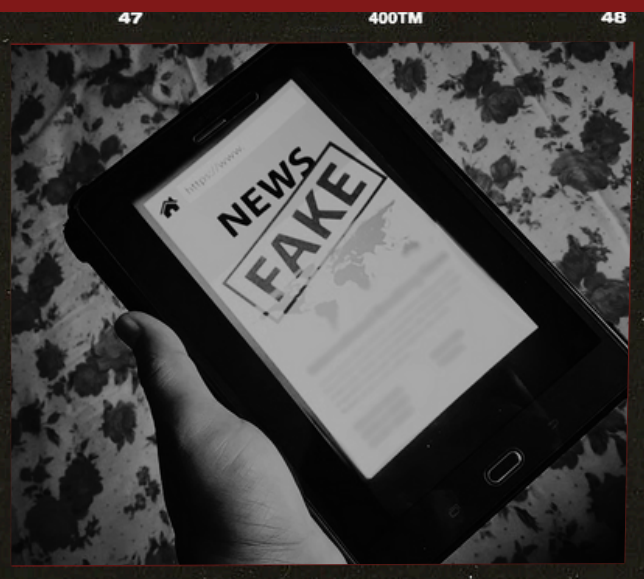
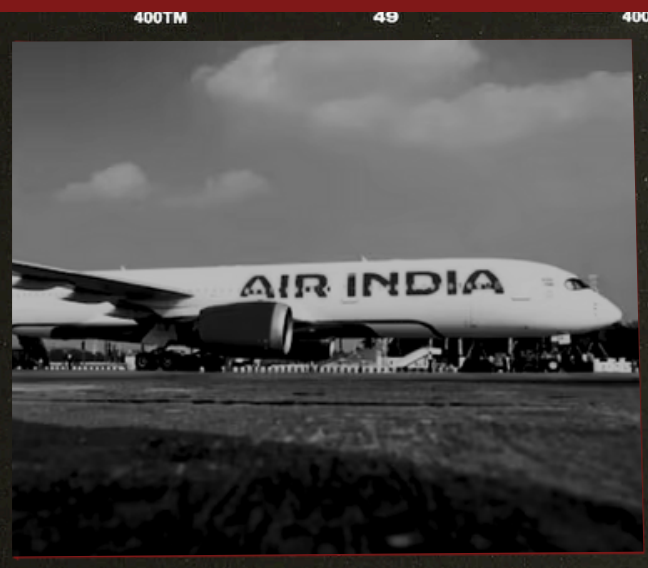
Kautilya Society, NLUO

PUBLIC POLICY POST

Monthly newsletter on recent legislations and public policy updates

JUNE 2025





Policy Updates from June

S.No.	Topic
1.	SEZ Amendments 2025: Enabling India's Chip Ambitions
2.	Maharashtra’s Public Security Bill: A Step Forward or a Threat to Civil Liberties
3.	The Aftermath of Ahmedabad: Legal Support Helpdesk Formed for the Families of the Ahmedabad Plane Crash Victims
4.	A cautionary approach to the draft Karnataka Misinformation and Fake News (Prohibition) Bill, 2025
5.	Cyber Security Reinforced: Draft Amendments to Telecom Cyber Security Rules Presented

SEZ Amendments 2025: Enabling India's Chip Ambitions

- Ishaani Garg

India's semiconductor ambitions received a significant policy update on June 3, 2025, when the Ministry of Commerce and Industry announced the Special Economic Zones (Amendment) Rules, 2025. The amendments to the Special Economic Zones Act, 2006, and the Special Economic Zones Rules, 2006, represent a strategic shift from the old "Assemble in India" model towards strengthening domestic semiconductor manufacturing capabilities.

Key Regulatory Changes

The most important change is perhaps amending Rule 5 of the SEZ Rules, 2006, which reduces the minimum contiguous land requirement for SEZs dedicated to semiconductor or electronics component manufacturing from 50 hectares to just 10 hectares. In the past, SEZs were only able to exist in isolated locations with areas that were large and suitable to accommodate the 50-hectare requirement. Manufacturers now simply require 10 hectares and can therefore establish themselves in the urban and semi-urban regions where it is easy to get skilled labour, infrastructure and access to the market.

The amendment introduces a broad definition of what constitutes "electronic components", encompassing display modules, camera modules, printed circuit boards, lithium-ion cells, and even wearable technology components. Since India has found its place in the international supply chain of wearable technology and IoT devices, it is necessary to have a clear category of regulations so that new products are not caught in the legal quagmire of definitions that might cause issues during approvals or in the tax field.

Rule 53 now permits goods received and supplied free of cost to be included with Net Foreign Exchange calculations. This aligns Indian practices with international customs valuation norms, ensuring that the semiconductor service providers receive proper credit for their export contributions.

Earlier the capital goods and raw materials used for export or supply to the Domestic Tariff Area (DTA) had to be procured directly from the manufacturer. The amendment to Rule 18 removes this restriction, thereby allowing SEZ units greater flexibility in sourcing. The earlier framework introduced unnecessary rigidity, undermining competitiveness. By removing these restrictions, the amendment enables greater flexibility and responsiveness, which is key for successful participation in international supply chains.

In addition, Rule 7 has been amended to allow the board of approval to relax land certification norms, allowing developers to proceed without encumbrance-free land certificates, when land is mortgaged or leased to government entities. However, this relaxation comes with appropriate safeguards like the requirement of clear documentation of why developers cannot furnish encumbrance-free certificates, ensuring that due diligence is maintained while removing unnecessary bureaucratic hurdles.

Strategic Implications and Challenges

These amendments align with India's post-pandemic industrial strategy, which seeks to diversify global supply chains and reduce reliance on foreign chipmakers. The semiconductor shortage of 2020-2021 demonstrated that chip manufacturing is of strategic importance. The global semiconductor ecosystem remains highly concentrated, with Taiwan's TSMC alone accounting for over 50% of global chip fabrication and nearly 90% of advanced-node chips. India's push to enter this space is not just economic, it is a strategic necessity to reduce external dependency on a few manufacturing hubs vulnerable to geopolitical risks. The step towards these amendments also indicates India's strategic shift towards recognition of the manufacturing sector as technology-intensive. Modern manufacturing requires skilled personnel, advanced infrastructure, and robust regulatory systems to keep pace with the rapid evolution of technology.

Although these reforms are positive, significant challenges remain. The semiconductor manufacturing establishments face significant gaps in infrastructure, power, water, logistics and specialised utilities not yet available nationwide. Another critical issue is the shortage of a skilled workforce, particularly in chip design, fabrication, and testing. This issue is not unique to India: according to Deloitte and SEMI (previously Semiconductor Equipment and Materials International), the global semiconductor industry is projected to face a shortage of over 1 million skilled professionals by 2030. For India, the challenge is more acute given the nascent nature of its fabrication ecosystem and the absence of large-scale chip design and process.

These amendments raise important questions about federal coordination and trade compliance. While SEZs are governed by central legislation, their implementation depends on State-level functions such

as land acquisition, utility provisioning, and environmental clearances. The relaxation of encumbrance-free land certification reflects the challenges States face due to fragmented land ownership and complex title systems. The rules must also be assessed in light of India's WTO obligations, particularly under the Agreement on Subsidies and Countervailing Measures, which prohibits export-contingent incentives. India's 2019 WTO loss over several export promotion schemes increases the legal sensitivity around SEZ-linked incentives, especially those tied directly or indirectly to export performance or domestic content requirements.

Looking Ahead

With India's semiconductor market projected to grow from USD 53.2 billion in 2024 to USD 161 billion by 2033, the SEZ (Amendment) Rules, 2025, arrive at a critical juncture. By aligning regulatory infrastructure with the operational needs of semiconductor manufacturing, the amendments create clearer ground for long-term investment in advanced technology sectors.

Yet India's semiconductor success depends on three fundamental pillars: reliable power infrastructure, skilled workforce development, and efficient regulatory coordination between central and state authorities. Future policy attention may also need to focus on integrating SEZ reforms with broader industrial programs such as the India Semiconductor Mission and the Production Linked Incentive (PLI) schemes, to ensure consistency and reduce overlap.

For investors, developers, and regulatory actors, the task ahead is not only to leverage these relaxed norms but to ensure that India's entry into high-tech manufacturing is competitive, sustainable, and institutionally grounded.

Maharastra Public Security Bill: A Step Forward or a Threat to Civil Liberties?

-Arunima

Overview of the Bill

The Maharashtra Special Public Security Bill, 2024 commonly referred to as the '*Urban Naxal*' bill, was tabled back in July 2024 with the intention of countering left-wing extremist or Naxal-affiliated activities in urban areas. It sparked widespread controversy due to its initial, blanket scope legislation, which allowed action against both individuals and organizations labelled by the state as engaging in "unlawful activities." Owing to the widespread pushback from various groups, the state legislature's Joint Select Committee ("JSC") undertook substantial revisions in June 2025.

The updated draft, expected to be tabled during the Monsoon Session, introduces crucial amendments such as the narrowing of its scope to organizations only. This means that the revised bill targets unlawful activities solely by "left-wing extremist or hardline organizations," deliberately excluding individuals and political parties from prosecution. Further, the term "Urban Naxal" has been altered in the revised bill, as the focus has now shifted entirely to targeting extremist organisations. Similarly, the term "unlawful activities" has been confined to actions linked to extremist or Naxal ideologies, rather than encompassing a broad portion of dissent or protest.

Additionally, several procedural safeguards have been introduced, such as the investigative authority has been raised from Police Sub-Inspector to Assistant Commissioner of Police in urban areas and Deputy Superintendent in rural regions. An Advisory Board, constituted prior to initiating investigations for examining the decision to designate an organisation as unlawful, must now be headed by a sitting or retired High Court judge, along with district magistrates or government pleaders. This is a change from the earlier draft, which only required the involvement of any senior law officer. A clear provision also prevents retrospective application of the law on individuals on the basis of their past associations with organisations barred under the new legislation.

Potential Implications of the Bill

Though the amendments to the bill mitigate some of its earlier lapses, significant challenges remain, one of the most pressing concerns being the continued existence of ambiguous definitions and its associated risks of misuse. The revised bill retains vague terms like “left-wing extremist” and “hardline,” without clearly outlining the legal thresholds or criteria for classification. Critics of the bill are of the opinion that this vagueness leaves room for arbitrary interpretation by state authorities. Without robust definitions, the law could easily be misused against student leaders, trade unions, grassroots activists, or any individuals critical of the government, simply by labeling them as part of extremist organisations. The term ‘urban naxal’, while seemingly altered in the revised draft, still remains as a political label rather than a legal construct, thus enabling the state to stigmatise and preemptively silence legitimate dissent under the guise of public security.

Procedural enhancements, in theory, suggest a move towards fairness, but reality is more complicated. The appointment of senior police officials as investigators in such cases adds a degree of gravity, and the creation of an Advisory Board chaired by a retired High Court judge appears to establish a system of checks and balances. However, these measures risk being symbolic rather than substantive, unless backed by enforceable standards and transparency. The Advisory Board for instance, lacks clear independent authority to investigate, seek evidence, or publish decisions. Without clear criteria or procedural protections for its operation, it becomes merely a rubber stamp for executive decisions rather than a genuine protector of rights.

Another area of concern is the redundancy and overlap between this state law and existing central legislation. India already has stringent anti-terror laws, including the Unlawful Activities (Prevention) Act, 1967 (“UAPA”) and the National Security Act, 1980 (“NSA”), which allow for wide-ranging surveillance, arrests, and bans on organisations. The Maharashtra bill replicates many of these powers, especially in relation to seizure of property, issuance of notices, and imposition of pre-trial restrictions, thus raising concerns about legal conflicts and the risk of double jeopardy. In trying to assert its own jurisdiction, the Maharashtra government risks complicating enforcement and undermining the uniform application of legal standards across states.

Perhaps the most worrisome implication of the bill, despite its revised form, lies in its potential impact on civil liberties and dissent. While the revised bill introduces exemptions for women and children in eviction procedures, these are general and lack enforcement guarantees. The absence of mandatory judicial review before issuing notices or seizures further undermines procedural justice. In practice, such powers are rarely used against hardened criminals but are more often deployed against the vulnerable, and people who rarely have the means to fight back. Without institutional safeguards, this law threatens to do more harm than good.

The Way Forward

Despite these concerns, it would be wrong to say that the revised bill failed to achieve any progress. The decision to remove individuals from the scope of prosecution is a crucial change, as is the elimination of retrospective application. The shift from overtly political term like *'urban naxal'* to a more neutral legal tone is a step in the right direction. Judicial representation on the Advisory Board and the requirement for senior officers to initiate action also help raise the bar for state interference, potentially deterring routine misuse. These adjustments indicate a responsiveness to public criticism and suggest that legislative checks are not entirely absent from Maharashtra's policy making framework.

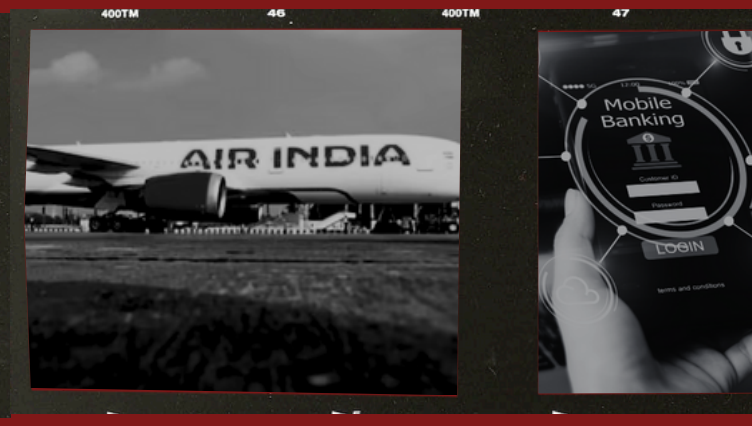
First and foremost is the need for definitional clarity. Without clear and legally enforceable definitions of terms like "extremist," "hardline," and "unlawful activity," the bill leaves room for interpretation. Ideally, these should be drawn from constitutional jurisprudence, especially from Supreme Court rulings that balance security concerns with civil rights. Secondly, the oversight mechanism must be strengthened beyond its symbolic presence; meaning that the Advisory Board should have investigative powers, the ability to summon documents and witnesses, and an obligation to make their decisions public along with the rationale behind the same. Thirdly, there must be provisions for judicial review and remedial action. Any individual or organisation wrongly targeted must have a clear, speedy, and accessible path to challenge the state's actions before a neutral authority. Fourthly, the bill should include explicit safeguards to ensure political neutrality, otherwise it risks becoming a weapon against any opposition to the ruling party, regardless of whether they pose any real threat. Finally, the bill must be harmonised with central laws to prevent legal conflicts and ensure that enforcement is coherent, proportionate, and grounded in constitutional principles.

Conclusion

The revised Bill marks a partial victory for democracy, demonstrating effective public participation and legislative scrutiny. It is a cautious step in the right direction, addressing some of the earlier, ambiguous elements, however, it is far from adequate. For it to earn broader legitimacy, deeper structural reforms focusing on clarity, neutrality, transparency, and judicial safeguards must be incorporated before it is put into place. If these elements are strengthened, the Bill may serve as a model for state legislation that tackles extremism without undermining civil liberties, but in their absence, the present version seems to be a potential instrument of political overreach.

The Aftermath of Ahmedabad: Legal Support Helpdesk Formed for the Families of the Ahmedabad Plane Crash Victims

-Adrija Dey



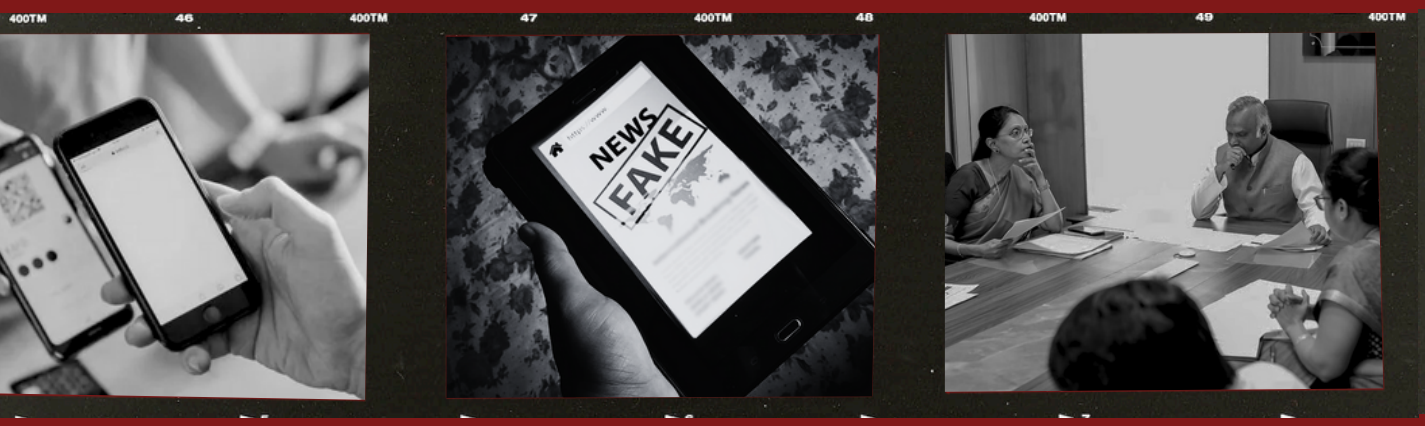
The Gujarat State Legal Services Authority, under the aegis of the National Legal Services Authority, has started a helpline for the families of the victims of the fatal plane crash that took place in Ahmedabad on 12nd June. This 24x7 helpdesk aims to provide legal as well as psychological assistance to the aggrieved families, while also streamlining the process of identity verification. A '*Trauma and Grievance Redressal Support*' has been set up under the helpdesk, where psychological counselling would be provided through the victimology centre named 'Sangathi'. Moreover, qualified legal aid lawyers would be in service to provide instant and walk-in legal support to the people. Since there were a large number of deaths that occurred in the crash, the helpdesk would aid in making documentation more convenient for the already distressed kin of the deceased passengers, while also making sure that their mental health needs are tended to.

While it is a welcome step, the Plane Crash Legal Support Helpdesk will not yield desired results if not implemented efficiently. In India, even though legal aid is a constitutional right of the citizens under Article 39A of the Indian Constitution, there lies a huge gap between the provision and its execution on the ground. There is a lack of awareness among the people about the right to free legal aid to those who cannot afford it. Additionally, since legal aid majorly deals with providing free legal support to people, the pay given to the advocates is often not proportional to the work that they do. This results in a lack of incentive for them, which consequently leads to a skill gap. Another challenge that the helpdesk may face is the smooth functioning of the psychological trauma helpline. The taboo regarding mental health in India is a cause of concern, and it prevents people from acknowledging their pain and being vulnerable in front of another individual. Exacerbating this issue are the shortcomings in the operation of psychological helplines in India, including inactive helpline numbers, non-timely responses, and lack of skilled professionals. These lead to the increase of the public's hesitation to reach out and seek help.

Hence, adequate funding for the legal aid framework in India and skill-enhancement of advocates are some steps towards the right direction of implementing the Legal Support Helpdesk. An improved pay structure for legal aid advocates would provide them with an incentive to perform up to their potential. This incentive, in return, would help reduce the skill gap. Also, recruitment of skilled counsellors on helplines is the need of the hour. The service of trained and expert professionals would yield positive responses from people in distress. This may result in a change in the overall attitude among people about paying more attention to their mental health, causing them to be more open to utilize helpline numbers in times of a psychological crisis. Moreover, since the Helpdesk aims to deal with grieving families, forming a support group of these families, along with professional counselling, can help them in finding closure by sharing their sorrow and pain with each other. Therefore, these reforms would bolster the functioning of the Plane Crash Legal Support Helpdesk, which would help the aggrieved families deal with the copious documentation processes with ease in their time of grief.

A cautionary approach to the draft Karnataka Misinformation and Fake News (Prohibition) Bill, 2025

-Vibha Vaikuntanath



Introduction

In the statement of objects and reasons of the leaked draft of the Karnataka Misinformation and Fake News (Prohibition) Bill, 2025 ('the Bill'), the Karnataka government believes that social media has blurred the line between personal and public. Ostensibly driven by the noble objective of curbing the circulation of unverified information in the digital age, the Bill seeks to introduce regulatory safeguards against its dissemination. However, the Bill is seemingly ridden with ambiguity on multiple levels. It warns the readers of an 'era of real-time news' where one person's idea is mistaken for a fact, and calls for a law that ensures digital speech aligns with 'Indian social decency and culture'. But who defines decency? And at what cost to fundamental rights? These questions remain unanswered.

Stakeholder analysis of the Bill and risks involved

The Bill's ambitious objective is not at the same level as the efforts put into curating a well thought-out draft. It brushes over the rights of multiple stakeholders and is lacking in various areas, as this article will go on to illustrate.

The largest stakeholders are, needless to say, individual social media users. They face a risk of being criminally prosecuted for false statements, which are generally provided protection internationally. There is a pervasive fear among the public of arbitrary enforcement due to the Bill being afflicted with many vague terms, such as 'anti-feminist' or 'disrespect to Sanatan symbols'. Additionally, these terms remain open to subjective interpretation. An exception has been carved out under the definition of misinformation for opinions, comedy, and satire, but given that there has been no precise definitions for these terms, it may not be possible in actuality to categorise instances as such. The same exception has not been afforded for 'fake news'.

More importantly, constitutional safeguards set up by judicial precedents have been ignored, such as the case of *Shreya Singhal v. Union of India*. The Supreme Court had held that Section 66A of the Information Technology Act, 2000 was unconstitutional due to the vague wording, absence of safeguards against arbitrary executive action, and disproportionate penalties for expression—which hence violated Article 19 of the Constitution of India. The Bill presents a similar case for a constitutional challenge - it creates new offences without precise definitions, empowers an executive authority to make a final decision on what is to be considered 'fake', and penalises speech with cognisable and non-bailable consequences.

Secondly, the Bill brings within its ambit social media intermediaries, publishers, and broadcasters. Non-compliance with the directions issued to it by the special courts which are to be constituted, is punishable with imprisonment and a fine. An important concern raised by digital freedom watchdogs has been that this provision disregards the safe harbour provision provided under the Information and Technology Act, 2000. Social media intermediaries are tasked with the responsibility to filter and monitor content uploaded by third parties on their platforms, and makes them liable to punitive action in the event that they do not do so.

Thirdly, the enforcement mechanism or the Fake News on Social Media Regulatory Authority ('Authority') has sweeping powers under the Bill, as pointed out by observers. It is appointed by the executive, raising concerns about its independent functioning. It has the power to decide, adjudicate, and block any content that is considered illegal. Furthermore, there are no minimum qualifications specified for the proposed members constituting the Authority.

The penalties proposed go against the principles of proportionality, and consider the offences to be cognizable and non-bailable, effectively enabling arrest without warrant. The Special Court proposed to be set up can issue orders to take down information via 'disabling directions' even before conviction, violating principles of natural justice and procedural fairness. The label of 'misinformation' stands the risk of being weaponized against journalists reporting uncomfortable truths, activists challenging dominant narratives, and opposition parties and dissenters.

The state cannot be the arbiter of truth

The Bill is not the first policy intervention with the objective of curbing fake news — there have been several attempts to do so earlier, albeit partly unsuccessful due to the fact that the state often ends up becoming the arbiter of truth. For example, in Kunal Kamra v. Union of India the Fact Check Unit which was proposed to be set up under the Information and Technology Rules 2023 was held to be

unconstitutional by the Bombay High Court, as it exceeded the limits enshrined in Article 19(2). It was successfully challenged due to the danger of empowering an executive body to define and punish 'misinformation'.

International Correlatives For Reference

European Union's Digital Services Act ('DSA')

The DSA serves to protect consumers, digital service providers, businesses, and society at large by setting up proportionate and clear rules to promote transparency, protection of minors online, reduce exposure to illegal content, and mitigation of disinformation. It makes rules for digital intermediaries, according to their size, role, reach, and impact. It ensures fairness and proportionality, and establishes clarity in this regard.

Germany's NetzdG law

The Network Enforcement Act or NetzdG law combats hate speech online, fining online platforms for systemic failure to delete illegal content. Some support this initiative as necessary to control extremism online, while critics point out that the delegation of censorship to private bodies is draconian, and forces social media platforms to undertake a painstaking process of takedown or removal. Although the Bill in question mandates takedown procedures, it also seeks to criminalise intermediaries, which goes a huge step further.

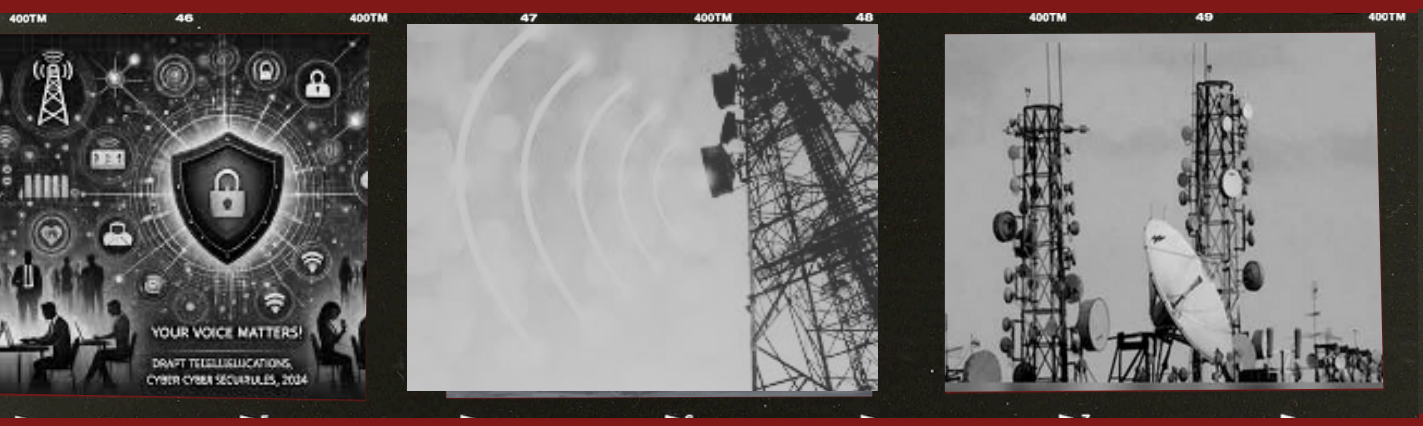
Singapore's Protection from Online Falsehoods and Manipulation Act 2019 ('POFMA')

The POFMA is an Act that was passed to prevent the spread of false factual statements from being circulated electronically, and to prevent support of the same. It permits a single government minister to unilaterally declare falsehood of information online, and order its correction or removal for the cause of public interest. Similar to the present Bill under discussion numerous, concerns were raised about the possible implications of the vague and ambiguous terms utilised and the uncertainties involved. The government is vested with too much power in its hands creating a 'chilling effect' on the freedom of speech, and leaves the Act open to judicial review.

Considering the widespread disagreement with the leaked draft of the Bill by watchdogs, academicians, and citizens alike, it is suggested that the Karnataka government reconsiders the contents of the Bill. The statement of objects and reasons plays out an all too real scenario which needs immediate attention, but not in the manner that has been adopted. It would be prudent to draw from both domestic and international examples, along with a close analysis of judicial precedents laid down by the constitutional courts of the country.

Cyber Security Reinforced: Draft Amendments to Telecom Cyber Security Rules Presented

-Aryan Chowdhury



Introduction

The digital landscape is constantly evolving, and are the challenges of cybersecurity and data privacy. In an effort to bolster its digital defense, the Indian Department of Telecommunications (DoT) recently introduced the draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025. It intends to amend the highly criticised Telecommunications (Telecom Cyber Security) Rules, 2024. These proposed amendments bolster the 2024 rules and aim to enhance the 2024 rules. This article delves into the intricacies of these new rules, examining their entailments, their impact on the status quo, and whether they truly represent a step in the right direction for India's digital future.

A Look At The Proposed Amendments

The digital landscape is constantly evolving, and are the challenges of cybersecurity and data privacy. In an effort to bolster its digital defense, the Indian Department of Telecommunications (DoT) recently introduced the draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025. It intends to amend the highly criticised Telecommunications (Telecom Cyber Security) Rules, 2024. These proposed amendments bolster the 2024 rules and aim to enhance the 2024 rules. This article delves into the intricacies of these new rules, examining their entailments, their impact on the status quo, and whether they truly represent a step in the right direction for India's digital future.

Key provisions of the draft amendments include:

- **Expanded Data Collection:** The government can now seek data related to telecommunication identifiers from TIUEs for cybersecurity purposes. Telecommunication identifiers refer to unique identifiers assigned to users, telecom equipment, or network elements.

- **TIUE Obligations:** TIUEs are mandated to provide required data digitally for processing and storage, and to suspend the use of specified telecommunication identifiers upon a government order.
- **Mobile Number Validation (MNV) Platform:** The central government is tasked with establishing an MNV platform. TIUEs can use this platform to validate mobile numbers of their customers, either voluntarily or under government direction. Charges for the same have been introduced, with 1.5 rupees for state-recognised entities and 3 rupees for other entities.
- **Centralized IMEI Database:** A centralized database will be maintained to track tampered or restricted International Mobile Equipment Identity (IMEI) numbers. Individuals involved in the sale or purchase of used telecom equipment must verify IMEI numbers against this database to ensure that they are not tampered with or restricted.

Impact on the Status Quo

The introduction of these amendments marks a significant shift in India's digital regulatory landscape. Previously, data collection and cybersecurity obligations were primarily focused on traditional telecom operators. The 2025 rules extend these responsibilities to a much wider ecosystem of digital platforms, fundamentally altering their operational frameworks and compliance burdens. The broad definition of TIUEs means that almost every digital application or service that uses a mobile number for user authentication or communication will now fall under this regulatory framework.

This expansion is poised to create considerable operational and financial challenges for many businesses, particularly small and medium-sized enterprises (SMEs) and startups. Integrating with a government-run MNV platform will require significant technical adjustments, including building new APIs, establishing real-time verification pipelines, and securely storing validation logs. For companies with legacy systems, this could necessitate a complete architectural overhaul, diverting resources from innovation and growth towards compliance.

Furthermore, the rules effectively assign Know Your Customer (KYC)-like duties to tech platforms, a responsibility previously limited to banks and telecom companies. This redefines the boundary between telecom regulation and digital innovation, potentially stifling entrepreneurship if not implemented with careful consideration for a phased rollout or government support.

A Step in the Right Direction?

On the Issue of Privacy

The expansion of data collection to TIUEs and the mandatory sharing of data with the government raises substantial privacy concerns. While the stated aim is cybersecurity, the broad scope of data

collection and the creation of centralized databases create significant repositories of user and device information. This centralization inherently increases the risk of data breaches, misuse, or unauthorized access. The lack of clear definitions for what constitutes 'public interest' when the government can bypass notice requirements to suspend telecom identifiers is particularly troubling. This absence of robust safeguards for due process and independent oversight undermines principles of natural justice and transparency, potentially leading to arbitrary decisions without recourse for affected individuals.

From a cybersecurity perspective, the amendments present a mixed bag. The establishment of a MNV platform and a centralized IMEI database could indeed enhance security and these measures could help in combating identity spoofing, impersonation, and fraudulent activations, which are significant challenges in the digital realm. The ability to track tampered or restricted IMEI numbers could also aid in curbing the use of illegal devices and improving overall device security.

However, the effectiveness of these measures hinges on their implementation. Centralized databases, while offering efficiency, also become attractive targets for cyberattacks. Robust security protocols, encryption, and strict access controls are paramount to prevent these databases from becoming susceptible to cyber attacks. Without these, the very tools designed to enhance cybersecurity could become vulnerabilities themselves. Furthermore, the broad definition of 'telecom cyber security' and 'applications' could lead to an overreach that stifles innovation and places undue burden on platforms, potentially hindering their ability to implement agile and effective security measures tailored for their specific services.

On the Issues of Government Surveillance

Perhaps the most contentious aspect of these amendments is their potential for expanding government surveillance. The provisions allow the government to seek traffic data and other specified data from both traditional telecom entities and the newly defined TIUEs. This coupled with the power to suspend telecommunication identifiers, significantly increases the state's capacity for monitoring. The centralized MNV and IMEI databases could facilitate easier tracking and profiling of individuals and their digital activities. While the government's stated aim is to protect national security and prevent cybercrime, the lack of transparency regarding how and when these powers will be exercised creates an environment ripe for potential overreach.

Conclusion

The Telecommunications (Telecom Cyber Security) Amendment Rules 2025 represent a significant legislative effort to adapt India's cybersecurity framework to the evolving digital landscape. While the intent to enhance national security and combat cyber fraud is commendable, the proposed

amendments raise serious concerns regarding individual privacy and the potential for increased government surveillance. The broad definitions, expanded scope of data collection, lack of robust safeguards, and the absence of clear oversight mechanisms create a regulatory environment that could inadvertently stifle digital innovation and erode public trust, inadvertently creating a compliance heavy regime.

Moving forward, it is crucial for the government to engage in a more transparent and inclusive dialogue with stakeholders, including privacy advocates, legal experts, and industry representatives. Refining the definitions, establishing clear boundaries for data collection, implementing strong data protection protocols, and introducing robust independent oversight mechanisms are essential to strike a balance between national security and individual rights. Only then can these amendments truly be considered a step in the right direction for India's digital future, fostering both security and freedom in the increasingly interconnected world.

EDITORS

Aryan Chowdhury
(Editor-in-Chief)
Tinashree J
Manasvi Singh
Shruti Shriram
Adrija Dey

DESIGN

Manasvi Singh
Ishani Garg

Connect with us: