CUTS Comments on the

Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

REGULATORY IMPACT ASSESSMENT

CUTS International
1983-2023

CUTS Comments on the Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

Regulatory Impact Assessment

Published by

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Author: Krishaank Jugiani, Senior Research Associate, CUTS International. For any clarifications or further details, please feel free to contact him at: kju@cuts.org

Acknowledgement: The author is grateful for the support and guidance of Amol Kulkarni, Director (Research), CUTS International, (amk@cuts.org) and for assistance from Sohom Banerjee, Research Associate, CUTS International (sje@cuts.org)

Table of Contents

Regulatory Impact Assessment

Regulatory instruments such as policies, legislations, rules, and regulations etc (regulations) have widespread impacts, which affect multiple stakeholders in different ways. Regulations tend to change behaviour of stakeholders, and thus impose additional costs. Consequently, only such regulations must be adopted which can achieve intended objectives with least possible distortions. Moreover, sub-optimal regulations have the potential to impose superfluous costs on stakeholders, raise complexity and uncertainty associated with obligations, which must be avoided. Therefore, it is important to understand impacts of proposed and existing regulations to formulate most optimal design.

One of the systematic approaches to critically assess the impacts of proposed and existing regulations is Regulatory Impact Assessment (RIA). RIA is a process of systematically identifying and assessing direct and indirect impacts of regulatory proposals and existing regulations, using consistent analytical methods. It is a scientific globally recognised methodology to identify market failures/problems which the proposed regulatory intervention intends to address, estimate costs and benefits of such proposals on different stakeholders, particularly industry and consumers, and examine the likelihood of such proposals achieving its objectives.

RIA is an important element of an evidence-based approach to policy making, as it involves a participatory approach via public consultation to assess such impact, determination of costs and benefits, and selection the most appropriate regulatory alternative. Impacts of regulatory options are compared with 'as is' scenario on the basis of scientifically developed tools such as cost-benefits analysis, cost-effective analysis etc. and thus best possible regulatory intervention is selected.

CUTS expresses gratitude to the Department of Telecommunications (DoT) for inviting comments and suggestions and is pleased to submit its comments on the draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025. We have observed a few critical issues in the draft Rules, which have been discussed in subsequent sections, which are stated in the RIA framework. By conducting RIA, we hope to quantify and monetise direct, indirect, apparent, latent, short term and long terms impacts of the Draft Amendment Rules on key stakeholders, digital markets, and growth of digital services in India. The unintended consequences in terms of disproportionate compliance burden, particularly on SMBs and exclusion and privacy concerns for consumers are also highlighted.

Regulatory Impact Assessment of the Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

1. Is the scope of Draft Amendment Rules within the purview of the parent Act and Rules?

1.1. Telecom Act and Rules only govern telecom licensees, telecom network and infrastructure

The Telecommunications Act, 2023 ("the Act" or "the Telecom Act") provides the legal foundation for regulating telecom networks, services, spectrum allocation, and critical telecom infrastructure. It grants the government specific rule-making powers under Sections 22(1) and 56(2)(v) to provide for measures to protect and ensure cyber security of telecommunication networks and telecommunication services.

As per the design of the Act, telecom network is used to provide telecom services. Both the provision of telecom services; and establishment, operation, maintenance and expansion of telecom network, are licensed activities, which can be undertaken only by authorised entities. A naturally corollary of this design is that the issue of cyber security of telecom networks and services can, and should, fall within the exclusive domain of authorised entities.

Any attempt to shift the responsibility of cyber security on entities other than the authorised entities may lie outside what is permissible under the Act, and invite unintended adverse consequences.

1.2. Draft Amendment Rules increase the scope to regulate digital service providers

The Draft Amendment Rules propose to recognise a completely new set of entities, namely the Telecommunication Identifier User Entities (TIUEs). This group could, potentially by definition and scope, include non-telecom licensed platforms/ entities not intended to be regulated under the Telecom Act, such as:

i. digital service providers such as fintech apps, OTT providers, and e-commerce services, and even small and medium digital businesses,

ii. predominantly offline stores which obtain telephone numbers for communication, sharing of offers and receipts, and

iii. even institutions like schools and hospitals will come into the ambit of TIUEs.

In addition, every potential seller and purchaser of mobile phones, including end consumers, can potentially be covered with the Draft Amendment Rules.

This raises significant jurisdictional and legal concerns. This also appears to be regulatory overreach, with the Draft Amendment Rules attempting to impose telecom-style compliance obligations on entities outside the telecom licensing regime, which include service-level operations and user transactions.[1] In effect, every person using a mobile phone can be held responsible for its telecom cyber security.

In reality, the telecom Act traditionally regulates the carriage i.e. carriers of signals i.e., voice, data, and video, over telecom networks, and not the content itself. The Act does not contain any explicit provision authorising the creation of a new class of regulated entity solely because it uses telecom identifiers for identification and communication services.

The persons to whom telecom identifies are issued are consumers of telecom licensees, and it is at this stage that telecom licensees need to ensure that rogue and fraudulent actors do not

[1] https://www.medianama.com/2025/06/223-dot-mobile-number-validation-business-impact-privacy/

enter the telecom network so that its cyber security remains robust. Entities engaging with consumers of telecom licensees for provision of services use telecom identifiers since such identifiers are supposed to be issued to genuine persons only. Shifting the burden of telecom cyber security on such service providers does not make sense.

Section 56 of the Act empowers the government to make rules consistent with the Act; Section 3(1) empowers licensing of telecom services; but neither provision envisages entities like TIUEs. This raises questions regarding whether subordinate legislation can expand regulatory scope beyond what is permitted by the parent legislation and risk being deemed ultra vires.[2]

The core concern is the lack of legal certainty. The proposed framework appears to extend the reach of the Act beyond its intended scope by effectively treating phone-number usage as sufficient grounds for telecom-style regulation. The framework also confuses identity verification with telecom infrastructure governance and imposes compliance obligations on entities already regulated under the Information Technology Act, 2000 ("IT Act").

1.3. Digital service providers are already regulated under IT Act and Rules

The inclusion of TIUEs, who are neither licensed operators nor network providers, appears to exceed the statutory scope of the Act and conflicts with the regulatory domain of the IT Act and Rules issued thereunder. Similarly, requiring data collection from TIUEs under proposed Rule 3(1)(aa) lacks a strong statutory connection to the regulation of telecom services.

These entities, while do use digital identifiers (e.g., phone numbers) to provide their services, are not licensees under the Act. This expansion may further generate incoherence between regulatory frameworks. DoT would require TIUEs to comply with telecom identifier validation obligations while telecom carriage remains under its remit, yet content and intermediary practices are under the Ministry of Electronics & IT (MeitY) and TRAI oversight. In addition, a lot of sector specific regulators, such as the Reserve Bank of India and Securities and Exchange Board of India, have already imposed cyber security related obligations on their regulated entities, which include digital service providers. TRAI has recently declined a request by DoT to regulate telemarketers,[3] highlighting confusion and broader fragmentation between the two regulators. Without clear demarcation and inter-agency coordination, service providers may face overlapping or contradictory mandates, compliance complexities, and legal ambiguity.

It is important to note that the then Minister of Communications Ashwini Vaishnaw had also publicly opined that platforms like OTTs will be kept out of the purview of the Act.[4] Such entities' possible inclusion under the new Draft Amendment Rules marks an expansion of scope, arguably exceeding the legislative intent of the parent Act.

1.4. Draft Amendment Rules propose creation of MNV platform and IMEI registry which appears to be excessive delegation

A more acute concern is the introduction of the Mobile Number Validation (MNV) platform under Rule 7A. The draft Rule mandates that the government will set up the MNV platform for the purpose of TIUEs to verify telecom identifiers from this platform. The Telecommunications Act, 2023 does not reference or empower the establishment of such a

[2] https://www.youtube.com/watch?v=MzHNeeYSPbQ

[3] https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-declines-dots-request-to-regulate-telemarketers/articleshow/122843855.cms?from=mdr

[4] https://www.medianama.com/2023/12/223-communications-minister-telecom-bill-ott/ and https://telecom.economictimes.indiatimes.com/news/policy/ott-not-under-ambit-of-telecom-bill-ashwini-vaishnaw/106224380

platform. As such, the authority to create this platform appears to exceed the powers delegated by Parliament. It potentially becomes a policy tool with operational and financial implications that has been created through delegated legislation, without direct parliamentary sanction—making it potentially ultra vires. In effect, this regulatory construct is a new invention by the draft Rules themselves. It likely falls outside the original ambit of the Act, rendering it potentially ultra vires. Without explicit legislative sanction or amendment to the parent Act, the legal basis for the MNV platform and imposition of charges for its use remains tenuous and susceptible to legal challenge.

In a similar vein, Rule 8's directive to create a national database of tampered IMEIs and to require ₹10-per-check validation before resale represents another case of excessive delegation. While OEMs are already subject to pre-registration via the existing CEIR framework,[5] this new mandate shifts post-sale compliance onto used-device buyers, resellers, and secondary market entities. The prevention of tampering of the Mobile Device Equipment Identification Number, Rules, 2017, which were superseded by the Telecom Cyber Security Rules 2024, mandated every mobile manufacturer or importer to register each device's IMEI in the Central Equipment Identity Register ("ICDR/CEIR") before the device is sold or imported.[6] However, the Draft Amendment Rules intend to go beyond, and include sellers and purchasers of used mobile phones.

The creation of a national database of tampered or restricted IMEIs, to be maintained by the government or an authorised agency, also raises concerns of excessive delegation. Such a database could potentially contain millions of device records and should not be left to subordinate legislation without adequate legal or procedural safeguards. There is nothing in the Telecom Act empowering DoT to require ongoing, repeated data submissions by private parties for secondary market enforcement. Moreover, this burdensome infrastructure effectively duplicates regulatory systems without clear statutory authorisation or coordinated governance structure, a case of over-delegation absent a legislative directive.

This change moves away from static, pre-sale equipment checks toward a dynamic, post-market surveillance model, significantly expanding both the compliance burden and the scope of enforcement, for both the regulator and buyers and sellers of used mobile phones, which can be users as well, since most of these providers are fragmented and unorganised smaller sellers across the country.[7] This is important considering that Microsoft reportedly blocks up to 7,000 password-based attacks per second, amounting to billions of unauthorised login attempts annually.[8] Scaling systems to handle oversight, logging, and compliance checks for millions of mobile number validations and IMEI number verifications would require a similarly unprecedented infrastructure. For fragmented vendors lacking formal onboarding or sophisticated IT support, meeting such demands in real time may be logistically and technically unsustainable.

[5] https://ceir.sancharsaathi.gov.in/Home/index.jsp

[6] https://thc.nic.in/Central%20Governmental%20Rules/Prevention%20of%20tampering%20of%20the%20Mobile%20Device%20Equipment%20Identification%20Rules,2017.pdf

[7] https://www.counterpointresearch.com/insight/india-unorganized-refurbished-smartphone-market-is-growing-with-organized-valueadded-services-contributing-to-its-maturation

[8] https://thevocalnews.com/scam-watch/microsoft-blocks-password-attacks-passkeys-future-security/cid15883168.htm

1.5. Draft Amendment Rules propose imposition of charges/ fees which appears to be excessive delegation

The monetary charges proposed for validation and verification under Rules Rule 7A(2) and 8(7) goes also beyond the intent of Section 22 and 56(2)(v), which enable standards, security practices, upgradation requirements and procedures, but not commercial pricing structures. The proposal to charge fees from TIUEs is not grounded in the Act and could be susceptible to constitutional challenge on grounds of ultra vires or violation of Article 14 due to arbitrary delegation. This is because these fees would significantly inflate compliance costs, especially for digital and identity-service platforms, and adversely impact businesses.

The directive compelling TIUEs to perform real-time validations via this platform, including associated fees, lacks a statutory backbone. Unlike the enumerated powers under Sections 19–22, which empower the government to ensure telecom cybersecurity through technical standards, emergency powers, and national security directives, there is no specific provision empowering the DoT to impose infrastructure mandates or fee regimes for identity verification for cybersecurity purposes. Under established principles of administrative and constitutional law in India, subordinate legislation must operate within the bounds of authority expressly delegated by the parent statute. Section 56 of the Telecommunications Act, 2023, which empowers the government to make rules, does not confer the power to expand the scope to any new entities and impose compliances on them, particularly financial obligations. Such substantive policy decisions, especially those which may have implications for privacy, access, and costs must be anchored in primary legislation, not left to executive discretion.

1.6. Draft Amendment Rules propose data sharing frameworks which appear inconsistent with Puttaswamy decision

The draft amendments Rules extend data-sharing obligations for TIUEs, requiring them to collect, store, maintain logs, and share personal identifiers and metadata with government agencies under Section 3 of the Telecommunications (Telecom Cyber Security) Rules, 2024. This fundamentally deviates from the constitutional safeguards enshrined by the Supreme Court in Puttaswamy v. Union of India (2017), which recognised privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution of India. The Puttaswamy judgment requires that any state action impinging on privacy must satisfy three constitutional tests: legality (existence of a valid law), legitimate state interest, and proportionality (least intrusive means proportional to the objective). The Draft Amendment Rules, particularly Rule 3 appear inconsistent with the Puttaswamy judgement and risk violating constitutional guarantees, by mandating extensive sharing of identifiers and datasets across entities and service providers, without any legislative backing, rationale, or consideration of proportionate alternatives.[9]

1.7. ***Finding: The scope of draft amendment Rules does not appear to be within the purview of parent Act and Rules***

2. Are the Draft Amendment Rules likely to achieve the desired objectives?

2.1. The objective of Draft Amendment Rules is not clearly stated

The objectives of the Draft Amendment Rules are not clearly stated in the official Gazette notification. The proposed Rule 7A (1), says, 'with a view to ensuring telecom cyber security and preventing security incidents,' indicating that the objective appears to address the growing

[9] https://www.hindustantimes.com/india-news/govt-plans-mobile-number-verification-for-apps-banks-101751107870061.html

cyber security risks that are becoming prevalent in the telecom ecosystem in India.However, these inferences are not clearly mentioned as objectives in the Draft Amendment Rules. As a result, the problem definition remains vague, giving the DoT wide discretion in implementation and raising concerns about disproportionality, lack of oversight, and misalignment with clearly articulated policy goals.

2.2. Draft Amendment Rules aim to address cyber security risks emerging from stolen sims and mobile phones

Upon a review of draft Rules, including proposed Rules 7A and 8, which deal with validating mobile numbers, through a centralised Mobile Number Validation (MNV) Platform–it appears that the objective is to combat misuse of dormant, stolen, fraudulently acquired, unused, forgotten, or otherwise misused telecom identifiers (phone numbers, SIMs, IMEIs) that could lead to security incidents such as identity theft, fraud, among others and other security incidents in the telecom ecosystem.[10]

Both the text and expert commentary also recognise this as an objective of the draft Rules. The DoT aims to prevent escalating telecom-related cyber threats, such as identity theft, SIM-swap fraud, and IMEI misuse.[11] Evidence underscores both the scale and urgency of the issue. In 2023, daily SIM-swap frauds were reported in every city, and criminals routinely exploited mobile number porting to steal OTPs.[12] Many entities, including companies have lost crores of rupees in SIM-swap cases, highlighting the massive scale of the issue.[13] Such figures clearly demonstrate a systemic and widespread nature of the problem, which the Draft Amendment Rules are attempting to address. Thus, the intention of Draft Amendment Rules appears legitimate.

There have been efforts to curb such incidents. In 2023, of the 1.14 billion active mobile connections in India, over 6.6 million were flagged as suspicious, leading to 5.2 million disconnections and over 67,000 telecom dealers being blacklisted. Moreover, nearly 1,700 FIRs have been filed against dealers involved in fraudulent KYC practices.[14] 2024's data shows that 7.3 million connections obtained via forged documents were also rooted out in mid-year.[15] In response, authorities have stepped up their efforts. Till October 2024, using AI-driven systems, 1.77 crore mobile connections acquired through fraudulent or forged documents had been identified and deactivated. Furthermore, 45 lakh spoofed international calls have been blocked from infiltrating India's telecom network.[16] Consequently, already, there are several initiatives which aim to address the problem.

2.3. Draft Amendment Rules are unlikely to achieve their objective

First and foremost, it is not clear how the MNV platform will work. For instance, the Draft Amendment Rules only describe the MNV platform, and that it will be used for "validation of

[10] https://www.storyboard18.com/how-it-works/centre-tightens-telecom-cybersecurity-rules-mandates-mobile-number-validation-for-all-service-platforms-71896.htm

[11] https://www.mondaq.com/india/telecoms-mobile-cable-communications/1651616/draft-amendments-to-the-telecom-cybersecurity-rules-strengthening-cybersecurity-or-regulatory-overreach

[12] https://www.protectt.ai/sim_binding_solution_protect_sim_swap_frauds

[13] https://perfios.ai/blogs/a-real-story-on-how-sim-swap-fraud-cost-a-company-millions/

[14] https://www.hindustantimes.com/india-news/union-government-announces-overhaul-of-kyc-norms-for-mobile-phone-connections-to-crack-down-on-cyber-fraud-industry-101692296237181.html

[15] https://www.business-standard.com/industry/news/7-3-million-connections-obtained-on-fake-documents-shut-down-dot-124080701465_1.html

[16] https://timesofindia.indiatimes.com/technology/tech-news/govt-has-deactivated-1-7-crore-mobile-connections-blocked-45-lakh-scam-calls-so-far/articleshow/113946754.cms

whether the telecommunication identifiers as specified by their customers or users, correspond to the users as present in the database". The users that do not match with provided data may face disconnect or suspension. Yet it is not clear how frequently records will be updated or how disputes (e.g. subscriber vs user name mismatches) will be resolved. This makes it unclear whether the platform will simply respond "valid/invalid" or provide more nuanced data. But more importantly, how it will handle edge cases where the difference of identity has been previously compromised or stolen.[17]

Moreover, fraudsters have repeatedly shown the ability to acquire subscriber identity and fool validation systems. Court and STF investigations have found criminal networks using fake or stolen Aadhaar credentials to activate SIM cards, then leveraging those SIMs for fraud or resale, all without triggering detection.[18] If the identity attributes (SIM subscriber, Aadhaar, alternate number, photographs) are stale or forged, and verification does not include robust live or liveness checks, the MNV platform will merely replicate existing fraud rather than prevent it.[19] Most of such frauds are the result of upstream vulnerabilities such as porous KYC process, gaps in telecom identifier issuance, or weak verification processes.[20] The proposed Rules may not adequately address issues like misuse of SIMs of leaked data on customer details through cyber breaches,[21] and misreporting and reissuance of SIMs for frauds.[22] A fraudster using a stolen or SIM-swapped number, but paired with the legitimate subscriber name, would still pass validation. Similarly, IMEI controls may be ineffective against inexpensive burner phones with valid identifiers and are commonly used in fraud—which sidesteps tampering detection altogether.[23]

Operationally, the system also faces monumental logistical challenges. With over 1.1 billion active mobile connections,[24] the platform will need to manage, refresh, and respond to massive real-time queries. Maintaining latency, accuracy, and data integrity at this scale is itself a security vulnerability, may create a honeypot for fraudsters, as any compromise in the verification API or mobile identity database could open the floodgates to systemic disruption or mass deregistration.[25]

2.4. Draft Amendment Rules do not target the core issue and may lead to inconsistent approaches

The framing of the Draft Amendment Rules remains too narrow given the broader threat environment. The core issue lies not solely in the misuse of SIMs or IMEIs, but in the porous and inconsistent identity verification processes that underlie telecom KYC (Know Your Customer) or customer verification procedures. While the Department of Telecommunications

[17] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com

[18] https://the420.in/up-stf-busts-illegal-sim-card-gang-prayagraj/

[19] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com

[20] https://telecom.economictimes.indiatimes.com/news/industry/cbi-cracks-down-on-pos-generating-ghost-sim-for-cybercriminals/121245390

[21] https://economictimes.indiatimes.com/industry/telecom/telecom-news/cybersecurity-co-claims-data-leak-of-750-mn-telecom-users-dot-asks-telcos-for-security-audit/articleshow/107239398.cms

[22] https://timesofindia.indiatimes.com/city/delhi/sim-swap-fraud-over-100-customers-duped/articleshow/92421686.cms

[23] https://timesofindia.indiatimes.com/city/nagpur/sextortion-accused-mahto-used-burner-phones-cops-probe-financial-trail/articleshow/121868512.cms

[24] https://www.trai.gov.in/sites/default/files/2025-06/PR_No.51of2025_0.pdf

[25] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com

(DoT) mandates subscriber registration through e-KYC, digital KYC (d-KYC), or paper-based KYC (p-KYC), the actual implementation of these procedures remains weak and fragmented. The KYC details are collected by TSPs (Telecom Service Providers), as self-declarations from subscribers. TSPs are required to fulfil mandatory KYC compliance checks of users prior to the issuance of SIM cards. KYC information is basic user information, including the full name, photograph, Date of Birth, address, etc., which is collected and verified based on certain official documents such as Aadhaar, driving licence, PAN card, passport, etc. Such information may not be completely accurate, and possibility of information mismatch exists. Moreover, the manual verification of KYC information can be filled with errors.[26] Moreover, forging of such official documents to get SIMs issued is not uncommon.

A joint study by the ISB Institute of Data Science and the Telangana Cyber Security Bureau found that telecom SIM subscription fraud continues to thrive in this environment, with identity verification failures forming the crux of the problem.[27] The study–based on analysis of over 1,600 Customer Acquisition Forms (CAFs), public complaints, and real-time data, found that nearly 91.76% of d-KYC users submitted Aadhaar as proof of identity. However, in 89.11% of these cases, the alternate number provided during onboarding was not linked to the submitted Aadhaar, rendering the OTP-based verification process largely ineffective. While this highlights a specific Aadhaar-based vulnerability, the broader issue was that Point-of-Sale (PoS) agents failed to verify identity documents (such as Aadhaar, voter ID, driving licences) with issuing authorities across KYC types. There was no real-time cross-verification of photographs from ID documents against live images captured at the time of SIM issuance, allowing fraudulent actors to successfully complete onboarding with mismatched or forged credentials.[28]

Importantly, these vulnerabilities were not limited to d-KYC. Even e-KYC procedures, which involve biometric submissions were undermined by the lack of real-time checks by PoS agents, making identity theft and subscription fraud viable through stolen or spoofed credentials. These findings emerged from Telangana—a state with one of the high per capita income[29] and a rural literacy rate of 66.54%[30]—implying that the problem could be significantly worse in other states, where compliance and verification oversight, digital literacy, and enforcement capacity may be weaker. Hence, the national scale of flawed KYC-driven fraud may be far greater. In terms of security too, the BSNL breach in July 2024 alone exposed 278 GB of sensitive telecom data.[31]

Furthermore, the data collected through KYC–often via self-declaration, is not routinely updated or re-verified, which turns it into a static and unreliable dataset over time. RTI responses indicate that the TRAI does not maintain or confirm the veracity of KYC data, and key infrastructure such as the Telecom Analytics for Fraud Management and Consumer Protection (TAF-COP) portal remains only partially operational.[32]

These findings highlight that telecom fraud primarily stems from fraudulent misuse of SIMs or leakages in the issuance process, facilitated by compromised KYC processes, rather than

[26] https://cuts-ccier.org/pdf/comments-on-the-trai-cnap-consultation-paper.pdf

[27] https://prodcd.isb.edu/media/wkrbce4o/iids-police-report-july-23-2024-1.pdf

[28] https://prodcd.isb.edu/media/wkrbce4o/iids-police-report-july-23-2024-1.pdf

[29] https://timesofindia.indiatimes.com/city/hyderabad/telangana-leads-in-per-capita-income-essential-consumption/articleshow/118338553.cms

[30] https://ecostat.telangana.gov.in/PDF/PUBLICATIONS/Telangana_at_Glance_2024.pdf

[31] https://www.business-standard.com/companies/news/bsnl-data-breach-exposes-278-gb-of-sensitive-telecom-info-twice-in-6-mts-124062600314_1.html

[32] https://cuts-ccier.org/pdf/comments-on-the-trai-cnap-consultation-paper.pdf

misuse after issuance. Without reforming KYC protocols, enforcing agent accountability, and implementing robust biometric verification, the proposed rules risk treating the symptoms while leaving the core vulnerability unaddressed. These figures point to foundational gaps in data protection, network security, and KYC verification—issues the current Rules do not aim to address. While the intent of the Draft Amendment Rules objective is valid, they focus on only one dimension of a much broader telecom cybersecurity crisis.

2.5. There are already several initiatives which aim to target the core issue

Several existing frameworks already target the core issues of telecom fraud and cybercrime, indicating that the Draft Amendment Rules duplicate regulatory efforts rather than build on them. The Indian Cyber Crime Coordination Centre (I4C), established under the jurisdiction of the Ministry of Home Affairs, already spearheads cross-jurisdictional coordination among law-enforcement bodies to combat telecom-related fraud. Its initiatives include the National Cyber Crime Reporting Portal, the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), and a dedicated helpline (1930). Under I4C's aegis, over ₹5,489 crore has been recovered from fraudsters through 17.82 lakh citizen complaints, and more than 9.42 lakhs SIMs and 263,348 IMEIs linked to scams have been blocked.[33] These efforts directly address cross-servicing risks and identifier abuse, rendering new MNV and IMEI mandates prone to overburden entities and increase compliance.

Telecom operators further employ advanced AI/ML systems to detect anomalous call patterns, block spam SMS/calls, and flag suspicious transactions in real time.[34] Google's DigiKavach initiative, launched in 2023, partners with I4C and fintech associations to leverage AI-driven alerts and user-awareness programmes.[35] Sectoral regulators such as RBI and SEBI already enforce KYC protocols for financial and capital-market services.[36] They also use other methods like Multi-Factor Authentication and Two-Factor Authentication, widely adopted methods that require users to provide two or more verification factors such as password + One-Time-Password via SMS, email or authenticator app, or password + biometric scan–significantly increasing security against unauthorised access.

There are also victim support and grievance redressal mechanisms such as through the National Cyber Crime Reporting Portal. It allows streamlined FIR registration across jurisdictions, and the I4C-launched e-Zero FIR in Delhi offers rapid incident reporting without jurisdictional hurdles.[37]

Finally, existing regulations already aim to tackle issues of impersonation, spam, and fraud over telecom and OTT channels, via both the Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2018) and the IT Act. These rules require telecommunications providers to scrub headers, block unregistered telemarketers, and penalise fraudulent communication. The IT Act also prescribes offences such as cheating by personation and identity theft for OTT platforms under Sections 66C and 66D.[38]

[33] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146786

[34] https://timesofindia.indiatimes.com/business/india-business/airtels-ai-powered-fraud-detection-system-blocked-1-8-lakh-malicious-links-shielded-5-4-million-users-in-telangana/articleshow/121783678.cms

[35] https://blog.google/intl/en-in/company-news/googles-safety-charter-for-indias-ai-led-transformation/

[36] https://economictimes.indiatimes.com/news/economy/policy/rbi-know-your-customer-kyc-rules-customer-onboarding-aadhaar-biometric-norms/articleshow/121797850.cms

[37] https://timesofindia.indiatimes.com/business/cybersecurity/e-zero-fir-initiative-launched-to-fast-track-cyber-fraud-cases-pilot-begins-in-delhi/articleshow/121379802.cms

[38] https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2080641

India's policy landscape already includes a mix of institutional mechanisms, technological solutions, and legal safeguards that aim to combat aforementioned fraud. The real challenge, however, lies in strengthening, effectively implementing, and cohesively integrating these efforts, across fragmented telecom vendors, financial institutions, law enforcement agencies, and both traditional and OTT communication platforms.

Rather than addressing these coordination gaps, the Draft Amendment Rules introduce overlapping regulatory regimes. Instead of fostering an interoperable, collaborative framework, they risk layering over-compliance burdens on already-regulated entities. This structural friction may undermine user trust, stifle innovation, and increase operational complexity. What is needed is regulatory convergence and targeted enforcement, not duplication and diffusion of accountability. The Draft Amendments Rules risk doing the latter, at the cost of former.

2.6. Finding: The Draft Amendment Rules are unlikely to achieve the desired objectives

3. What are the impacts of Draft Amendment Rules on businesses?

3.1. Cost of MNV framework

3.1.1. Regulatory cost

The proposed MNV framework introduces a recurring financial burden on TIUEs in the form of per-request validation charges–₹1.50 for government-directed mandatory checks and ₹3 for voluntary verification. Though the per-unit cost appears modest, scaling it to large platforms reveals its significance.

For example, Zomato, with approximately 30.7 million weekly active users nationwide,[39] would have around 4.39 million daily active users. Assuming 10 percent will require validation, which means 439,000 daily validation requests. **At a rate ₹1.5 per verification, this translates to ₹658,500 per day, which can mean ₹240.35 million (₹24.035 crores) annually**. At higher compliance thresholds of 20% and 30%, these costs would proportionally rise to ₹480.71 million (₹48.07) crores and ₹721.06 million (₹72.10 crores) respectively.

Uber India, with 33.6 million monthly active users, would have approximately 1.12 million daily active users.[40] **Assuming 10 percent require validation, that's 112,000 daily validation requests and at a rate ₹1.5 per verification, this translates to ₹168,000 per day, or ₹61.32 (₹6.13 crores) million annually.** At higher compliance thresholds of 20% and 30%, these costs would proportionally rise to ₹122.64 million (₹12.26 crores) and ₹183.96 million (₹18.4 crores) per year, respectively.

PhonePe, has 600 million registered users,[41] and 281.96 million transactions daily in the month of June 2025.[42] **At 10% validations (around 28 million), it could face ₹15,330 million annually (₹1,533 Cr).** For 20% and 30% validations it translates to ₹30,660 million (₹3,366 Cr) and ₹45,990 million (₹4,599 Cr) annually respectively.

[39] https://www.moneycontrol.com/news/business/startup/blinkit-s-weekly-user-base-of-over-30-million-within-striking-distance-of-zomato-widens-lead-over-instamart-and-zepto-clsa-13099185.html

[40] https://www.equentis.com/blog/14-cabs-31-autorickshaws-56-bike-taxis-is-rapido-set-to-outpace-ola-uber/

[41] https://www.phonepe.com/press/phonepe-crosses-600-million-registered-users/

[42] https://www.rbi.org.in/Scripts/Statistics.aspx

Further, over 30,000 small and medium retail brands cater to nearly 1.15 billion Indians.[43] Assuming that among these MSMEs, 51% handle fewer than 1,000 orders monthly, while 25% manage 1,000–10,000, and 6.6% process over 10,000.[44] This translates into a collective volume of over 82 million orders per month. Further, consumers use their mobile numbers for such orders to keep a track and enable communication. If MNV validations are mandated, **even at 10% compliance, these businesses would collectively need to validate 8.25 million orders monthly, costing ₹1.24 crore per month, or ₹14.85 crore annually at ₹1.5 per validation.** At 30% compliance, the cost could surge to over ₹44 crore a year - a significant burden for small businesses. It is important to note that voluntary validation at ₹3 per request doubles these figures, pushing churn-sensitive platforms toward prohibitively high compliance bills.

The Indian startup failure rate is exceptionally high. About 90 % of startups fail within the first five years, with regulatory compliance cited as a critical contributing factor, accounting for about 10–20 % of operational expenses for startups, significantly eroding capital available for innovation and scaling.[45] The requirements for MNV and IMEI verifications would lead to startups diverting a large chunk of early-stage capital towards associated compliances. Further, many startups are using SIM binding methods which are OTP-less login aimed at enhancing secure access. These entities might also be caught in this compliance and the solution will become less feasible, which in turn will increase security threats, reducing innovation.[46]

If the regulator limits obligations to big TIUEs, it might be assumed that those players can internalise costs. However, this imposes significant opportunity costs. First, the opportunity cost–even when large TIUEs absorb these expenses and divert the funds towards compliances. This might eat away from the funds earmarked for innovation, research and development, improving service quality, or enhancing access These firms may cut back on innovation investments as compliance burdens grow, reducing their collaborations or support for startups.

Second, there are waterbed effects too. When large TIUEs internalise costs, these indirect burdens can often cascade into other areas. TIUEs provide adjacent digital services such as cloud hosting, data storage, and advertising platforms,[47] and are highly likely to raise their pricing structures to offset rising compliance costs. This price escalation inevitably ripples through the digital value chain, significantly increasing operational costs for downstream service providers and small and medium businesses, including startups, reliant on these platforms. Further, it may not be an easy task to design an intelligible and logical rationale for differentiating big from small TIEUs. Will the basis of differentiation be total users, active users, revenue generated by TIEUs, profit made by TIEUs, utility of unique mobile numbers for logging in and communication by TIEUs, fraud attempts at TIEUs, or measures put in place by TIEUs to address scam, spam, and fraud callers? Some TIEUs with large user base may not be profit making and it may not make sense to ask them to internalise the cost of telecom cyber security. At the same time, some niche TIEUs with smaller active user base

[43] https://www.financialexpress.com/business/sme-msme-eodb-over-30000-small-medium-brands-in-retail-catering-to-80-of-indias-population-cait-2494199/

[44] https://cxotoday.com/press-release/get-the-msme-perspective-msme-highlight-their-biggest-pain-points-and-preferences-reveals-borzo-data/

[45] https://www.linkedin.com/pulse/why-indian-startups-fail-due-non-legalregulatory-kappillil-anilkumar-ziapc and https://bfsi.economictimes.indiatimes.com/news/fintech/how-much-do-indian-fintechs-spend-on-compliance/110858284

[46] https://economictimes.indiatimes.com/markets/options/sim-binding-in-trading-apps-how-otp-less-login-enhances-secure-trading-access/articleshow/121288349.cms

[47] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

might be profit making. The guidance provided by the DPDP Act on Significant Data Fiduciary may not be of much use in this case. Ultimately, these accumulated costs can translate into increased prices for end consumers.

3.1.2. Staff/ time cost

Beyond direct per-query fees, the Draft Amendment Rules can impose substantial operational burdens on TIUEs that extend well beyond per-query verification fees. Managing the MNV system will require API integration, real-time monitoring of verification requests, handling failures, managing disputes, and coordinating with multiple government platforms. For small and mid-sized firms, this translates into hiring or reallocating staff-including compliance officers and technical personnel. These are recurring operational expenses that divert resources from core product development, innovation, or service delivery to compliance and potentially unproductive uses –especially for startups or lean firms operating on tight margins.

This is also separate from the time spent understanding the mechanism, responding to verification failures, and ensuring compliance with evolving regulatory protocols. For startups, these obligations divert scarce human resources away from core product development and innovation.

3.1.3. Substantive cost

The proposed requirement will also demand significant investment in digital infrastructure. Firms will have to build and maintain secure API integrations, ensure latency and transaction integrity, develop real-time dashboards for query monitoring, and maintain audit trails. These technical requirements are capital-intensive. Moreover, since the MNV platform will depend on coordination with evolving government platforms, firms will also have to budget for continuous updates, platform alignment, and periodic security enhancements. These costs are particularly burdensome for smaller players who lack economies of scale or in-house engineering bandwidth.

3.2. Cost of IMEI verification framework

3.2.1. Regulatory costs

Rule 8 mandates ₹10 per verification request for resale device IMEI validation before each sale. With rising mobile penetration and frequent device upgrades, India has emerged as third-largest markets for refurbished and resold smartphones.[48] This includes major players like Cashify, Amazon Renewed, Flipkart's 2GUD, OLX, and a large number of informal vendors participating in the ecosystem.

For users and small businesses engaged in purchasing and selling second-hand mobile phones that is a common practice due to affordability—there is now an additional burden of IMEI verification. In 2024, India's organised secondary smartphone market, **i**ncluding refurbished and used, grew by about 10%, with 20 million used smartphones traded.[49] **At ₹10 per verification, this translates to ₹200 million (₹20 crore) in annual compliance costs** in just the formal segment. Considering that 85% of this market remains unorganised,[50] the real impact is likely to be far greater–potentially affecting tens of millions of users. Such provisions are likely to hit small businesses and poorer consumers the hardest, many of whom depend on

[48] https://www.ccsinsight.com/blog/the-rise-of-indias-second-hand-smartphone-market/

[49] https://economictimes.indiatimes.com/industry/cons-products/electronics/second-hand-becomes-first-choice-as-indians-go-bargain-hunting-for-5g-devices/articleshow/117610233.cms

[50] https://www.ccsinsight.com/blog/the-rise-of-indias-second-hand-smartphone-market/

this market for affordable access to smartphones, flexible financing, and better value for money.
3.2.2. Staff/ time cost IMEI verification will also impose operational burdens on vendors, many of whom currently operate offline, cash-based businesses. They would need staff to handle verification workflows, interface with the database, maintain records, and audit rejections or errors. Informal micro-entrepreneurs may struggle to hire or train personnel for these tasks, increasing informal costs and require them to divert time from business operations to compliance management.
3.2.3. Substantive cost Beyond per-transaction charges, sellers (formal or informal) will have to upgrade systems or establish manual procedures to connect to the validation portal. For the organised sector, this may involve API integration, dashboard creation, merchant dashboards, and error-handling modules. For the unorganised sector, it may require manual processes or reliance on third-party providers–introducing delays, uncertainties, and inconsistent compliance. These systemic costs may divert working capital and reduce efficiency in what is already a low-margin business.
3.3. Cost of data sharing requirements
3.3.1. Staff/ time cost To operationalise these data-sharing protocols, TIUEs will have to assign teams to manage intake of legal directives, oversee log submission, respond to government requests, handle exception or dispute cases, and ensure regulatory compliance. These roles are novel to many firms and require continuous training and oversight.
3.3.2. Substantive cost Draft Rule 3 extends the requirement of collection, sharing and analysis of data to TIUEs. Implementing this would require creating backend infrastructure, storage systems, secure channels, and audit mechanisms to meet unspecified data formats or deadlines. Costs may include development of logging modules, encryption, secure servers, and retention management–none of which existing platforms may have pre-built without costly upgrades.
3.4. Benefits for businesses If implemented effectively, the Draft Amendment Rules may lead to some benefits for businesses such as reduction in scam calls, fewer cases of stolen or cloned identifiers, etc. However, these potential benefits may come at disproportionately high costs due to significant operational impacts, leaving businesses minimal returns and limiting their ability to innovate.
3.5. Finding: Service Providers, especially MSMEs, and startups are likely to be significantly adversely impacted due to Draft Amendment Rules
4. What are the impacts of Draft Amendment Rules on consumers?
4.1. Costs of MNV mechanism
4.1.1. Loss of access The impact of the proposed telecom verification mandates on consumers is likely to be both immediate and far-reaching, particularly for digitally marginalised groups. The proposed

mechanism could disrupt the current ease of access to digital services by introducing new layers of identity authentication and device verification. While the Draft Amendment Rules aim to enhance telecom security, they fail to account for India's complex realities of mobile ownership, shared phone usage, and digital literacy gaps. As a result, millions of users such as women, elderly, children, low-income families, and rural residents, may find themselves either excluded from essential digital services or burdened by new financial and procedural requirements.

Indian families commonly share a mobile number or children use parent's number for essential activities like education apps. Approximately 85.5 per cent of households possessed at least one smartphone.[51] In many households, economic constraints mean only one smartphone is purchased and shared among all members, and the majority of Indian women use shared devices.[52] Similarly, there could be instances wherein for bank accounts or financial services availed by senior citizens, female members and children of the households, mobile number of a male member of the household is registered.

As per the recent Global Findex survey report 2025, even when mobile phones are distributed to women under a govt programme in India, nearly 40 percent of women had lost control over their devices within a month after distribution, despite 98 percent of women having received the phones, highlighting the gendered dimensions of device access and control.[53]

India's digital access has been premised on mobile-first connectivity, with over 1.14 billion active mobile connections users.[54] However, mobile ownership is not synonymous with mobile usage. Data indicate that in many households, especially rural or low-income ones, only one member owns a mobile phone while others use it in a shared fashion.[55] This is especially true for women, children, and elderly family members,[56] many of whom rely on a their father's, husband's or son's phone to access services like digital payments, telemedicine, online learning, and food delivery. Indeed, in India, having a family member with an account is the most common reason adults without accounts give for not having their own, underscoring the prevalence of shared or proxy usage in digital access.

According to national surveys, around 76.3% of rural women aged 15 and above use mobile phones, but just 48.4% own one–which means roughly one in four female users does not have personal ownership of the device they operate.[57] In a survey, among women, roughly 80 per cent reported using a phone, but only about half owned one—suggesting that around 215 million women are likely secondary users. Similarly, most of the 165 million children aged 5–14 who use mobile phones do so on a shared basis, contributing an estimated 149 million to the count of non-owning users. Among elderly Indians, who face higher barriers to digital access, nearly 28 million phone users are estimated to depend on family-owned devices.[58] In total, nearly 400 million Indians—primarily women, children, and older adults—may be using phones that they do not personally own, highlighting a critical dimension.

[51] https://www.communicationstoday.co.in/85-5-indian-households-posses-at-least-one-smartphone-mospi-survey/

[52] https://ifmrlead.org/whose-phone-is-it-anyway-women-users-india/

[53] https://www.worldbank.org/en/publication/globalfindex

[54] https://dot.gov.in/sites/default/files/Annual%20Report%20English%20Dot%202024.pdf

[55] https://www.dataforindia.com/comm-tech/

[56] https://ifmrlead.org/whose-phone-is-it-anyway-women-users-india/

[57] https://www.livemint.com/economy/upi-usage-india-rural-women-digital-access-mobile-phone-ownership-rural-women-digital-divide-india-rural-internet-usage-11749021032545.html

[58] https://www.dataforindia.com/comm-tech/

Under the proposed MNV system, if a user logs in using their name but the SIM is registered to another person—say, a father or spouse or son (in case of seniors)—the mismatch will likely lead to verification failure and consequent denial of service. Thus, the Draft Amendment Rules risk severing digital access for millions of "secondary users" who are legitimate users but not legal subscribers.

Further exclusion may occur if TIUEs migrate to email-based authentication to avoid MNV charges. But email adoption in India is neither universal nor uniform. As discussed above, a significant portion of the digitally connected population lacks an active email address or the skills to operate one. For such users, the shift from mobile to email as a primary verification mode may result in the loss of access to services.

4.1.2. Cost pass-on

If the cost of compliance is passed on by service providers to consumers, even partially, users face rising service prices. A platform like Uber or Zomato or PhonePe, processing millions of authentications per month, may factor these into pricing structures, subtly increasing the cost of access across urban and rural markets.

Even a seemingly nominal fee can compound quickly for end-users. For instance, if each login incurs a charge of ₹1.50 and a typical user log in at least three times a day across different platforms, the daily cost would be ₹4.50–amounting to roughly ₹135 per month. If a typical user logs in five times per day across different platforms, the daily cost becomes ₹7.50, amounting to ₹225 per month. For users logging in more frequently, say seven times a day, the monthly expense rises to ₹315. For TIUEs opting into voluntary validations, priced at ₹3 per validation, the cost effectively doubles for consumers, pushing the monthly burden to ₹450 or more for high-usage users.

This figure is comparable to the price of a basic subscription plan for a digital service–whether educational, financial, or skill-building.[59] At scale, the economic impact becomes even more pronounced. With over 800 million mobile phone users in India, and assuming just 400 million interact with services offered by TIUEs, even if 10% of them (40 million users) are subject to verification costs of ₹135 per month, the **total consumer costs could add up to ₹540 crore per month--or over ₹6,480 crore annually.** For many, this cost competes with essentials. For context, data from the Periodic Labour Force Survey (PLFS) 2023–24[60] reveals that the bottom 10% of earners in India have a monthly income of just ₹3,900. A validation related **cost of ₹135 per month would amount to nearly 3.5% of their total income**—and could rise to over 10% in high-use or voluntary verification cases. In effect, this verification cost could represent a significant opportunity cost, particularly for low-income users who may be forced to reduce their usage or cancel subscriptions to other platforms that offer tangible value.

4.2. Costs of IMEI mechanism

4.2.1. Loss of access

This cost being passed onto consumers' pressure will also exacerbate existing divides. According to PLFS data for 2023–24, the bottom 10% of earners in India brought home just ₹3,900 per month.[61] Given that such poorer households operate on per-day expenditures, incurring ₹10 per resale amounts to an insurable economic barrier, and repeated sales would

[59] https://www.proskills.in/pricing

[60] https://www.competitiveness.in/wp-content/uploads/2025/04/Report_Labour_markets_Income_Inequality_in_India_Web_version.pdf

[61] https://www.competitiveness.in/wp-content/uploads/2025/04/Report_Labour_markets_Income_Inequality_in_India_Web_version.pdf

magnify that burden. It also disincentivises sellers in the unorganised sector, who cannot easily absorb or pass on the cost. That erosion of affordability is projected to widen existing digital divide between richer and poorer households, limiting the ability of low-income users to participate fully in the digital economy. As costs rise, many may delay or forgo upgrading to smartphones that support critical digital services, further entrenching exclusion from education, healthcare, financial services, and employment opportunities. Moreover, the shrinking presence of informal sellers, who often serve as vital access points in underserved areas, could reduce the availability of affordable devices, leaving communities disconnected. Without targeted interventions or subsidies to offset these costs, the intended goals of digital inclusion risk being undermined by the very policies designed to safeguard the ecosystem.

4.2.2. Cost pass-on

Even a one-time ₹10 IMEI verification fee can represent a meaningful cost when passed onto the consumer segment of used phones. Refurbished smartphones on platforms like OLX or Cashify often retail in the range of ₹2,500–₹6,000, and for a buyer at the lower strata of the income pyramid—earning ₹3,900 per month on average—this single fee amounts to over 0.25% of their monthly income. For users who buy or sell devices more than once a year, or for micro-entrepreneurs trading used phones for livelihood, this cost could accumulate further. As with MNV fees, this IMEI cost represents an opportunity cost, forcing economically constrained users to choose between maintaining affordable device access and continuing their engagement with value-added digital services. In doing so, it risks further eroding the affordability and inclusivity of India's mobile-first digital ecosystem.

4.3. Costs of data sharing requirements

4.3.1. Exacerbated privacy and data protection risks

From the consumer's perspective, expanded data sharing requirements under Rule 3 pose significant risks to privacy and digital security. As TIUEs collect, store, and transmit personal information, the likelihood of data breaches or unauthorised access grows. This can potentially expose sensitive identity details to malicious actors. Consumers may face increased risks of identity theft, fraud, or misuse of their personal data without their consent or knowledge. Consequently, the Draft Amendment Rules risk aggravating problems identified in the intended objectives, instead of resolving it.

Stakeholders have pointed to the lack of adequate safeguards such as clearly defined procedures, explicit consent protocols, or strict limitations on the use and sharing of personal data collected through verification platforms. Without these safeguards, there is a risk of conflict with privacy principles enshrined in the Digital Personal Data Protection Act, especially concerning consent, purpose limitation, and data minimisation.[62]

The complexity of these data flows and the involvement of multiple intermediaries also reduce transparency, making it harder for consumers to know who holds their information and how it is used. This erosion of control over personal data undermines trust in digital platforms and identity systems, discouraging users, particularly vulnerable groups such as women, elderly, and low-income individuals from fully engaging with digital services.

Additionally, the fear of privacy violations may lead consumers to limit their use of essential services like digital payments, telemedicine, or online education, thereby deepening existing digital divides. Without robust privacy protections and clear accountability mechanisms,

[62] https://www.youtube.com/watch?v=MzHNeeYSPbQ

consumers may have to bear the brunt of systemic risks stemming from mandatory data sharing.

4.4. Benefits for consumers

If implemented effectively, the Draft Amendment Rules may lead to some benefits for consumers by preventing certain types of telecom-related frauds, like SIM-based identity theft and cloning. However, the gains may likely be narrow and overshadowed by cost implications and barriers to access, leaving consumers minimal utility.

4.5. Finding: Consumers are likely to be significantly adversely impacted due to Draft Amendment Rules

5. What are the impacts of Draft Amendment Rules on digital market growth?

5.1. Slowdown in the growth rate of digital market

The proposed amendments may pose a threat to India's digital economic ambitions by introducing structural inefficiencies and exclusionary costs. These include financial and operational burdens on each of these entities compounded at a large scale, distort competition in the market, negatively impact the growth and dynamism of telecom markets, and limit consumer access. For instance, in 2022-23 India's digital economy accounted for 11.74% of the GDP (INR 31.64 lakh crore or USD 402 billion),[63] and is expected to rise to 13.42% by 2024-25.[64] Assuming that the growth rate slows by 10% due to increased costs, compliance friction, and restricted market access, this could have translated into a **loss of over ₹2.5 lakh crore** in economic activity by FY2025 alone.

The impact would be more impactful for startups and new entrants. For instance, over 159,000 startups have been recognised under the Startup India initiative by 2025.[65] In 2023, the number was 117,254.[66] The corresponding figures on direct jobs are 1.7 million. If this momentum is slowed by even 10%, approximately **4,000–5,000 potential startups may be excluded** from the market, **risking a loss of nearly 150,000–200,000 direct jobs**, and significantly higher indirect employment impact through service networks and vendor linkages.

Similarly, in the same period (march 2023 to march 2025), the wireless (mobile) subscriber base grew from 1,143.93 millions[67] to 1,163.76 millions,[68] registering a net addition of 19.8 million users. This corresponds to a total growth of approximately 1.73% over the two-year period. A 10% decline in new user additions would mean roughly 2 million fewer consumers gaining access to mobile and internet services over a two-year span.

For India, which is still attempting to bridge the digital divide, especially in rural and aspirational districts, this slowdown would disproportionately affect first-time users, who often rely on low-cost services. In effect, this would deepen digital exclusion for those who are at the very edge of inclusion.

When considering the combined costs of both MNV and IMEI validation fees, these charges act as a persistent micro-tax on digital access. For lean startups and smaller TIUEs, these fees

[63] https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2097125
[64] https://indbiz.gov.in/indias-digital-economy-to-outpace-national-growth-by-2030/
[65] https://www.orfonline.org/research/reflections-on-the-first-decade-of-startup-india
[66] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2002100
[67] https://www.trai.gov.in/sites/default/files/2024-09/16th.pdf
[68] https://www.trai.gov.in/sites/default/files/2025-05/PR_No.35of2025_0.pdf

erode margins and viability by diverting scarce resources away from innovation, product development, and customer service improvements. Ultimately, this cumulative burden threatens to stifle competition, reduce consumer choice, and slow India's progress toward a more inclusive digital economy.

5.2. Lack of access to potential consumers

As of March 2025, India's wireless subscriber base stood at 1.16 billion, with a net addition of 19.8 million users over the preceding two years. However, this growth rate has decelerated, with a 0.15% year-over-year decline in total wireless subscribers, indicating a slowdown in new user acquisition.[69] The introduction of additional costs for device resale and MNV verification will disproportionately affect first-time users, who often rely on affordable second-hand smartphones. These users, predominantly from rural and aspirational districts, are particularly sensitive to price increases.

5.3. Entry barriers to potential service providers

The rapid expansion of India's startup landscape has also introduced a phenomenon often referred to as "startup dwarfism," where a large number of small-scale startups struggle to scale effectively. This will be at risk of deepening due to the financial and operational burden imposed by the Draft Amendment Rules. Many new potential entrants in the startup ecosystem may feel disincentivised and demotivated due to proposed compliance burden. This trend will be at risk of deepening due to the financial and operational burden imposed by the Draft Amendment Rules. The cumulative effect of the compliance threatens to divert scarce resources away from core product development, market expansion, and research & development, thereby hindering the ability of nascent ventures to achieve sustainable growth and compete effectively in the broader market.

5.4. Finding: The digital markets are likely to be significantly adversely impacted due to draft amendment Rules

6. Recommendations

6.1. The requirement and scope of Draft Amendment Rules need to be revisited

The net impact (benefits minus costs) of the Draft Amendment Rules on key stakeholders such as businesses, consumers and digital markets, is likely to be significantly negative. It introduces critical compliance obligations without a clearly defined legal foundation. Notably, as highlighted above, the creation of a new category of regulated entities in TIUEs, appears to lack statutory backing under the Telecommunications Act. This raises serious concerns about regulatory overreach, particularly when fundamental obligations are being imposed on entities that are not traditionally governed under the Act. These must be introduced through primary legislation such as the forthcoming Digital India Act, not through subordinate rule-making.

Moreover, the draft conflates identification and authentication–two distinct processes with different use-cases, security implications, and regulatory needs. A clear demarcation is essential to ensure that compliance burdens are proportionate to the risk. Without legal clarity and narrowly tailored obligations, the proposed framework risks inviting constitutional challenges and inconsistent enforcement. Until the appropriate legislative architecture is in

[69] https://www.lightreading.com/regulatory-politics/subscriber-growth-stagnates-but-data-boom-continues-in-india---trai-report

place, the scope of the telecom rules should be limited to entities that are already explicitly governed under the Act.

6.2. The government should rather focus on strengthening the ongoing initiatives aimed at addressing the issue of telecom cybersecurity and avoid inconsistent approaches

India's digital landscape is already governed by multiple sector-specific cybersecurity frameworks—including the CERT-In guidelines, the RBI's mandates for financial institutions, and various data protection norms under the Digital Personal Data Protection Act. Overlaying an additional compliance regime for telecom cybersecurity, without aligning it with existing standards, risks creating an incoherent and contradictory regulatory environment.

Rather than expanding new compliance requirements through the telecom Act alone, there is a pressing need to harmonise efforts across sectors, and focus on effective implementation. Establishing an inter-ministerial coordination mechanism, bringing together the DoT, MeitY, RBI, and other key regulators, along with consumer groups (which can act as eyes and ears of regulators on the ground) would ensure a unified approach to digital risk management. This would reduce duplicative obligations, promote predictability for service providers, and encourage meaningful compliance without regulatory fatigue.

The design and implementation of any new rule must also be grounded in evidence. A phased rollout, beginning with sandbox environments, could help test the technical feasibility and societal impact of mechanisms like MNV or IMEI authentication. Such pilots would not only show potential pitfalls but also allow the Rules to be iteratively improved based on real-world feedback, making regulation more responsive and robust.

6.3. The government should undertake a comprehensive Regulatory Impact Assessment and take into account costs on SMBs and consumers before issuing new requirements

To avoid the unintended effects inhibiting market competition, raising the bar for small and medium business, and preventing consumers from falling into the trap of digital divide, the government should consider undertaking comprehensive Regulatory Impact Assessment before issuing any new requirements. It should essentially consider differentiated compliance models depending on the risks and scale. Privacy impact assessments should also be mandated to ensure that data handling remains aligned with DPDPA principles of consent, purpose limitation, and data minimization. These adjustments will help ensure that India's digital growth remains inclusive, innovation-friendly, and legally sound.

About CUTS

Consumer Unity & Trust Society (CUTS)[70] is an independent, nonpartisan, and non-profit policy think and action tank that has been working towards enhancing the regulatory environment through evidence-based policy and governance-related interventions across various sectors and boundaries. In its 40 years of operation, CUTS has come a long way from being a grassroots consumer centric organisation headquartered in Jaipur, having centres in Delhi,[71] and Kolkata,[72] to now opening overseas Resource Centres in Vietnam,[73] Kenya,[74] Zambia,[75] Ghana,[76] Switzerland,[77] and in the United States of America.[78] CUTS has been actively representing consumers' interest before different state governments and central government ministries through various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE),[79] Centre for Consumer Action, Research & Training (CART),[80] Centre for Human Development (CHD)[81] and Centre for Competition, Investment & Economic Regulation (CCIER).[82]

CUTS works on various issues to foster an inclusive digital economy,[83] including issues of multi-party privacy,[84] data localisation,[85] and other general issues of data protection,[86] and encryption.[87] CUTS also works with various ministries and government departments for advocacy efforts[88] on issues within digital economy, more recently on the draft digital personal data protection rules,[89] report on AI governance,[90] draft broadcasting bill,[91] draft guidelines for prevention and regulation of dark patterns,[92] draft registration of consumer organisations (amendment) regulations[93], draft telecommunication mobile number portability regulations,[94]

---

[70] CUTS International – Consumer Unity & Trust Society (cuts-international.org)
[71] CUTS Delhi Resource Centre
[72] CUTS CRC
[73] CUTS HRC
[74] CUTS Nairobi
[75] CUTS Lusaka
[76] CUTS Accra
[77] CUTS Geneva
[78] CUTS WDC
[79] CUTS Citee
[80] CUTS Cart
[81] CUTS CHD
[82] CUTS CCIER
[83] Inclusive Digital Economy - Ccier (cuts-ccier.org)
[84] "My data or yours?" Unravelling Multi-Party Privacy (MPP) among Consumers of Digital Credit in India
[85] Understanding the Impact of Data Localization on Digital Trade - ccier
[86] https://cuts-ccier.org/cdpp/
[87] Understanding Consumers' Perspective on Encryption - ccier
[88] Advocacy - Ccier
[89] https://cuts-ccier.org/pdf/comments-on-the-draft-digital-personal-data-protection-rules-2025.pdf
[90] https://cuts-ccier.org/pdf/comments-on-the-subcommittees-report-on-AI-governance-and-guidelines-development.pdf
[91] CUTS Comments on Broadcasting Services (Regulation) Bill, 2023
[92] CUTS Comments on Draft Guidelines on Prevention and Regulation of Dark Patterns
[93] CUTS comments on TRAI Consultation Paper on the draft Registration of Consumer Organisations (Amendment) Regulations, 2023
[94] CUTS comments on Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023

digital competition,[95] competitive neutrality,[96] among others.

CUTS International has significant experience and expertise in conducting RIAs, generating awareness, and conducting capacity building programmes on RIA for government and other stakeholders. CUTS has been helping the government build internal capacity on the Regulatory Impact Assessment (RIA) framework, and has conducted training programmes for regulators in the financial and communications sectors in this regard. [97]

[95] Comments By CUTS International On Draft Digital Competition Bill, 2024

[96] Promoting Competitive Neutrality in Government Using Advocacy

[97] https://cuts-ccier.org/regulatory-impact-assessment/

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).