should be on incident response and threat migration for the purpose of cyber security and not for general law enforcement. Communication with law enforcement

[25] International Telecommunications Union, *Definition of cybersecurity*, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

should be limited to a specific case where cross-communication is required for reasons to be provided in writing. The inclusion of a wide data access provision in the cyber security rules could otherwise be misused to bypass the requirements of seeking interception orders and violate the right to privacy.

We recommend that Rule 3 include an explicit prohibition on use of this data for surveillance or access to this data by law enforcement and provide that any exception to this prohibition must require judicial approval.

It is also unclear as to what is meant by the inclusion of "users" in this Rule. The broad reference to users does not clarify which users, the extent of data which will be shared with them, and when. Without clear and published guidance in the Rules, broad data-sharing provisions will result in over-sharing of data or sharing at an inappropriate time, which will also undermine the objective of promoting healthy cybersecurity practices.

We recommend that Rule 3 include clear guidance for sharing data with users, including which users, the time, type of data to be shared, and how such sharing will be recorded.

3. The Rules must not create broad obligations, in the nature of offences, applicable to individuals — Rule 4.

At the outset it may be noted that there appears to be a typographical error in the printing of Rule 4(3), which, as printed, reads that no person is permitted to use telecommunication services, identifiers, networks or equipment. This may require correction and re-printing for consultation.

The purpose of creating cyber security rules is to provide measures — technical and infrastructure-based — which would better protect people's safety. For example, the rules should provide guidance as to the development, updating, and maintenance of standards for device security, cloud security, and risk management, some of which are mentioned in Rule 4(5).[26] The inclusion of vague prohibitions against individual actions in Rule 4 is misplaced and ineffective towards combating serious cyber security risks. Reading Rule 4 and Rule 5 together, the Rules propose a mechanism to summarily deprive people of their right to use telecommunications networks through an opaque process controlled by the

[26] UK National Cyber Security Centre, *Information for large organisations* https://www.ncsc.gov.uk/section/information-for/large-organisations#section_2.

Central Government and based on vague and overbroad references to behaviour, which is not envisaged by the Act.

Rules 4(1), 4(2), 4(3), and 4(4) prescribe extremely broad obligations applicable not only to telecommunication entities and service providers but to all persons. With respect to all these four sub-rules, the language used is vague, making generalisations and references to acts which are not contemplated by the Act. The general prohibitions proposed in Rule 4 with respect to individuals do not appear to fit the mandate of the Rules, that is, to provide measures to protect cyber security.

It is important not to conflate cyber security with other undesirable uses of telecommunication networks, as they are not interchangeable and cyber security requires distinct attention and specific protections. It may be noted that Chapter IX of the Act deals with general contraventions of the Act exhaustively.

These parts of Rule 4 are briefly discussed below.

- Rule 4(1) is a general provision prohibiting any person from endangering telecom cyber security with no explanation as to what would constitute endangering. Given the broad meaning of telecom cyber security, this rule is capable of giving rise to multiple interpretations, creating uncertainty.

- Rule 4(2) prohibits the sending of any message which "adversely affects telecom cyber security." It is unclear as to how a message could affect telecom cyber security or what is contemplated by this rule. It is also unclear as to what is meant by the subjective term "adversely affects", and whether it denotes a lower or higher standard of harm than "endanger."

- Rule 4(3) as mentioned appears to contain a printing error, reading as a blanket prohibition of the use of telecom services. Assuming that it refers only to the listed activities, the rule is overbroad and beyond the scope of the Rules.

- Rule 4(3)(a) and Rule 4(3)(b) — It is unclear as to what is meant by using telecommunications networks "through fraud, cheating or personation" or by "transmitting any message which is fraudulent." The term "fraudulent" is used in law in conjunction with some other action. For e.g. Section 83 of the Bharatiya Nyaya Sanhita, 2023 makes it an offence to marry a person while being married to

some other person, “dishonestly or with a fraudulent intention”. Similarly, in the Act, Section 42(3)(e) prescribes that it is an offence to obtain subscriber identity modules through fraud, cheating or personation. Therefore, it is unclear as to how to identify a message which is simply “fraudulent” or use of a telecommunication network through “fraud” or “cheating”.

- Rule 4(3)(c) — The term “security incident” is not defined in the Act and is sought to be defined in Rule 2(1)(e) as “an event having actual or potential adverse effect on telecom cyber security.” As mentioned, “adverse effect” is a broad, subjective term which could give rise to multiple interpretations and a lack of clarity.

- Rule 4(3)(d) — This is a general prohibition against engaging in “any other use” which may be contrary to provisions of law. This is a very broad reference which is not required as if an act is prohibited by another law, that law is applicable regardless of this reference.

- Rule 4(4) — This rule gives a general power to the Central Government to “issue directions and standards” to prevent “misuse” of telecom services, networks, or identifiers, which shall be “binding on all persons on which it is applicable.” This appears to be a further delegation of power to the Central Government through the Rules to issue certain binding directions, which is not a permissible sub-delegation of power. The term “misuse” is also not in keeping with the purpose of the Rules which is to protect telecom cyber security and not generally regulate any “misuse” of a network which could be much broader.

Vagueness in policy-making is not desirable because of the uncertainty of application and the potential “chilling effect” it can have in the context of freedom of expression. In *Shreya Singhal v. Union of India*, the Supreme Court noted that offences should have “narrowly and closely defined contours”, and a provision which was “vague and overbroad” had to be struck down (which in that case was Section 66A of the Information Technology Act, 2000).[27]

We recommend that Rules 4(1), 4(2), 4(3), and 4(4) be omitted.

[27] Supreme Court of India, *Shreya Singhal v. Union of India*, https://indiankanoon.org/doc/110813550/.

4. The adjudication mechanism set up under Rule 5 violates fundamental rights, does not adhere to the principles of proportionality or natural justice, and is beyond the mandate of the Rules — Rule 5.

Through Rule 5, the Central Government is empowered to determine "based on its assessment of facts and submissions" whether a person has endangered telecom cyber security and to either temporarily or permanently suspend the telecom identifier of such person. Further, such person may be barred from accessing telecommunication services through any other identifier or other network or service provider, essentially being cut off entirely from accessing telecommunications.

Rule 5 therefore proposes up a quasi-judicial mechanism controlled by the Central Government and not contemplated anywhere in the Act to suspend or terminate any person's use of telecommunications, seriously infringing fundamental rights and the right to liberty, and in particular the right to freedom of speech and expression under Article 19(1)(a) and the right to practise any profession or carry on any occupation, trade or business under Article 19(1)(g) of the Constitution.

- It may be reiterated that the Act does not contemplate any action which "endangers" telecommunications through "any act", and this as well as the provisions in Rule 4(3) are a creation of the Rules and are not connected with telecom cyber security. The basis of Rule 5 is overbroad, vague, and cannot be sustained.

- The Central Government is singularly empowered to identify a person, conduct a "prima facie examination", and determine whether a person has "endangered telecom cyber security" without any independent inquiry or oversight.

- The procedure proposed in Rule 5 essentially permits suspension or termination of telecommunications connections on the basis of the Central Government's subjective satisfaction that it is "necessary or expedient in the public interest." Suspension or termination of a connection is a restriction on Article 19(1)(a) of the Constitution and must satisfy the proportionality test. It may be noted that "public interest" is not a permissible ground for reasonable restrictions under Article 19(2) of the Constitution and therefore cannot be a ground to restrict a person's use of a telecommunication identifier.

- Even where notice is proposed to be sent to the affected individual, seven days is an inadequate time for response and renders the procedure arbitrary and unjust.

- The proposals to permanently block an individual from accessing any telecommunication services in Rules 4(8), 4(9), and 4(10) — including by extending an order of suspension or termination of service to "other" connections or "equipment" and to prohibit other telecommunication service providers from offering services to a person against whom an order has been passed — are disproportionate. The Rule does not even require reasons for such an extreme measure which are a clear and permanent violation of fundamental rights.

It may be noted that the freedom to share and receive information is a fundamental right under Article 19(1)(a).[28] The right to access the internet is also a fundamental right deserving Constitutional protection, as declared in *Anuradha Bhasin v. Union of India & Ors.*[29] by the Supreme Court:

> "We declare that the freedom of speech and expression and the freedom to practice any profession or carry on any trade, business or occupation over the medium of internet enjoys constitutional protection under Article 19(1)(a) and Article 19(1)(g). The restriction upon such fundamental rights should be in consonance with the mandate under Article 19 (2) and (6) of the Constitution, inclusive of the test of proportionality."

We recommend that Rule 5 be omitted, and that any proposal to suspend or terminate an individual's access to telecommunications be proposed only through an amendment to the Act, and in consonance with the Constitution and the principle of proportionality.

5. Reporting of security incidents should be realistic, transparent, and involve affected individuals — Rule 7.

In Rule 7(1), it may be difficult for telecommunication entities to provide all the required information in 7(1)(a) - (f) within six hours which will discourage active compliance with

[28] Supreme Court of India, *Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal*, https://indiankanoon.org/doc/539407/.
[29] Supreme Court of India, *Anuradha Bhasin v. Union of India & Ors.*, https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf .

the Rule and undermine cyber security protections for all people across telecommunication services.

We recommend that entities be required to provide the information "without undue delay" and no later than seventy-two (72) hours from the time when they become aware of the incident.

Under Rule 7(2), the public — including individuals who are affected by a security incident — is not notified unless the Central Government determines there is a public interest in Rule 7(2). This undermines the right of people to safe and secure communications and their right of control over their personal data. Telecommunication entities have an obligation towards all people to be transparent about gaps in cyber security. This will also encourage and enable useful research and improvements in the field.

We recommend that the occurrence of a telecom cyber security incident must be made public, including to subscribers or users of such affected services, with a clear timeline.

Summary of suggestions

S. No.	Rule/ provision	Suggestion
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 specific reference to human rights under the Constitution of India as well as international human rights law, and affirm the approach to cybersecurity as based in protection and promotion of human rights online and offline, , as also envisaged by the Freedom Online Coalition (FOC), a partnership of 41 governments from around the world.
3.	Rule 3(1)(a) - data collection.	We recommend that the words "and any other data" be removed from Rule 3(1)(a) to avoid any ambiguity or misinterpretation requiring judicial

S. No.	Rule/ provision	Suggestion
		intervention.
4.	Rule 3(1) - data collection.	We recommend that clear limitations be incorporated in Rule 3(1) in respect of collection of traffic data. The type of traffic data collected and accessed, the specific purpose for access, the period for which it is being accessed, and the duration of its retention must be specified in a request for data by the Central Government and such a request must require prior judicial approval.
5.	Rule 3(2) - access to data collected.	We recommend that Rule 3 include an explicit prohibition on use of this data for surveillance or access to this data by law enforcement and provide that any exception to this prohibition must require judicial approval.
6.	Rule 3(2) - access to data collected.	We recommend that Rule 3 include clear guidance for sharing data with users, including which users, the time, type of data to be shared, and how such sharing will be recorded.
7.	Rule 4 - obligations.	We recommend that Rules 4(1), 4(2), 4(3), and 4(4) be omitted.
8.	Rule 5 - measures to protect and ensure telecom cyber security.	We recommend that Rule 5 be omitted, and that any proposal to suspend or terminate an individual's access to telecommunications be proposed only through an amendment to the Act, and in consonance with the Constitution and the principle of proportionality.
9.	Rule 7 - reporting of security incidents.	We recommend that entities be required to provide the information "without undue delay" and no later than seventy-two (72) hours from the time when they become aware of the incident.
10.	Rule 7 - reporting of security incidents.	We recommend that the occurrence of a telecom cyber security incident must be made public, including to subscribers or users of such affected services, with a clear timeline.