To,
Shri Neeraj Mittal
Secretary, Ministry of Communications
Government of India

10th October, 2025

In Re: Submission of Comments from Public on The *Telecommunications (User Identification) Rules, 2025.*

Respected Sir,

This letter is in reference to the circular issued by the Department of Telecommunications, Ministry of Communications, Government of India, inviting comments from the public on the Telecommunications (User Identification) Rules, 2025. In furtherance of our commitment to contributing to the legal, regulatory, and technological discourse in the country, and working for public welfare in the capacity of law students, the team at the Cell for Law and Technology ("CLT"), National Law Institute University, Bhopal, hereby submits its suggestions in response to the draft rules.

At the outset, we would like to express our appreciation for this progressive initiative aimed at strengthening the framework for user verification and identity management in the telecom sector. This consultative approach adopted by the Department of Telecommunications to seek stakeholder participation ensures that the proposed regulatory framework is transparent, inclusive, and effective in addressing concerns relating to misuse of telecom resources, privacy protection, and national security. As digital connectivity expands rapidly across India, the formulation of robust identification norms will be instrumental in fostering accountability, preventing fraud, and building public trust in the telecom ecosystem.

The proposed draft has been thoroughly analysed, and the CLT team has identified a number of key points for consideration, which we have compiled as detailed comments under each mission of the policy. We hope these submissions will contribute meaningfully to the ongoing discussions on creating a strong, secure, and transparent framework for user identification and verification within India's telecommunications ecosystem.

Thank you for your consideration.

Warm Regards,

Dr. Atul Kumar Pandey
(Professor of Cyber Law; Head, Department of Cyber Law; Faculty in Charge, Cell for Law and Technology)

The team which has been instrumental in putting forward this suggestion comprises of the following members of the Cell for Law and Technology, NLIU Bhopal:

1. Hansika Kumari (Joint Convener) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
2. Samrudhi Memane (Joint Convener) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
3. Raj Rajeshwari Meena (3rd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
4. Rujuta Bapat (3rd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
5. Yash Singh (3rd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
6. Sandali Akram (3rd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
7. Ipsa Mittal (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
8. Utkarsh Anand (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
9. Harshita Shukla (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
10. Aharnish Singh (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
11. Tibisha (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
12. Palak (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
13. Dharmpriya (2nd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
14. Anushka Pandey (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
15. Aayushmman Verma (1st Year MCLIS Student, NLIU Bhopal)
16. Mahi Mittal (1st Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
17. Vikram Singh Rathore (1st Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)

COMMENTS ON THE
DRAFT TELECOMMUNICATIONS (USER IDENTIFICATION) RULES, 2025

Rule No.	Sub-Rule (if any)	Provision	Issues Identified	Proposed Solutions
2		Definitions	1. "Live photograph" definition could raise privacy or implementation issues The rule mandates real-time photographs using technology capable of verifying "a living person physically present." Without specifying privacy safeguards, storage limits, or permissible technologies, this could raise data protection and surveillance concerns. 2. Inconsistency in referenced terms Some terms draw definitions from Aadhaar related regulations, while others from telecommunications rules. The difference in regulatory authorities (DoT vs. UIDAI) may lead to inconsistency in procedures if both define similar processes differently. 3. Unclear role and	1. Inclusion of privacy safeguards under "live photograph" Clarification that processing and storing live photos must adhere to data protection guideline, for example, outlining encryption specifications and retention limitations. 2. Ensure definitions are consistent across agencies. 3. Ensure coordination between DoT and UIDAI to align definitions of e-KYC, D-KYC, and biometric verification to prevent contradictory procedures. 4. Define operational control and audit responsibility for BIVS 5. Indicate if the approved entity, a licensed data fiduciary, or the DoT/UIDAI

			accountability of “authorised entities” in biometric processing Although the BIVS is described as "established by an authorised entity," it is unclear from this definition who is in charge of or conducts audits of the system, including if it is government-run, vendor-managed, or connected to UIDAI. In the event of identity fraud, false positives, or data leaks, this ambiguity may result in legal limbo.	will oversee BIVS management and mandate independent security audits at defined intervals.
3	(1)	These rules shall be applicable to: (a) entities providing notified telecommunication services, whether such entity holds authorisation under clause (a) of sub-section (1) of section 3 of the Act or a license in accordance with sub-section (6) of section 3 of the Act, which shall each be referred to as	1. Ambiguity regarding “notified telecommunication services” : The term “notified telecommunication services” is not defined here. Without a clear definition, entities may face uncertainty about whether a particular service (e.g., messaging app) falls under these rules. 2. Ambiguity regarding users’ responsibilities: The exact role or compliance obligations of the user are not specified here. This may create uncertainty about whether users have active duties (like verification steps) or are	1. Define “notified telecommunication services” : A detailed definition in the rules would clarify which services fall under these rules, reducing ambiguity and compliance risk. 2. Clarification the extent of user involvement: An explanation should indicate whether users have compliance obligations or are simply subject to identification requirements by the service providers.

		"authorised entity" for the purpose of these rules; and (b) users of notified telecommunication services.	merely affected by the rules indirectly.	
4		Principles and objectives	1. Ambiguity regarding the "authorised entity's" role and accountability: The rules provide wide powers to authorised entities to manage biometric systems, but don't specify who audits them, how securely data is stored, or whether government oversight exists or not. 2. Lack of clear data protection and usage safeguards: The rule allows for biometric collection, storage, and verification, but does not mention data minimisation, consent, retention period, or data sharing restrictions. 3. Over-reliance on Aadhaar-based and biometric identification: The entire system depends on biometric verification, either via D-KYC + BIVS (for non-Aadhaar users)	1. Define clear accountability and oversight mechanism: Specify whether biometric systems (BIVS, D-KYC) will be audited by government entities like DoT, UIDAI or a certified third-party auditor. 2. Include explicit data protection safeguards: Mandate adherence to the DPDP Act, 2023, which outlines the obligations for consent, encryption, storage restriction, and breach reporting for all biometric data gathered. 3. Introduce alternative non-biometric verification options: Allow other government-issued IDs (like PAN, Passport, or DigiLocker credentials) as valid alternatives where biometric collection is not possible or consent is withheld. This will ensure inclusion and

			or e-KYC (connected to Aadhaar). Citizens who are unable or unwilling to give biometric data run the risk of being excluded, and ongoing biometric processing raises privacy issues.	alignment with the voluntary use principle.
	(6)	Where the user is a business user seeking business connection, an authorised entity shall undertake biometric based identification, as applicable, of the authorised representative of such business user, as well as of each end user of such business connection.	1. Burdensome procedure for business users: It is not feasible for large businesses to require biometric verification of each end-user of a business connection, as well as the approved representative, and this could cause delays in service delivery.	1. Limit biometric verification to the authorised representative and provide a defined exemption process with clear criteria and timelines.
5	(1)(b)	Obtain the consent of the user, in accordance with applicable laws in respect of data protection, for: (i) clicking his live photograph or any other biological attributes of an	1. Unclear limits on data retention and access controls: This permits the storing of live photos and Aadhaar information, but does not mention for how long this information may be kept, who may view it, or how it may be shared. 2. Storage of complete Aadhaar number in unmasked form: The	1. Provide retention and access control provisions: In accordance with the Digital Personal Data Protection Act of 2023, include explicit retention and access control clauses with specified deletion procedures and retention periods. 2. Inclusion of the provision to include only masked Aadhar

		individual as may be specified by the Central Government; and (ii) storage of the live photograph and information including complete Aadhaar number in unmasked form, as received from UIDAI, other than core biometric information, in the CAF and SDR, in the form and manner as may be specified by the Central Government on the portal.	rule explicitly permits the complete Aadhaar number to be stored in the CAF and SDR, which is against the security and privacy policies of UIDAI. It raises the possibility of identity theft and data leakage.	numbers: Store only masked or tokenised Aadhaar numbers which is in compliance with UIDAI's regulations and restrict access to authorised personnel only.
	(2)	The authorised entity may also, in accordance with the directions or instructions specified by the Central Government, allow users to comply with the process of e-KYC set forth under sub-rule (1), by using the self-KYC process on the relevant website	1. Lack of safeguards for self-KYC via website or app: Allowing users to complete e-KYC through online portals or apps introduces cybersecurity risks if encryption and authentication standards are not mandated.	1. Frequent security audits for permitted organisations: Specify minimum technological requirements for online self-KYC (authentication, encryption, and audit logs) and mandate frequent security audits for permitted organisations.

		or mobile application of such authorised entity.		
6	(1)	Each authorised entity, before providing notified telecommunication services, shall, individually or collectively with such other authorised entities, establish, operate, maintain and expand BIVS for biometric based identification of user, using live photograph or any other biological attributes of an individual as may be specified by the Central Government on the portal.	1. Ambiguity in scope of "biological attributes" This rule allows use of "any other biological attributes" beyond live photographs, which could include sensitive biometrics like iris or fingerprints without limitation. This creates potential for privacy violations and misuse.	1. Clearly defining permissible biometric attributes and prohibiting expansion without explicit legal notification and user consent would prevent the violations.
	(4)(a)	Storing and maintaining the user information relating to name, gender, date of birth, live photograph, unique user-id and any other information as may	1. Broad data collection mandate: The rule grants undue discretion that could result in an overabundance of personal data by permitting the preservation of "any other information as may be specified" by the government.	1. Restrict collection to data strictly necessary for identification and require a data minimisation clause aligned with the Digital Personal Data Protection Act, 2023.

		be specified by the Central Government on the portal from time to time;		
	(7)	The user information maintained by an authorised entity in BIVS shall be shared with all other authorised entities, providing notified telecommunication services, to enable real-time verifiable biometric based identification of user, while ensuring data integrity and privacy in compliance with the applicable laws along with any directions as may be specified by the Central Government for this purpose.	1. Sharing of biometric and personal data among all authorised entities: This inter-entity sharing increases the risk of data breaches and inconsistent privacy practices.	1. Mandate sharing via only government approved APIs, strict access logs and end-to-end encryption.
	(10)	The data submitted by the authorised entity to the Central Government pursuant to sub-rule (9) shall be provided in an intelligible format,	1. Requirement to provide unencrypted data to the Government: This rule requires that information be shared in an understandable (unencrypted) manner, which is against secure handling guidelines and may	1. Allow only safe, encrypted government channels for data sharing, and only permitted audit environments should be used for decryption.

		and not in an encrypted manner.	reveal private biometric information.	
7	(1)	The authorised entity shall record in the CAF and SDR the reasons for a user using D-KYC.	1. The clause lacks clarity on what constitutes valid "reasons" for using D-KYC. 2. No guidance on whether the user must be informed or consent to such record. 3. "CAF" and "SDR" are undefined; creates interpretational ambiguity.	1. Define "CAF" (Customer Application Form) and "SDR" (Subscriber Database Record) in the definitions clause. 2. Require the authorised entity to inform the user of the reasons for using D-KYC and maintain an auditable record. 3. Add a clause mandating periodic review or audit of such entries.
	(2)	The authorised entity shall obtain consent of the user in accordance with applicable data protection laws for (a) capturing live photograph or other biological attributes, and (b) storage of such data in CAF and SDR.	1. "Applicable laws" is vague, does not reference the Digital Personal Data Protection Act, 2023 (DPDP Act). 2. "Any other biological attributes" gives excessive discretion to include highly sensitive biometrics without safeguards. 3. Lacks details on how consent is obtained (explicit, informed, revocable). 4. No mention of data security, retention period, or deletion	1. Explicitly align the provision with the DPDP Act, 2023, mandating "free, informed, specific and unambiguous" consent. 2. Limit data collection to minimum necessary identifiers. 3. Specify encryption, retention, and deletion standards. 4. Require that consent can be withdrawn and data erased unless retention is legally

			protocol.	mandated.
	(3)	The authorised entity shall obtain proof of identity and address as specified by the Central Government on the portal.	1. The term "portal" is undefined. 2. No clarity on verification method (digital, physical, or electronic KYC). 3. Lacks procedural safeguards to ensure secure transmission and prevent misuse.	1. Define the "designated portal" in the rules. 2. Specify that document verification must occur through secure, encrypted digital means. 3. Mandate compliance with government cybersecurity standards (e.g., CERT-In guidelines).
	(4)	The authorised entity shall comply with any directions and instructions specified by the Central Government in relation to the complete procedure for D-KYC process..	1. Over-delegation of power to the executive without requirement of publication or stakeholder consultation. 2. No transparency mechanism, directions may remain internal. 3. Absence of oversight or redress mechanism.	1. Require that all government directions be published in the Official Gazette or notified on the designated portal. 2. Include a clause ensuring periodic review or audit by an independent authority (e.g., TRAI or MeitY). 3. Provide an appeal mechanism or clarification procedure for authorised entities.
	(5)	Where a user having a unique user-id in	1. No procedure to verify if existing BIVS data is current or	1. Mandate user confirmation of existing details before re-

		the BIVS seeks a new connection or updating of telecommunication services, such user shall be identified using its existing details in the BIVS.	accurate. 2. No requirement for user confirmation before re-use of old data. 3. Risk of outdated or incorrect data being propagated across systems.	use. 2. Provide a mechanism for updating outdated data in BIVS prior to reuse. 3. Require audit logs to record every instance of BIVS-based authentication.
8		The authorised entity shall activate the telecommunication service of the users enrolled under these rules in accordance with rule 45 of the Telecommunications (Authorisation For Provision of Main Telecommunication Services) Rules, 2025 and in compliance with any directions, procedures or instructions as may be specified by the Central Government from time to time in this regard.	1. Over-dependence on cross-reference: The provision relies entirely on Rule 45 of another set of Rules, making it incomplete and difficult to interpret in isolation. 2. Excessive executive discretion: "Directions, procedures or instructions as may be specified by the Central Government from time to time" gives broad, unqualified power to the Government without ensuring publication or stakeholder consultation. 3. Lack of user-centric safeguards: No mention of timelines for activation, user communication, or conditions for rejection/suspension. 4. No reference to audit or accountability standards: Fails	1. Incorporate key procedural elements of Rule 45 by brief reference (e.g., activation after KYC verification, validation, and CAF entry). 2. Mandate that all directions and procedures by the Central Government be published in the Official Gazette or on a designated portal for transparency. 3. Include a time-bound requirement (e.g., within 24 or 48 hours post-verification) to ensure service activation efficiency. 4. Require authorised entities to maintain activation logs and user confirmation records for audit and compliance. 5. Add a safeguard clause: "No service shall be activated

			to ensure traceability in activation to prevent misuse or unauthorized activation.	without completion of prescribed verification under these rules.”
9	(1)	An authorised entity shall re-verify the identity of a user through e-KYC or D-KYC process, as applicable, in the following circumstances: (a) when a user seeks to replace or upgrade an already subscribed telecommunication service including replacement or upgradation of a SIM card; (b) in case of Mobile Number Portability; and (c) on directions of the Central Government	Ambiguity on triggers and scope of “re-verification”: The provision leaves undefined what specific events or risk thresholds will warrant re-verification beyond SIM replacement, MNP or Government direction. This creates potential for arbitrary or inconsistent demands by operators or authorities. Excessive compliance load: Mandatory e-KYC/D-KYC re-verification for every SIM replacement or MNP could lead to user inconvenience and cost escalation for service providers. Unclear privacy safeguards: There is no express linkage with data minimisation or purpose limitation under the Digital Personal Data Protection Act, 2023.	Define objective triggers: Specify the conditions and periodicity for re-verification For example - post data breach, suspected misuse or once every three years. Adopt risk-based verification: Permit simplified or digital verification, via OTP or Aadhaar-based check for low-risk scenarios, reserving biometric verification for high-risk cases. Integrate DPDPA safeguards: Include an explicit clause that all re-verification processes must adhere to the DPDPA principles of purpose limitation, storage limitation, and data security
	(2)	Change of user of a telecommunication service shall be permitted only between blood relatives and legal	(a) Overly restrictive transfer limitation: Limiting user change only to “blood relatives” or “legal heirs” excludes legitimate transfers to partners,	(a) Broaden permissible categories: Replace the restriction with “immediate family members, nominees, or lawful transferees recognised

		heirs, and for this purpose: (a) such request shall be accompanied by a submission of a no objection certificate from the original user whose identity shall be re-verified by the authorised entity, and in case of death of the original user, the death certificate of such user, and any other document as may be specified by the Central Government on the portal; and (b) telecommunication services provided to the new user shall be treated as a new telecommunication service connection, and accordingly, the authorised entity shall carry out biometric based identification of such user.	guardians or lawful assignees. (b) Ambiguity in documentation: The clause refers to "any other document as may be specified by the Central Government on the portal" without standardised formats, creating operational uncertainty. (c) Exclusionary phrasing: The phrase "blood relatives" may not legally include adopted children or dependents recognised under personal laws.	under law." (b) Prescribe uniform documentation: DoT should publish standard NOC templates and heir-proof formats on the Central KYC Portal. (c) Ensure inclusivity: Replace "blood relatives" with "immediate family members or lawful heirs" to include adoptive or dependent relations.

	(3)	Change of end user in a business connection shall be permitted, and for this purpose: (a) the authorised representative of the business user shall inform the authorised entity about such change immediately; and (b) biometric based identification of new end user shall be carried out within 7 days failing which the authorised entity shall disconnect such connection after 7 days from the date of intimation of such change.	(a) Unrealistic compliance window: The seven-day timeline for completing biometric identification is impractical for large enterprises managing multiple corporate connections. (b) Lack of graduated enforcement: Immediate disconnection after seven days provides no interim suspension or grace mechanism. (c) Absence of user notice: The Rule is silent on whether the outgoing and incoming users will be notified before disconnection.	(a) Extend verification timeline: Allow 15 working days for enterprises (or 30 for large entities) to complete end-user verification. (b) Introduce staged enforcement: Permit temporary suspension for non-verified connections before full disconnection. (c) Mandate notice requirement: Require operators to send prior notification (SMS/email) to both the business and affected user before disconnection.
	(4)	An authorised entity shall comply with the instructions specified by the Central Government in respect of any request by a user for migration from prepaid to postpaid telecommunication	(a) Absence of procedural clarity: The Rule does not outline how migration requests will be authenticated or processed, nor any timeline for completion. (b) Risk of arbitrary delays or refusals: Without time-bound mandates, operators may inconsistently handle migration	(a) Codify migration protocol: DoT should prescribe a standardised digital workflow for migration with a fixed timeline (e.g., 48 hours). (b) Ensure user consent and transparency: Require digital consent verification (OTP/e-sign) before migration to prevent unauthorised

		services or vice versa.	requests	conversions.
	(5)	All changes to user information undertaken in furtherance of sub-rule (1) to (4), shall be duly updated by the authorised entity in the CAF, SDR and BIVS.	(a) No timeline or accountability mechanism: The Rule does not specify the timeframe within which updates to CAF, SDR and BIVS must be completed. (b) Risk of data inconsistency: Without automated synchronisation, discrepancies between databases may result in outdated or conflicting records. (c) Absence of rectification process: Users lack an explicit mechanism to correct erroneous records in SDR or BIVS.	(a) Prescribe update timelines: Mandate real-time (within 24 hours) update of CAF, SDR and BIVS following any verified change. (b) Implement audit and reporting: Require quarterly compliance reporting and maintain audit logs for every data modification. (c) Introduce correction procedure: Establish a user-initiated grievance mechanism for rectifying inaccurate records in SDR/BIVS under DoT oversight.
10	(1)	The authorised entity shall, in addition to the obligations set out in other provisions of these rules, comply with the provisions set forth below.	(a) Redundant and vague drafting: The clause merely restates that the authorised entity must comply with subsequent sub-rules but lacks a distinct operative function. (b) Ambiguity on enforcement mechanism: The clause does not specify which agency will oversee compliance with these "additional obligations."	(a) Clarify oversight authority: Specify that compliance with Rule 10 shall be monitored by the Department of Telecommunications under the Unified License framework. (b) Merge with a compliance declaration clause: Instead of a standalone provision, integrate this sub-rule with the general compliance and reporting obligations under Rule 13

	(2)	The authorised entity shall inform users of consequences provided in the Act for: (a) their duties and obligations to provide correct information when establishing identity for availing of telecommunication services; (b) obtaining SIMs or other telecommunication identifiers through fraud, cheating or personation; and (c) providing false particulars, suppressing any material information, or impersonating another person, while establishing his identity for availing of telecommunication services.	(a) Lack of standardized communication format: The Rule does not specify how users are to be informed leading to inconsistency. (b) Potential non-compliance due to user illiteracy or language barriers: The rule assumes user comprehension of legal obligations, which may not hold true across India's linguistic diversity. (c) No penalty for omission: The Rule lacks deterrence or consequence if authorised entities fail to provide such information	(a)Standardize communication templates: DoT should prescribe multilingual, plain-language templates (SMS/email/portal pop-up) for conveying these obligations at the time of SIM activation. (b) Mandate acknowledgment of receipt: Require digital acknowledgment (e-sign/OTP) by users confirming they have been informed of these duties. (c) Introduce accountability: Include a compliance reporting requirement or penalty for authorised entities that fail to educate users as mandated.
	(3)	The authorised entity shall inform users of ensuring bona fide use of the subscribed	(a) Lack of defined scope for "bona fide use": The term "bona fide use" is undefined, which may create confusion	(a) Define "bona fide use": Specify that bona fide use refers to lawful, non-fraudulent and non-transferable use of

		telecommunication services; and caution about any kind of misuse of the subscribed telecommunication services and corresponding consequences as per the applicable laws.	regarding what constitutes "misuse." (b) Absence of periodicity or mode of intimation: The Rule does not state whether such caution should be issued only at activation or periodically. (c) Insufficient linkage to cybersecurity or fraud awareness programs: The provision isolates user cautioning from ongoing cyber hygiene initiatives.	telecom identifiers. (b) Mandate periodic user alerts: Require quarterly SMS/email reminders on misuse consequences and cyber safety. (c) Integrate with DoT/TRAI awareness drives: Link user education efforts with national cybersecurity and consumer protection campaigns (e.g., "Chakshu Portal," "Cyber Surakshit Bharat").
	(4)	The authorised entity shall ensure that: (a) biometric information and other information of a user shall not be stored on PoS's devices and be securely transmitted to the relevant systems of the authorised entity; and (b) the SDR and BIVS are operated and maintained in compliance with the applicable laws, rules and regulations in relation to data protection and	(a) Absence of technical standards for "secure transmission": The Rule does not define encryption or transmission protocols, leaving it open to varied interpretation. (b) Lack of independent audit mechanism: There is no mandate for periodic cybersecurity or data protection audits of PoS systems, SDR, and BIVS. (c) No accountability for third-party PoS operators: Many authorised entities outsource PoS operations, but this Rule doesn't clarify their liability for breaches.	(a) Specify security standards: Mandate end-to-end encryption and secure API protocols for transmission from PoS devices. (b) Introduce independent audits: Require annual third-party cybersecurity audits certified by CERT-In empanelled auditors. (c) Extend liability chain: Explicitly hold authorised entities responsible for compliance of third-party PoS vendors under contractual terms.

		security for the time being in force.		
	(5)	Where it comes to the notice of an authorised entity that false, incorrect, or forged information or documents were used during user enrolment and identification, the authorised entity shall: (a) initiate a police complaint or file a first information report with the relevant law enforcement agency with the requisite details, including the details of the false, incorrect, or forged information or documents; and (b) notify to the Central Government, in the form and manner as may be specified for this purpose, the steps taken pursuant to clause (a) above.	(a) Lack of procedural clarity: The Rule does not define what constitutes "coming to notice", whether through user complaint, audit, or data verification. (b)Potential over-criminalisation: Mandating immediate police action for all discrepancies, even minor clerical ones, may overburden law enforcement and penalise users unintentionally. (c) Absence of protection for good-faith errors: There is no distinction between intentional fraud and genuine documentation mistakes.	(a) Define "false or forged information": Limit the scope to intentional fraud or material misrepresentation verified through due diligence. (b) Introduce graded response: Require preliminary internal verification before lodging FIRs to prevent misuse. (c) Establish reporting format: DoT should issue a digital reporting form specifying timelines, content, and authentication standards for notification to the Central Government.
	(6)	Where it comes to the	(a) Lack of proportionality in	(a) Introduce graded penalties:

		notice of the Central Government that an authorised entity has not taken any action as specified in sub-rule (5) above, it may take action against such authorised entity under the Telecommunications (Adjudication and Appeal) Rules, 2025 and may direct the authorised entity to initiate a police complaint or first information report with the relevant law enforcement agency.	sanctions: The provision allows direct action against the authorised entity but does not prescribe proportional penalties based on the severity or frequency of non-compliance. (b) Overlap with existing adjudicatory mechanisms: The reference to the *Telecommunications (Adjudication and Appeal) Rules, 2025* creates overlap with TRAI and Unified License enforcement mechanisms. (c) Absence of due process for the entity: The Rule does not provide the authorised entity an opportunity to be heard before coercive action.	Differentiate sanctions based on the gravity of non-compliance. (b) Clarify jurisdictional overlap: Define coordination between DoT and TRAI to avoid regulatory duplication. (c) Ensure procedural fairness: Insert a proviso that no action shall be taken without giving the authorised entity an opportunity of being heard.
11		Disconnection of Telecommunication Services on Request of User	1. Lack of standardized disconnection process: The Rule provides a user an opportunity to request disconnection in accordance with the instructions of the Central Government, however, no structural procedure is outlined concerning how to initiate disconnection, authenticate, and certify such disconnection. This leaves an opportunity for irregularity of	1. Develop a consistent national disconnection policy: Develop a standardized, digitally verifiable system of user-requested disconnections by way of authorised portals, and connect it to BIVS and SDR to prevent its abuse. 2. Confirm biometrically prior to disconnection: Requirement Before terminating any connection, perform a final biometric authentication (via e-

			practices among service providers. 2. Absence of verification prior to disconnection: There is no clear mandate of re-authentication of user identity prior to accepting disconnection request which may result in fraudulent or rogue request. 3. Data update issues after disconnection: Although the rule states that Subscriber Database Record (SDR) and Biometric Identity Verification System (BIVS) must be updated in real-time, it does not specify the length of the data retention period, deletion procedures, or the processing of historical data of connection. 4. No wrongful or delayed disconnection redress: The users do not have any specific avenue to challenge wrongful disconnection or slow response time to their requests which may have a negative impact on consumer rights and confidence.	KYC or D-KYC) to ensure that the identity of the user is validated. 3. Establish data retention and data deletion periods: Introduce certain data retention policies regarding the SDR/BIVS (e.g., 12-24 months) and how and when this data should be deleted in accordance with data protection regulations. 4. Create a consumer redressal system: Have a systemic grievance system under DoT or TRAI to resolve wrongful disconnections, delays, or errors in systems and ensure they are resolved within a given time (e.g., 15 working days).

12	(2)(b)	A user shall not: resell or transfer or lease or share his telecommunication connection to any other user: Provided that, this clause shall not restrict the change of user of telecommunication services as per sub-rule (2) or sub-rule (3) of rule 9.	1. The blanket prohibition on "sharing" is overly broad and may criminalize or lead to penal action for common and harmless household practices, such as a father providing a SIM to his adult son, or family members sharing a mobile hotspot, which do not pose a fraud risk. 2. Rule 9(2) allows change of user only between blood relatives and legal heirs, but the prohibition in Rule 12(2)(b) does not align with the needs of modern households (e.g., in-laws, step-siblings, or guardians who are not legal heirs).	1. The definition of "share" should be strictly limited to "sharing for commercial gain" or for the "commission of an offence". Amend the provision to read: "resell or transfer or lease his telecommunication connection to any other user, or share his telecommunication connection for the purposes of commercial gain or for the commission of an offence." Rule 9(2) should be expanded to allow transfers to a wider circle of family members (including in-laws, step-siblings, or individuals recognized as part of the family unit) to prevent unnecessary disconnections and ensure the service continuity and legitimate use.
	(4)	Any change in address of user shall be intimated to the authorised entity within one month of such change along with proof of new address and the said details shall be duly updated in the CAF	1. The mandatory one-month timeline for updating the address places an unnecessary compliance burden on users, especially considering that the telecommunication service itself is not tied to a fixed location and no immediate fraud risk is posed by the address change alone.	1. Remove the strict "within one month" timeline for updating the address. Instead, make the update a mandatory requirement upon the user's next KYC or re-verification cycle as specified by the Central Government under Rule 12(5) or Rule 9(1).

		and SDR by the authorised entity.		
	(5)	A user shall re-verify its identity through e-KYC or D-KYC process, as applicable, in a periodicity as may be specified by the Central Government for this purpose.	1. Mandatory periodic re-verification for all users without an established fraud risk or a clear public interest justification could lead to mass disconnections and inconvenience, especially for senior citizens and rural users, thereby contradicting the policy objective of ubiquitous access.	1. Limit mandatory periodic re-verification to specific, clearly defined circumstances, such as: (a) cases where the Central Government detects a high-risk indicator of fraud or non-compliance; (b) users enrolled under the old Indian Telegraph Act, 1885 regime (as already covered by Rule 12(6)).
13	(2)	Any violation or non-compliance of these rules by a user, shall be subject to the provisions of the Act.	1. The Act specifies severe penalties for users, including imprisonment up to three years or a fine up to two crore rupees for fraud or personation, but Rule 13(2) could subject users to these extreme penalties for even minor non-compliance with the Rules (e.g., late address	1. Introduce a clear distinction between severe and minor user violations by amending Rule 13(2) to: "Violations of this Rule shall be subject to penalties as specified in the Third Schedule of the Act". This ensures minor rule infractions are addressed

			update or accidental use of a false document).	through civil penalties rather than criminal charges.
	(3)	Where it comes to the notice of the Central Government that the telecommunication services of a user has been activated by an authorised entity in contravention of these rules, the Central Government shall direct the authorised entity to suspend the telecommunication services of such user immediately, and re-verify the identity of such user in accordance with these rules within a specified period...	1. The mandate for immediate suspension could lead to the disconnection of a legitimate user's service without a prior opportunity to be heard, impacting their basic right to communication and access to digital services (e.g., banking, social welfare). 2. Rule 13(3) focuses solely on the penalty for the user (suspension/disconnection), while the root contravention was committed by the authorised entity (improper activation).	1. Replace "suspend immediately" with "initiate the process for suspension". The provision should mandate a minimum 48-hour notice to the affected user (via SMS, email, or post) before suspension, allowing the user to initiate the re-verification process and avoid service disruption. 2. The Central Government's direction to the authorised entity should explicitly include an instruction to impose a civil penalty on the authorised entity for the improper activation, in addition to demanding re-verification, ensuring accountability aligns with Rule 13(1).
14	(1)	Access to CAF, SDR and BIVS provided to the Central Government or an authorised agency by the authorised entity.	1. The draft provides the central government and its agencies access to CAF, SDR and BIVS. The rules do not define conditions, purposes, or authorisation levels leaving room for unrestricted access to sensitive biometric and	1. To resolve this purpose-based access can be restricted to national-security investigations, telecom-fraud prevention and for compliance with other IT related acts. 2. An authorisation and accountability framework can

			demographic data. 2. The draft lacks an authorisation and accountability framework specifying scope, duration or reason for access or verifying lawful use 3. Lack of transparency for the users, they are not informed when their information is accessed by the government. 4. Provision disregards data minimisation and purpose limitation requirements under DPDP Act.	be established requiring each access request to be approved in writing or authorised under a judicial warrant. A database can be maintained containing records of each access instance. 3. A clause can be introduced requiring that users be notified of any government access to their data 4. A sub-clause can be introduced that access and use of data under this rule must comply with the DPDP Act, including principles of purpose limitation and data minimisation.
	(2)	Issuance of clarifications, orders or procedures by Central Government	1. The clause by allowing the central government to issue clarifications, orders, or procedures enables the executive to formulate rules and laws without the oversight of the legislature. 2. The process of issuance of such clarifications is opaque as it is unclear whether such orders need to be published in the Official Gazette or will go through consultation by	1. It can be specified that clarifications or procedures cannot alter substantive rights or obligations and must be confined to administrative or procedural implementation. 2. Transparency and accountability can be ensured by mandating that all orders issued under this clause need to be published in the Official Gazette and uploaded on the notified portal. Further, it can be mandated that for any order

			stakeholders. 3. The phrase "Not inconsistent with these rules" is too broad, vague and open to multiple interpretations. It allows the government to issue directions that may modify data-protection standards or access norms.	that materially affects user data, the public or the Data Protection Board of India must be consulted before enforcement. 3. Establish parliamentary or judicial oversight making such order subject to review to prevent misuse.
15		Notification of a portal by the Central Government for digital implementation of rules.	1. The rule is silent on encryption, data-retention duration, access control, or storage location i.e. domestic and foreign servers. This omission risks centralising massive volumes of biometric and identity data without lifecycle safeguards. 2. The rule does not specify which body will maintain the portal. It also doesn't define how the portal will interact with other digital-governance systems, creating scope for duplication and inconsistent handling. 3. The portal has no defined process for users to check, correct, or delete their data, nor to raise grievances in case of	1. A comprehensive data-protection framework can be established requiring end-to-end encryption, secure domestic storage, and retention limits. Periodic third-party security and data-protection audits can be mandated. 2. It needs to be specified which designated government body shall operate the portal. CERT-In guidelines and MeitY's cybersecurity framework can be followed. Clear data-exchange procedures with UIDAI, licensed telecom operators and other digital-governance systems need to be developed. 3. The portal should provide a dashboard showing users their

			misuse or breach. 4. A single government-controlled database connecting BIVS, SDR, and CAF increases the impact of any data breach or unauthorized access.	data and access logs, a grievance-redressal mechanism with defined timelines, and an option to request correction or deletion. 4. The portal should only be rolled out after conducting proper pilot testing and a Data Protection Impact Assessment. Annual certification by an independent cybersecurity auditor can also be seeked.