Regulation Of Ott Platforms Under the Telecom–Cybersecurity Legal Framework in India

Kavya R. Krishnan[1], Gayathri Narayan N[2]
[1,2] *B. A. LL.; B (Hons.)*

"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."

— Eric Schmidt, Google CEO and Alphabet executive chairman

Abstract—**This paper examines the evolving nature of the mechanism used to regulate Over-The-Top (OTT) platforms. Understanding OTT platforms by examining the various definitions provided through varying regimes then by analyzing the intertwining legal regime of telecom and digital platform regulations in India. OTT services subsume multiple services ranging from messaging platforms, films, social media, filesharing facilities etc., that are provided over the public internet without using the telecom infrastructure, Organizations like BEREC and ITU explain that OTTs are unique in the sense that they are not controlled by regular networks and disrupt the activities of telecom and media companies.**

Globally, regulators have taken two approaches: some have maintained a combination of co-regulation and multi-stakeholders, that is attentive to competition, business influence, and infrastructure; others are more attentive to economic markers and data privacy. Since OTTs are not required to pay network charges, to obtain licenses, or to comply with the quality-of-service regulations that telecoms should, it poses a regulatory gap and individuals are demanding a more equalized model of oversight.

One of the concerns that continues to pose a challenge is that OTT apps rely on phone numbers as universal identifiers, which leads to large-scale cyber-attacks such as phishing, vishing and social engineering. Address book syncing and caller id integration are features on which hackers find opportunities to conduct large scale attacks. The telecommunications Cyber Security Amendment Rules 2025 are expected to address these problems by providing digital platforms, such as OTTs that use mobile-based verifications, with real-time verification and suspension capabilities under that name of Telecommunication Identifier User Entity (TIUE). These proposals threaten overregulation by authorizing authorities, raising constitutional issues, due process issues, and potential adverse effects on innovation and economic development.

Index Terms—**OTT Platforms, Telecommunications, Cybersecurity, Telecommunication (Cyber Security) Rules, 2024, Telecommunication (Cyber Security) Amendment Rules, 2025, Phishing Attack, Vishing Attack, Whaling Attack**

I. INTRODUCTION

An average Indian user consumes 27.5GB data per month, growing at 19.55 CAGR which is expected to reach 50GB in 2030[1]. The internet data usage has become the most prominent revenue driver in the telecommunication sector. Motivated by the concept of "world in the palm of my hands" and inevitably by the internet revolution during COVID, every household now at least has one smartphone and a data pack. This has led to an exponential increase in the use of online services being used that utilize the internet protocol (IP). The availability of data packs and smartphones facilitated a boom in OTT services, making entertainment ever so more commodified. OTT services thus began to encroach upon or replace

[1]The Hindu Bureau, 27.5 GB Average Monthly Data Consumed by Indians, FWA Using 12× More Data Than Mobile Users, The Hindu (May 25, 2025), https://www.thehindu.com/sci-tech/technology/indians-consuming-275-gb-average-monthly-data-fwa-using-12x-more-data-than-mobile-users/article69352909.ece (last visited Nov. 1, 2025).

multiple traditional industries like that of cable television (TV), telecom operators etc. The OTT services utilize the existing infrastructure, without undergoing any regulation, payment of any fees or securing license while providing the same services as that of the telecom operators. This leads to the question of how the OTT platforms should be regulated.

This takes us to understand what an OTT platform is in the first place and what are the different types of OTT platforms. Then the paper tries to traverse into the jurisprudential aspects by explaining the existing legal framework and the discussions undertaken by the ministry, executives and the industrial experts.

Sociological need of a law explains how and what aspects should it govern, thus this paper delves into what kind of cybersecurity threats do these platforms pose, consequentially the requirements to address it. Whether the current legal framework is sufficient in addressing these concerns while benchmarking with global best practices.

II. MAIN BODY

What is an OTT Platform?

OTT Platform or Over-The-Top Platform is the buzzword of the last decade. It is impossible to delve into the paper without defining what an OTT Platform possibly can be. There is no single accepted definition of OTT Platforms nevertheless there have been attempts to define it whenever a new angle of regulation was discovered. OTT Platforms include a wide range from video delivery platforms like Netflix, messaging platforms like WhatsApp and file sharing platforms like Dropbox.

- OTT Platform was defined in the BROADCASTING SERVICES (REGULATION) BILL. 2023[2] under Section 2(1)(y) as "Over-the-top broadcasting service" or "OTT broadcasting service" means a broadcasting service (i) made available on-demand or live to subscribers or users in India, and (ii) where a curated catalogue of programmes owned by, licensed to, or contracted to be transmitted, over the internet or a computer resource, not being a closed network; [3]
- The International Telecommunication Union defines it as "Internet application that may substitute or supplement traditional telecommunication services, from voice calls and text messaging to video and broadcast services"[4].
- TRAI defines 'OTT provider' as: "a service provider offering ICT (Information Communication Technology) services, but neither operates a network nor leases network capacity from a network operator. Instead, OTT providers rely on the global internet and access network speeds (ranging from 256 Kilobits for messaging to speeds in the range of Megabits (0.5 to 3) for video streaming) to reach the user, hence going "over-the-top" of a telecom service provider's (TSP's)network."[5]
- BEREC defines OTT platforms as "content, a service or an application that is provided to the end-user over the public Internet"[6].

The question of whether these OTT platforms should be regulated by the telecom rules arises because there are platforms like Jio Hotstar that provide online video services along with broadcasting services like the live telecast of cricket. Conversely, platforms like Netflix that primarily provide online entertainment services and produce their own films and web series. Additionally, live content can also be telecasted through social media platforms such as Instagram live. The OTT Platforms have increasingly become a

[2] Broadcasting Services (Regulation) Bill, 2023, Gazette of India, Extraordinary, Part II, Sec. 2 (Dec. 2023) (India)

[3] Broadcasting Services (Regulation) Bill, § 2(1)(y) (2023) (India).

[4] International Telecommunication Union, Technical Report on Economic Impact of OTTs (2017), https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ECOPO-2017-PDF-E.pdf.

[5] Telecom Regulatory Authority of India, Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services, Consultation Paper No. 10/2023 (July 7, 2023).

[6] Body of European Regulators for Electronic Communications (BEREC), BEREC Report on OTT Services (2016).

competition to the traditional telecom services as they do not have to obtain any license and can deliver analogous service with the help of existing Internet Service Providers (ISPs)

The Net Neutrality Committee Report[7] therefore has distinguished the OTT Services for the purpose of regulating them under the telecom rules.

i) OTT communications services – These services (e.g. VoIP) provide real-time person to person telecommunication services. These ser-vices are similar to the telecommunication services provided by the licensed telecom service providers (TSPs) but are provided to the users as applications carried over the internet using the network infrastructure of TSPs. Essentially OTT communications services compete with the services provided by TSPs riding on the infrastructure created by TSPs.

(ii) OTT application services – All other OTT services such as media services (broadcasting, gaming), trade and commerce services (e-commerce, radio taxi, financial services), cloud services (data hosting & data management platforms/applications), social media (Internet based intermediary applications like Facebook, YouTube) offer services to end-users using the network infrastructure created by TSPs but do not directly compete with the service offerings for which the TSPs have obtained a licence under the applicable law i.e. the Indian Telegraph Act, 1885.

Convergence and Conflict: OTTs and Telecom Service Providers

OTT platforms and TSPs are critically interdependent of each other; their relationship can be described as symbiotic, complementary, and mutually reinforcing. The OTT platforms drive the data demand when rich applications increase the demand for high-value date plans and the value for broadband networks increases. Increased demand for content drives the demand for Internet connectivity services, increasing traffic and, consequently, the revenue of TSPs. The TSPs have a problem with OTT Platforms primarily because the OTT platforms operate without any infrastructure. They rely on the network infrastructure provided by the TSPs. TSPs are obligated under the Unified License Agreement to regulate lawful interception, ensure privacy and security, provide emergency services and customer verification, which do not apply to the OTT platforms. TSPs must pay a one-time non-refundable entry fee, an annual license fee (currently 8% of Adjusted Gross Revenue or AGR), and spectrum-related charges[8], if applicable. OTTs do not have these financial obligations, leading to competitive conflict.

Globally and in India, there is a general trend of transition from voice and SMS towards data as a primary source of revenue for TSPs. The composition of Average Revenue Per User (ARPU) per month for wireless services in India shows that the contribution of data usage grew from 8.10% in QE June 2013 to 85.1% in QE December 2022.[9] The revenue from SMS per subscriber per month decreased by about 94% between 2013 and 2022.[10] International voice traffic has also migrated to OTT service provision due to pricing arbitrage. Global data suggests cross-border OTT traffic overtook international carrier traffic in 2016.

OTT domestic Voice over Internet Protocol (VoIP) communication services have the potential of significantly disrupting existing revenue models of TSPs, as voice revenues historically contributed approximately three-fourths of total TSP revenues. The pricing arbitrage between conventional voice calls and VoIP offered by OTTs has been cited as a major concern. The shift is technologically driven by the delayering of communication networks through Internet Protocols (IP), which allows the applications layer (OTTs) to function independent of the media layers (TSPs). This separation has allowed OTT communication service providers to bypass the traditional requirement of obtaining a license and establishing a network to offer services.

Even though the TSPs have dubbed their problems with the advent of OTT platforms as that to free riding on their network infrastructure they were also the

[7] A.K. Bhargava et al., Net Neutrality Committee Report (Dep't of Telecommunication May 2015), https://dot.gov.in/sites/default/files/Net_Neutrality_Committee_report%20%281%29_0.pdf (last visited Oct. 27, 2025).

[8] TRAI, supra note 5, at

[9] Id.

[10] Id.

earliest ones to recognize their potential and jump into the bandwagon. Most OTT platforms are owned by TSPs which leads to another issue of competition. TSPs/ISPs with bigger market power tend to favour their own applications or contents and engage in illegal traffic management by blocking or throttling competing OTT applications. Historically, this tendency has been seen in cases like Airtel's attempted premium charge for VoIP services like Skype, which the TSP views as competition to its legacy voice services.[11] TSPs/ISPs may prioritize certain traffic based on exclusive arrangements with specific content providers. When TSPs collaborate with content providers, they enable that entity to play a "gatekeeper" role, determining which applications or services are accessible or prioritized for users. If TSPs prioritize content based on exclusive arrangements, small start-ups will have a difficult time establishing their business. Start-ups lack the financial resources of major companies to afford fees necessary to deliver content to customers, leading to an unfair playing field.

Cybersecurity Concerns: OTTs and the Exploitation of Telephone Numbers

The accessibility of telephone numbers that OTT Platforms (e.g. WhatApp, VIber and WeCHat) can be exploited maliciously to commit a range of cyber offences like Phishing Attacks, Vishing Attacks or Whaling Attacks.

The attackers generate a large pool of phone numbers and insert them into the address book of a device under their control. The attackers then use a caller ID lookup application like Truecaller to gather personal details. The attackers exploit the address book syncing feature common in OTT messaging applications to identify which of those numbers are registered users of that specific OTT application who will become potential victims. The attackers then collect information about the victim's social circle through the public information that is available in social networking platforms which they gather using the name and phone number that they have secured using the caller id lookup application. This provides authenticity and increases success rate. They use the information that is collected from the social networking platform to generate personalized messages that increases their chances of deceiving the victims consequentially. This attack can be scaled to a larger population by automating these procedures.

Vishing Attacks would be using voice caller application to phish i.e. Voice phishing. Attackers register themselves in these Caller Id Lookup Application as legitimate entities like banks or legitimate companies. Since these applications generally rely on user-provided information without rigorous verification, the attacker compromises the integrity of the caller ID information. This increases the likelihood of the victim picking the phone up. The attackers can also use the personalized information that they have secured from the social networking platform. Whaling Attacks are also another type of phishing attack that is targeted towards senior executives or high-profile individuals. Attackers identify potential targets by enumerating or obtaining specific vanity phone number patterns (e.g., 99999-xxxxx), which are typically bought at a higher price and are associated with people of influence or wealth.[12]

India's Legal Framework for OTT Platforms

OTT Platforms or digital platforms were primarily governed by the Information Technology Act[13], 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[14].

However, these rules fundamentally deal with content regulation and establishing an internal complaint and grievance redressal mechanism system. Under the IT act and its consequent rules, they are governed by the Ministry of Electronics Information and Technology (MeiTY). The OTT platforms are categorized under

[11]Chaitanya Ramachandran, How to Design an Indian Net Neutrality Law, 12 Indian J.L. & Tech. 1 (2016).

[12]Srishti Gupta et al., Exploiting Phone Numbers and Cross-Application Features in Targeted Mobile Attacks, SPSM '16, Oct. 24, 2016, at 1, http://dx.doi.org/10.1145/2994459.2994471.

[13] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, Sec. 3(i) (Feb. 25, 2021).

three categories: news providers, intermediaries, and OTT platforms. Under the IT rules 2021, the OTT entertainment platforms are governed as "publishers of online curated content"[15] whereby *"a publisher who, performing a significant role in determining the online curated content being made available, makes available to users a computer resource that enables such users to access online curated content over the internet or computer networks, and such other entity called by whatever name, which is functionally similar to publishers of online curated content but does not include any individual or user who is not transmitting online curated content in the course of systematic business, professional or commercial activity;"*.

They have rules regarding content classification, age ratings, and self-regulation. They are required to appoint individuals for removing information upon government orders and to ensure compliance. They must also establish a grievance redressal mechanism. They need to establish a three-tier grievance redressal and oversight mechanism. Level I constitutes Platform's own self-regulation, Level II deals with a Self-Regulatory Organization composed of retired judges or eminent persons to oversee the compliance of code of ethics and Level III includes Government Oversight through MIB. The content needs to be classified based on a five-tier age-based content classification system which include U, U/A 7+, U/A 13+, U/A 16+ and A. In addition to these the OTT platforms must comply with due diligence guidelines under Section 3(1) (d) to enjoy the safe harbour protection under Section 79 and can be held liable under Section 67, 67A and Section 69A for the violation of the due diligence clause.

Other than these, OTT platforms came under self-regulation whereby the Internet and Mobile association of India (IAMAI) has introduced the Digital Publishers Content Grievance Council (DPCGC) as a self-regulatory body for streaming platforms. They have distinguished between broadcaster-based OTT platforms to control platforms like Jio Hotstar, ZEE5, SonyLIV, Voot etc. that will be governed by Indian Broadcasting and Digital Foundation (IBDF) and platforms like Netflix, Amazon Prime, MX Player will fall under IAMAI.[16]

After the Digital Personal Data Protection (DPDP) Act, 2023, IT Act's sector specific approach is replaced with consent first regime, whereby OTT platforms must replace pre-ticked boxed, bundled consents, conditional consent requiring individuals to waive statutory rights or blanket "I agree to all" terms should be replaced with granular, purpose-specific consent under Section 6. OTT platforms as data fiduciaries need to comply with the general principles of Notice and Transparency, Record Maintenance and Accountability, Data Minimization and Purpose Limitation and Data Retention & Erasure under Section 8. Section 11-14 provides for rights of Correction and Updating, Right to Erasure and Right to Grievance Redressal.

Regulatory Friction Between TDSAT and the Government

The Telecom Disputes Settlement and Appellate Tribunal on October 4th 2023 settled a legal dispute between All India Digital Cable Federation (AIDCF)[17] and Star India Private Limited. AIDCF alleged that Star India violated the principle of non-discrimination under Regulation 3(2) of the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017[18]. AIDCF alleged that Star India charged the cable distributors for access to their sports channel signal and simultaneously permitted viewers to view Star Sports free of charge through Jio Hotstar (its own OTT platform). AIDCF argued that OTT platforms should be classified as distribution platforms under the TRAI regulations because they use Broadband internet.

[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 2(u), Gazette of India, Extraordinary, Part II, Section 3(i) (Feb. 25, 2021).

[16] Ashaawari Datta Chaudhuri, Do OTT Platforms Deserve a Separate Regulation?, Centre for Rsch. & Analysis in Fin., Tech. & L. Working Paper No. 2/2021 (2021).

[17] All India Digital Cable Fed'n v. Star India Pvt Ltd, BROADCASTING PETITION/217/2023 (Telecom Disputes Settlement & Appellate Tribunal Oct. 4, 2023).

[18] Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017, Telecom Regulatory Authority of India, Gazette of India, Extraordinary, Part III, Sec. 4 (Mar. 3, 2017) (India).

Since they use broadband internet, they fall within the definition of Telegraph thus granting the tribunal jurisdiction. Telegraph is defined as

"*telegraph" means any appliance, instrument, material, or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric, or magnetic means.*[19]

TDSAT held that OTT platforms do not fall within the purview of TRAI Act, 1997 but under the purview of the Information Technology Act, 2000 and its rules. The tribunal observed that the definition of distribution platform is exhaustive therefore OTT platforms cannot be read into it and added to the definition. OTT platform is not a television (TV) channel and the 2017 regulations in essence govern the TV channels thus will not apply to OTT platforms. Even TRAI's Explanatory Memorandum about the 2017 regulations suggested that the OTT platform was not covered.

In response to this judgement of the tribunal the Ministry of Information and Broadcasting (MIIB) released a draft of the 2023 Broadcasting Services (Regulation) Bill[20] in place of the 1995 Act. It aimed at including the OTT services within the ambit of traditional broadcasting services. In 2024, it circulated another 2024 Bill with select stakeholders with an aim to extend it to social media intermediaries as well. The 2024 Bill categorizes tweets "transmission of textual programme(s)", blogs as "broadcasting" and digital content creators as "Digital News Broadcasters". The 2023 Broadcasting Bill concentrates on regulating "how" content is transmitted (its underlying network and delivery mechanisms) whereas the IT Rules are more concerned with "what" is being transmitted, focusing on the nature and type of digital content itself. The confluence of IT rules and Broadcasting regulations just makes the compliance process excessively cumbersome for the digital platforms serving no practical purpose. Therefore the 2024 bill was withdrawn and the consultation process was reopened with the 2023 Bill.

Comparative Global Approaches

European Union: The EECC Regime

The European Union introduced the Electronics Communications Code (EECC) as a part of the EU directive 2018 which the members were obliged to implement by 21st December 2020. The EECC defined "electronic communications services"[21] as a service normally provided for remuneration via electronic communications networks and services consisting wholly or mainly in the conveyance of signals. Remuneration may be in the form of direct payment, being exposed to advertisements or providing data. The OTT services are classified under the interpersonal communications services cover both 'number-based services' meaning interpersonal communications services which connect with publicly assigned numbering resources (classic phone calls on the Public Switched Telephone Network (PSTN) network or on-line services allowing connection with classic telephone numbers), as well as 'number-independent services,' those being services which do not connect with publicly assigned numbering resources. Therefore, EECC applies not only to traditional telecommunication services like telephone calls, e-mails, or SMS services but also to OTT services covering internet communications involving applications like WhatsApp, Viber etc.

The new definition of ECS will also affect the scope of e-Privacy Directive (ePD) since the ePD is also based on the EU directive's definition of ECS which primarily concerns confidentiality of correspondence and content.

There are two landmark cases before the ECJ that clarified the scope of ECS. In the SkypeOut[22] Case, the

[19] The Indian Telegraph Act, No. 13 of 1885, § 3(1AA), INDIA CODE (1885).

[20] Broadcasting Services (Regulation) Bill, 2023, supra note 2,

[21] Directive (EU) 2018/1972, art. 2(4), establishing the European Electronic Communications Code (EECC), 2018 O.J. (L 321) 36.

[22] Case C-142/18, Skype Commc'ns Sàrl v. Institut belge des services postaux et des télécommunications (IBPT), ECLI:EU:C:2019:460, (June 5, 2019).

ECJ clarified that SkypeOut does fall within the definition of ECS since they were providing VoIP service for which they were remunerated whereby the user can call a mobile number covered by a national numbering plan from a terminal via the PSTN of a member state. In addition to that the provision of that service involves the conclusion of agreements between that software publisher and telecommunications service providers that are duly authorized to send and terminate calls to the PSTN.[23] The court clarified that even though the actual transmission is not carried out by Skype, the transmission is the result of an agreement between Skype a telecommunication service provider and that is sufficient for it to be included within the scope of ECS.

In the Gmail Case[24], the ECJ clarified that Gmail does not fall within the scope of ECS. For the ECJ, the supplier of a web-based email service that actively participates in sending and receiving emails does not appear to be regarded as consisting wholly or mainly in the conveyance of signals as required by the definition of an electronic communication service. In the case of a webmail service, the internet access providers of the senders and recipients of the emails convey the signals necessary for the functioning of the web-based email service, and it is they who bear responsibility. That is what distinguishes the Gmail case from the SkypeOut case.[25]

The providers must ensure a level of security proportional to the risk that they supposedly face. The code also insists on encryption to prevent security incidents on the users over the network. The code promotes end-to-end encryption where necessary. The providers of public electronic communication networks or services must notify the competent authority of a security incident that has had a significant impact on the operation of networks or services without undue delay. The competent authority may inform the public or require the providers to do so, if it determines that disclosure of the security incident is in the public interest. The European Union Agency for Network and Information Security (ENISA) helps to facilitate coordination among Member States to avoid diverging national requirements. The Commission may adopt implementing acts, taking utmost account of ENISA's opinion, to detail the technical and organizational measures and the procedures for notification requirements, based on European and international standards. Competent authorities can obtain assistance from a designated Computer Security Incident Response Team (CSIRT) in relation to certain issues. They can require providers to supply information needed to assess the security of networks and services, including documented security policies. They can also require providers to submit to a security audit carried out by a qualified independent body or a competent authority, with the cost of the audit paid by the provider.

Even though OTT platforms now fall within the definition of ECS but since they are Number-independent ICS they are subject to lighter obligations appropriate to the risk to the extent that certain consumer protection rules may be exempted for providing only number-independent ICS. ECS providers must provide detailed contractual information, ensure transparency regarding price and quality of service, and offer facilities to monitor expenditure.

South Korea: The “Netflix Law”

The core legislation in South Korea of messaging apps in South Korea stems from the amendment of Telecommunications Business Act that the National Assembly passed in May 2020, dubbed popularly as the “Netflix Law”. The revised law applies to platforms that account for more than 1 percent of domestic internet traffic and that have more than 1 million daily users on average over a three-month period. The foreign platform operators like Netflix and YouTube must share costs associated with securing stable services. Nevertheless, critics argued against the

[23]Christoph J.J. Engelmann, ECJ Clarifies Scope of Telecoms Regulation for OTT Services, Technology’s Legal Edge (July 2, 2019), https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/ (last visited Oct. 29, 2025).

[24]Case C-193/18, Google LLC v. Bundesrepublik Deutschland, ECLI:EU:C:2019:492 (June 13, 2019).

[25]Skype Commc’ns Sàrl, supra note 22,

vague definitions in the amendment that did not define what exactly constitutes "stable service." Both local and foreign telecommunications platform operators are required to be equipped with server capacity that can mitigate sudden spikes in internet traffic while also ensuring stable servers and services. The amendment binds network operators to negotiate deals about network usage fees and other expenses. In addition to this foreign telecommunication platform operators were asked to have representatives within a country. [26]

Vietnam: Light-Touch Regulation

Vietnam has also categorized OTT platforms as telecom services and subjected them to a brand-new legislation of Telecom Law of 2023 which has been in operation for OTT, IDC, and cloud services from 1st January 2025. The approach Vietnam has taken towards these services has been described as "light touch" since they are not subjected to license requirements as that of the traditional telecom operators. Nevertheless, they must register and notify. They need to declare the quality of their services and comply with laws of cybersecurity, consumer protection, data protection, cyberinformation security, national security, and service quality. In addition to these requirements, the offshore big players that provide cross-border services must comply with the principle of respecting independence and sovereignty, equality, ensuring information safety and security as well as common commitments under international treaties to which Vietnam is a member. The government must roll out clear regulations regarding the rights and obligations of cross-border providers of these services. [27]

Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

The Draft of the Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 were notified on 24th June 2025 inviting objections from public and came into force on 22nd October 2025, The Amendment defines Telecommunication Identifier User Entity (TIUE) as "a person, other than a licensee or authorized entity, which uses telecommunication identifiers for the identification of its customers or users, or for provisioning, or delivery of services".[28] The definition targets entities that consume and use telecom resources mainly telecommunication identifiers like mobile numbers. Therefore, based on this definition OTT platforms that utilize mobile numbers to identify their customers will also be governed by the Telecommunication Cyber Security rules. Services like Netflix that provides entertainment services and WhatsApp that provides communication services will also be governed by these rules since they use mobile numbers for registration of customer accounts. They apply to OTT communication platforms, fintech apps and e-commerce players.

A telecommunication identifier initially as defined in Telecommunications (Telecommunication Cyber Security) Rules, 2024 implied a telecommunication equipment identification number which consists of two types of identifiers: International Mobile Equipment Identity (IMEI) Number and Electronic Serial Number (ESN). According to the Amendment Rules the definition was expanded to bring the identifier used by digital platforms for user authentication and service delivery, strongly implying mobile numbers.

The rules aim to combat telecom-enabled cyber fraud and prevent the misuse of unique telecommunication identifiers. The Central Government is to form a centralized Mobile Number Validation (MNV) platform. The TIUEs are directed to use these MNV platforms to validate customer identifiers against licensed KYC operators.[29] The TIUE may place a request with the MNV platforms to seek validation

[26]Shim Woo-hyun, Korea Reveals Details of "Netflix Law", The Korea Herald (Sept. 8, 2020), https://www.koreaherald.com/article/2416335 (last visited Oct. 30, 2025).

[27] Y. Bae et al., OTT, IDC and Cloud-Computing Services under Telecom Law 2023, Int'l Bar Ass'n (2024), https://www.ibanet.org/OTT-IDC-and-Cloud-Computing-services (last visited Oct. 30, 2025).

[28]Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 2(1)(i), G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[29]Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 7A, G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

regarding whether a telecommunication identifier specified by their customer or user corresponds to the actual user available in the database of an authorized entity or licensee. This request can be initiated Suo mot or upon the direction from the Central Government. If the TIUE generates a Suo moto request, the decision to allow the use of the MNV platforms rests with the Central Government. The financial burden of this verification process is borne by TIUEs i.e. if the TIUEs are having their customers verified by the MNV platforms the service fee for the verification process is paid by them, which fee is shared by the government and the agency maintaining the MNV platform.

The Central Government can suspend or terminate a TIUE's use of a relevant identifier for service delivery if it endangers telecom cyber security, in certain situations without prior notice. TIUE can also be directed to share data related to identifiers. These suspension or termination powers can be exercised in public interest without prior notice.[30] The Central Government may "seek data related to telecommunication identifiers used by a TIUE in the form and manner as specified on the portal"[31] for security purposes.

No person, including a TIUE, shall use any telecommunication equipment, identifier, network, or service for the purpose of:

- Fraud, cheating or impersonation.
- Transmitting any message which is fraudulent.
- Committing or intending to commit any security incident.
- Engaging in any other use contrary to any provision of any law in force[32]

An Appraisal of the 2025 Telecom Cybersecurity Framework

Previously the OTT regulation came primarily under the ambit of the Information Technology Rules however with this amendment it is brought under the scope of the Ministry of Broadcasting. The MNV platform cross-checks whether a suspected or flagged number belongs to the reported customers or users as the licensee's database. This legislation was rolled out to verify the phone numbers whereby the MNV platforms will prevent the fraudsters from using temporary or virtual phone numbers thus stopping the creation of fake accounts using burner numbers.

The concerned TIUE must pay ₹3 for a suspected request and if it was required by the government then the TIUE must pay ₹1.5 per request. This increases the compliance cost of OTTs since there can be no definite limit to the requests that can be made by the government to the extent that it can require all the customers to be validated. It can cost companies ₹15,00,000 for only 5 lakh requests thereby discouraging startups from using mobile numbers as verification methods and resort to riskier methods for verification like email or exit segments.

The 2025 amendment has been received with mixed response. While some believe that this streamline the verification process for OTTs which were providing data on a demand basis, can now send a list of suspected numbers to the MNV platforms for verification[33]. While others are raising privacy and constitutional validity concerns.[34] There is no appeal process provided under the rules or how the MNV platform must be structured. Since mobile numbers are used a plethora of services ranging from mobile banking transactions to booking a railway ticket, there

[30]Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 5, G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[31]Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 3(a)(aa), G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[32]Telecommunications (Telecom Cyber Security) Rules, Rule 4(3), G.S.R. 520(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Aug. 28, 2024) (India).

[33]DoT Brings OTTs Under Mobile-Number Validation Framework, The Hindu BusinessLine (Oct. [date] 2025),https://www.thehindubusinessline.com/info-tech/dot-brings-otts-under-mobile-number-validation-framework/article69741394.ece (last visited Nov. 1, 2025).

[34]Pranav Bhaskar Tiwari, Written Comments: Draft Telecom Cybersecurity Amendment Rules (The Dialogue July 2025).

are concerns of what will be the redressal process if a mobile number was flagged for genuine or mistaken reasons that are of no fault to the users. If a person who has travelled abroad for a while leading to inactivity of their mobile number or has ported their number to another telecommunication operator, has had their mobile number flagged due to inactivity, whom should they appeal to against the suspension?
Telecom experts on the other hand have found these measures entirely unnecessary for the problems that these rules claim to combat like temporary VoIP lines used by fraudsters or customer service numbers used by fraudsters. They suggest that this could be solved by directly working with telecom operators and platforms.[35]

The EECC tries to deal with internal market, competition, and end-user rights, therefore focusing on encouraging network deployment, ensuring interoperability, and guaranteeing strong consumer protections. The Telecommunications amendment aims to deal with telecom enabled cyber fraud and prevent the abuse of mobile numbers. Under the EECC OTTs are subjected to lighter security requirements that are appropriate to the risk. The 2025 amendment on the other hand has high intervention from the Government and the TIUEs face a higher compliance burden including the financial and technical responsibility of integrating and utilizing the MNV system.

The definition of Telecommunications Identity User Entity was not defined in the Telecommunication (Cyber Security) Rules nor in the Telecommunications Act of 2023, wherefor the inclusion of the OTT Platforms within the purview of the Act by way of the 2025 amendment and the establishment of an MNV Platforms raises questions of excessive delegation, absence of procedural safeguards and unchecked executive authority. The ***re: Delhi Laws Case***[36], the Supreme Court held that the delegating legislation should lay policy and standards of the delegating authority which the delegated authority can execute; in order to pass the test of arbitrariness the delegated legislation should have a parent act that lays down clear guidelines, powers and functions of the delegated authority that can exercise the power, nonetheless neither the constitution of a MNV platform nor a redressal mechanism against its decisions is provided in the amended rules. The MNV platform is given a blanket power of terminating a mobile number without any opportunity to be heard being provided.

The blanket definition of TIUE definition can risk including multiple entities that merely use mobile numbers for ancillary uses like delivery updates. There is privacy concerns raised since the system creates metadata trails linking mobile numbers to online services thus mandating identity validation for users across digital platforms and posing risk to user privacy and user anonymity. These checks will happen in the background invisibly therefore the users have no way of knowing if they have been verified or rejected. The amendment assumes a one-to-one relationship between user, a device, and their telecom identifiers, however in reality most households have 1 or 2 mobile numbers that are used by the entire family. This can lead to a situation where legitimate users can be rejected from essential digital services.

III. CONCLUSION

The paper aims to understand the position of the OTT players in comparison to its telecom counterparts. OTT platforms subsume a vast variety of services leading to the primary and most important problem when it comes to their regulation. Identifying a comprehensive mechanism for classifying the OTT platforms in terms of the services offered by them would ease the process. The paper does not try to give a one size fits all solution; however, it aims to understand the services that have become an integral part of every person's life despite cultural, economic, regional differences. It aims to shed light on a discussion that has been going on for a while on the sidelines. Though numerous countries have not

[35]Charles Assisi, The Many Troubling Questions About Upcoming MNV System, Hindustan Times (July 19, 2025, 06:44 a.m. IST), https://www.hindustantimes.com/india-news/the-many-troubling-questions-about-upcoming-mnv-system-101752893678999.html (last visited Nov. 1, 2025).

[36] In re Delhi Laws Act, AIR 1951 SC 332, 1951 SCR 747 (India).

subjected OTT platforms to telecom regulations, they are only subjected to content moderation; there is a pressing need in India to regulate the OTT players. The global regime though slightly shifting to subject OTT platforms to telecom regulations have undertaken only a lighter less hands on approach. The unique demographic construct of India poses a different challenge and an even pressing need for this unique amalgamation of telecom and cybersecurity regime. It stresses the importance of keeping things fair between OTT platforms and traditional telecom providers, suggesting a simpler licensing system that still covers essentials like data localization and security. However, the regulation should have procedural safeguards, open public discussions, and privacy security.

IV. SUGGESTIONS

1. Regulatory Harmonization

OTT platforms should not be subjected to multiple regulations, under the governance of multiple different regulators. This discourages upcoming players in the market, affecting small players disproportionately. Rules should be aligned with parallel frameworks like RBI rules, DPDP Act and CERT-In to prevent duplicative or contradictory requirements.

2. Calibrated Obligation

While OTT platforms should be subjected to cybersecurity regulations they should be calibrated based on the risk and entity size through exemption or lighter compliance for MSMEs.

3. Calculated Categorizations

OTT players are of multiple types and has been rightly categorized as OTT communication services and OTT entertainment services. To resolve the jurisdictional differences, OTT Communication Services should be permitted to be governed by MIB while OTT entertainment should be governed by MeitY and consequentially IT Act, Rules, and DPDP Act.

4. Transparency and Privacy Safeguards

The MNV system involves sensitive identity verification therefore should be a public-facing audit mechanism so that the MNV platform is not abused behind closed doors. A dashboard could be implemented that shows the users if their mobile numbers were verified or not.

5. Appeal mechanism

An appeal mechanism to fix errors if numbers were wrongly flagged should be provided. Any temporary emergency suspension must be limited to high-risk cases and subject to post-facto review and appeal.

6. Procedural Safeguards

The rules must codify who may issue directions, on what basis and with oversight.

REFERENCES

[1] The Hindu Bureau, 27.5 GB Average Monthly Data Consumed by Indians, FWA Using 12× More Data Than Mobile Users, The Hindu (May 25, 2025), https://www.thehindu.com/sci-tech/technology/indians-consuming-275-gb-average-monthly-data-fwa-using-12x-more-data-than-mobile-users/article69352909.ece (last visited Nov. 1, 2025).

[2] Broadcasting Services (Regulation) Bill, 2023, Gazette of India, Extraordinary, Part II, Sec. 2 (Dec. 2023) (India)

[3] Broadcasting Services (Regulation) Bill, § 2(1)(y) (2023) (India).

[4] International Telecommunication Union, Technical Report on Economic Impact of OTTs (2017), https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ECOPO-2017-PDF-E.pdf.

[5] Telecom Regulatory Authority of India, Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services, Consultation Paper No. 10/2023 (July 7, 2023).

[6] Body of European Regulators for Electronic Communications (BEREC), BEREC Report on OTT Services (2016).

[7] Broadcasting Services (Regulation) Bill, 2023, supra note 2,

[8] A.K. Bhargava et al., Net Neutrality Committee Report (Dept. of Telecommunication May 2015), https://dot.gov.in/sites/default/files/Net_Neutrality_Committee_report%20%281%29_0.pdf (last visited Oct. 27, 2025).

[9] TRAI, supra note 5, at

[10] Id.

[11] Id.

[12] Chaitanya Ramachandran, How to Design an Indian Net Neutrality Law, 12 Indian J.L. & Tech. 1 (2016).

[13] Srishti Gupta et al., Exploiting Phone Numbers and Cross-Application Features in Targeted

Mobile Attacks, SPSM '16, Oct. 24, 2016, at 1, http://dx.doi.org/10.1145/2994459.2994471.

[14] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, Sec. 3(i) (Feb. 25, 2021).

[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 2(u), Gazette of India, Extraordinary, Part II, Section 3(i) (Feb. 25, 2021).

[17] Ashaawari Datta Chaudhuri, Do OTT Platforms Deserve a Separate Regulation? Centre for Rsch. & Analysis in Fin., Tech. & L. Working Paper No. 2/2021 (2021).

[18] All India Digital Cable Fed'n v. Star India Pvt Ltd, BROADCASTING PETITION/217/2023 (Telecom Disputes Settlement & Appellate Tribunal Oct. 4, 2023).

[19] Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017, Telecom Regulatory Authority of India, Gazette of India, Extraordinary, Part III, Sec. 4 (Mar. 3, 2017) (India).

[20] The Indian Telegraph Act, No. 13 of 1885, § 3(1AA), INDIA CODE (1885).

[21] Broadcasting Services (Regulation) Bill, 2023, supra note 2,

[22] Directive (EU) 2018/1972, art. 2(4), establishing the European Electronic Communications Code (EECC), 2018 O.J. (L 321) 36.

[23] Case C-142/18, Skype Commc'ns Sàrl v. Institut belge des services postaux et des télécommunications (IBPT), ECLI:EU:C:2019:460, (June 5, 2019).

[24] Christoph J.J. Engelmann, ECJ Clarifies Scope of Telecoms Regulation for OTT Services, Technology's Legal Edge (July 2, 2019), https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/ (last visited Oct. 29, 2025).

[25] Case C-193/18, Google LLC v. Bundesrepublik Deutschland, ECLI:EU:C:2019:492 (June 13, 2019).

[26] Skype Commc'ns Sàrl, supra note 23,

[27] Shim Woo-hyun, Korea Reveals Details of "Netflix Law", The Korea Herald (Sept. 8, 2020), https://www.koreaherald.com/article/2416335 (last visited Oct. 30, 2025).

[28] Y. Bae et al., OTT, IDC and Cloud-Computing Services under Telecom Law 2023, Int'l Bar Ass'n (2024), https://www.ibanet.org/OTT-IDC-and-Cloud-Computing-services (last visited Oct. 30, 2025).

[29] Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 2(1)(i), G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[30] Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 7A, G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[31] Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 5, G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[32] Telecommunications (Telecom Cyber Security) Amendment Rules, Rule 3(a)(aa), G.S.R. 771(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Oct. 22, 2025) (India).

[33] Telecommunications (Telecom Cyber Security) Rules, Rule 4(3), G.S.R. 520(E), The Gazette of India: Extraordinary, Part II, Sec. 3(i) (Aug. 28, 2024) (India).

[34] DoT Brings OTTs Under Mobile-Number Validation Framework, The Hindu BusinessLine (Oct. [date] 2025),https://www.thehindubusinessline.com/info-tech/dot-brings-otts-under-mobile-number-validation-framework/article69741394.ece (last visited Nov. 1, 2025).

[35] Pranav Bhaskar Tiwari, Written Comments: Draft Telecom Cybersecurity Amendment Rules (The Dialogue July 2025).

[36] Charles Assisi, The Many Troubling Questions About Upcoming MNV System, Hindustan Times (July 19, 2025, 06:44 a.m. IST), https://www.hindustantimes.com/india-news/the-many-troubling-questions-about-upcoming-mnv-system-101752893678999.html (last visited Nov. 1, 2025).

[37] In re Delhi Laws Act, AIR 1951 SC 332, 1951 SCR 747 (India).