To,

Shri Akhilesh Kumar Trivedi,
Advisor (Network, Spectrum & Licensing), TRAI

Sub: Stakeholder comments on the Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services dated July 7, 2023 ("OTT Consultation Paper")

Dear Sir/Madam,

We welcome the opportunity extended by the Telecom Regulatory Authority of India ("**TRAI**") to stakeholders for providing comments on the OTT Consultation Paper through your press release dated July 7, 2023.

IndusLaw is a law firm with offices in Bengaluru, Chennai, Delhi, Hyderabad, and Mumbai. It has been our constant endeavour to regularly contribute to thought leadership and policy formulation for the country for various industries, and to support government initiatives through our submissions and research. Over the years, IndusLaw has been advising a wide spectrum of clients in the technology and media space, including clients in the OTT and telecommunications sectors. We have also undertaken comprehensive comparative studies across various jurisdictions and provided inputs based on our experience and research to assist the government in shaping the direction and content of their policies.

Through our policy advocacy efforts, IndusLaw's focus has been to act as a bridge between the industry and the regulator, to not just enable a meaningful regulatory regime but also ensure its smooth and effective implementation. As we represent multiple stakeholders impacted by the questions posed in the OTT Consultation Paper, we are happy to continue to provide our inputs in this journey for the TRAI.

The submission herein represents IndusLaw's response to the TRAI's OTT Consultation Paper.

1. Regulating Internet Based Communication Services

1.1 The enduring commitment of the TRAI to ensure a level-playing field between communication services provided by traditional telecommunications service providers i.e., service providers licensed under Section 4 of the Indian Telegraph Act, 1885 ("**TSPs**") and Internet Based Communication Services (i.e., OTT Communication Services) ("**IBCS**") is noted and appreciated. It is also one of the primary arguments advanced for the regulation of the latter. However, there are technical and functional features that separate IBCS from TSPs which we have briefly touched upon here. IBCS should not be deemed as substitutes for traditional TSPs owing to their absolute and complete dependence on TSPs. For instance, while the TSPs have exclusive rights over the allocated spectrum and corresponding obligations concerning its efficient use, IBCS do not have control over the underlying network infrastructure. In fact, most IBCS (such as audio calling service providers and/or video calling service providers) only provide a software solution free of charge, which is accessible over an already regulated telecommunication network (i.e., internet) versus the traditional telecommunication services providers that are direct/primary users of the spectrum. This is a fundamental difference between the two categories.

1.2 For the purposes of understanding the aforementioned, it is helpful to distinguish between the "application layer" and "network layer". IBCS, operating in the application layer, are delivered over a licensed network of a TSP which forms the network layer. TSPs have access to both the 'network' and 'application' layers since they retain the rights to offer public access thereto vide the terms of their Unified License Agreement with the Department of Telecommunications ("**ULA**"). Accordingly, in the absence of any control over the network layer, IBCS are precluded from even offering their services to users without relying on a TSP for the requisite internet infrastructure.

1.3 Notably, the TRAI already regards this separation of the 'application' and 'network' layers as a corollary of the technological advancements being undertaken in the sector.[1] Accordingly, subjecting entities that only offer their services (not being a scarce public resource) over the TSPs' networks to obligations similar to those levied on TSPs does not have sufficient basis and rationale and would be disproportionate.

1.4 Additionally, while the OTT Consultation Paper makes note of the differing obligations of OTTs and TSPs,[2] it must also be noted that the TSPs have been given some exclusive rights such as those concerning the right to a) acquire spectrum, b) have an independent network for transmission and delivery, c) interconnect with PSTN, d) manage their infrastructure for undertaking end-to-end operations, and e) obtain numbering resources,[3] *inter alia*. The inherent differences between TSPs and IBCS necessitates the imposition of differing obligations since the latter only provide their services over the former's network infrastructure, having no autonomy over the utilization of the network infrastructure. Lastly, the revenue generation models of IBCS providers (which are mostly advertisement driven) are different compared to the traditional TSPs (which are subscription, usage, and meter based).[4]

1.5 In this context, we can place some reliance on the European Union (EU), where only number-based interpersonal communication services ("**NB-ICS**"; which connect using publicly assigned numbering resources) are strictly regulated and licensed, leaving number-independent interpersonal communications services ("**NI-ICS**"; which do not connect using publicly assigned numbering resources) such as some forms of IBCS subject to a light touch set of obligations and, that too, only where public interest specifically demands it.[5] Per the lighter-touch regulatory framework envisioned for NI-ICS under the European Electronic Communications Code ("**EEC**"), several exemptions have been granted to such platforms, including exemptions from undertaking general authorisation and registration,[6] since they neither maintain a publicly-

[1] TRAI, 'Recommendations on Regulatory Framework for Internet Telephony' (2017), available here: "The separation of network and service layers of telecom service offerings is the natural progression of the technological changes in this domain. It is now possible to separate provision of service contents, configuration and modification of service attributes regardless of the network catering to such service."
[2] OTT Consultation Paper, pg 41-44.
[3] Asia Internet Coalition, 'Comments on the Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services in India' (*AIF*, 10 December 2018) available here; Internet Freedom Foundation, 'Counter-comments to the Consultation on OTT Platforms and Services' (*IFF*, 21 January 2019) available here.
[4] OTT Consultation Paper.
[5] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code ("**EEC**"), available here.
[6] Article 12(2) of the EEC; 'Improving Member States' approaches to number-independent services in light of the EECC' (*Digital Europe*, 29 November 2022) available here.

assured interoperable system nor benefit from the utilization of public numbering resources.[7] Prescribing lighter obligations on NI-ICS pertaining to the establishment of appropriate technical and organisational measures to manage security risks[8] has also been proposed in the EEC since NI-ICS platforms do not exercise actual control over the transmission of signals over publicly-accessed networks.[9] Additionally, from the standpoint of end-users' rights prescribed in the EEC,[10] microenterprises offering NI-ICS services are only obligated to comply with obligations regarding non-discrimination,[11] and safeguarding of end-users' fundamental rights.[12] IBCS providers (constituting NI-ICS under the EEC) have a new set of obligations imposed onto them which largely focus on areas of security,[13] accessibility for specially-abled end-users,[14] emergency services,[15] etc.

1.6 The approach of the EU seems commensurate to the principle of following a risk-based and public-interest oriented approach to regulation where over-regulation of IBCS has been avoided by recognising the distinction between NB-ICS and NI-ICS. Similar to this, other agencies of the Government of India have also followed the above approach. For example, the Ministry of Electronics and Information Technology ("**MeitY**") has adopted such an approach in the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021. At its core, it is recommended that India should identify, analyze, and prioritize the risks that these distinct set of industries pose and focus its efforts on mitigating the most serious ones.

1.7 Drawing parallels from this balanced approach adopted by EU, we strongly recommend that a clear distinction may be built into the Indian legislative framework to mirror the operational model of distinction, and regulations/obligations should be imposed proportionately on IBCS. This approach is consistent with the understanding that the application layer is distinct from the network layer and any potential regulatory intervention should not be agnostic to this technological difference. Technological differences such as the presence or absence of spectrum, use of public numbering resources, interconnection capabilities, etc., constitute *intelligible differentia* between the two classes of businesses, i.e., in case of TSPs, one involving a finite natural resource and the other not involving such a finite natural resource.

1.8 Further, it is pertinent to clearly mention the categories of IBCS' that may be subject to regulations, if any. It is to be noted that not all IBCS' primary object is to facilitate communications. For example, a taxi aggregation platform provides its users an option to communicate with the taxi driver; however, the primary purpose of such platform is travel. Similarly, a food aggregation platform provides the users an option to communicate with the restaurant or the delivery agent. Treating such applications on the same footing as a messaging/calling service provider would be disproportionate and unreasonable.

[7] Recital 44 of the EEC.
[8] Article 40 of the EEC.
[9] Recital 95 of the EEC.
[10] Title III of the EEC.
[11] Article 99 of the EEC.
[12] Article 100 of the EEC.
[13] Article 40 of the EEC.
[14] Article 103 of the EEC.
[15] Article 59 of the EEC.

1.9 It would be apposite to regulate IBCS under the Information Technology Act, 2000 ("**IT Act**") and the rules framed thereunder, given that such service providers are already subjected to a light-touch regulation therein basis their classification as 'intermediaries'[16] and 'social media intermediaries'.[17] Notably, obligations such as the institution of grievance redressal mechanisms, reporting of cybersecurity breaches, and interception/monitoring of computer resource(s) have already been levied on IBCS under this framework. Under the current allocation of government business, regulation of IBCS and other internet-based platforms is MeitY's responsibility.[18] Accordingly, MeitY has proposed to replace the IT Act with a 'Digital India Act', and with the recently-notified Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), there will be a significant overlap in the regulatory mechanisms available to regulate IBCS. For example, aspects such as the maintenance of security and integrity of data collected by IBCS platforms would soon be governed by the DPDP Act and the rules framed thereunder. Hence, it would be prudent to not disturb the *status quo* by introducing an entirely new set of regulations by bringing IBCS under the Department of Telecommunications' and TRAI's domain.

1.10 Hence, TRAI may contemplate adopting its earlier recommendation viz., allowing the market forces to respond to the situation without prescribing any regulatory intervention.[19] This has become particularly crucial in light of the current narrative surrounding the regulation of IBCS, with the proposed enactment of the Digital India Act and the recent notification of the DPDP Act, the enforcement date of which is yet to be notified. This approach could be undertaken since (a) there appears to no clarity on whether IBCS platforms could be treated as perfect substitutes or complements of traditional TSPs, as also highlighted by TRAI in the OTT Consultation Paper,[20] and (b) to minimise the chances of regulatory clashes since the implications of the DPDP Act and the overhaul of the IT Act regime by the proposed Digital India Act on IBCS can only be assessed once such changes are enacted.

1.11 Basis our foregoing observations, we recommend that the TRAI may consider the following courses of action on the regulation of IBCS:

(i) Allowing IBCS to be regulated as intermediaries under the IT Act regime and subsequently under the proposed Digital India Act; and

(ii) Allowing market forces to respond to the situation without undertaking any legislative intervention, in light of the ongoing as well as the proposed regulatory developments in the sector.

2. Banning of OTT Services

2.1 TRAI is empowered under the Telecom Regulatory Authority of India Act, 1997 ("**TRAI Act**") to provide its recommendations in respect of IBCS towards facilitating competition and

[16] Section 2(w) of the IT Act states that an "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.
[17] Rule 2(w) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 defines "social media intermediaries" to mean an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
[18] The Government of India (Allocation of Business) Rules, 1961, available here.
[19] TRAI, 'Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services', available here.
[20] OTT Consultation Paper, pg 37.

promoting efficiency in the operation of telecommunication services.[21] However, it is respectfully submitted that the TRAI is not empowered to make recommendations concerning OTT applications beyond IBCS. The questions posed by TRAI in the context of selectively banning certain OTT services may not fall within the purview of TRAI's mandate, which could make any regulation introduced in this regard subject to challenge. For brevity, our responses are focused on addressing the selective banning of IBCS, which are within 'TRAI's regulatory ambit and relevant to TRAI.

2.2 The issue of selective banning of IBCS has, in our assessment, already been adequately covered by Section 69A of the IT Act, which grants the government wide powers to deal with such situations. Section 69A empowers the government to issue directions for blocking access to specific content on the internet, if it is deemed necessary in the interests of national security, public order, or preventing certain offenses. While we acknowledge the existence of concerns surrounding the implementation of Section 69A,[22] in terms of transparency, due process, and potential abuse of power, we are optimistic that these concerns could be addressed in future consultations, particularly in the context of the upcoming Digital India Act. The Digital India Act, if appropriately drafted and implemented, could provide a more comprehensive and effective framework for dealing with issues related to the regulation of digital services, including the selective banning of IBCS applications.

2.3 In this context, we applaud TRAI's intent in minimizing blanket internet shutdowns, as such broad shutdowns can have severe negative consequences on the affected population. Blanket shutdowns can lead to communication disruptions, hinder access to essential services, impact businesses, and impede the free flow of information and payments, which is crucial in this digital age. As we move forward, it is vital to strike a balance between national security and public order concerns and safeguarding the rights of individuals and businesses in the digital space. Transparent and accountable mechanisms must be put in place to ensure that any restrictions or bans on digital services are proportionate, necessary, and in line with the principles of a free and open internet.

3. Responses to specific questions

Question 1: What should be the definition of over-the-top (OTT) services? Kindly provide a detailed response with justification?

Question 2: What could be the reasonable classification of OTT services based on an intelligible differentia? Please provide a list of the categories of OTT services based on such classification. Kindly provide a detailed response with justification.

[21] In accordance with Section 11(a)(iv) of the TRAI Act, TRAI's functions include providing recommendations on request by the Central Government for measures to facilitate competition and promote efficiency in the operation of telecommunication services to facilitate growth in such services.
A 'telecommunication service' has been defined in the TRAI Act as a "service of any description (including electronic mail, voice mail, data services, audio tax services, video tax services, radio paging and cellular mobile telephone services) which is made available to users by means of any transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature, by wire, radio, visual or other electromagnetic means but shall not include broadcasting services."
[22] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

Question 3: What should be the definition of OTT communication services? Please provide a list of features which may comprehensively characterize OTT communication services. Kindly provide a detailed response with justification.

Question 4: What could be the reasonable classification of OTT communication services based on an intelligible differentia? Please provide a list of the categories of OTT communication services based on such classification. Kindly provide a detailed response with justification.

INDUSLAW's Response: As noted in the OTT Consultation Paper,[23] there have been several attempts to define 'OTT services' over the years by regulators and international bodies. These attempts to define have largely focused on the following key ingredients:

(i) a service or an application; and
(ii) delivered or provided over the public internet.

In a regulatory sense, the term 'OTT' is often referred to in the context of internet-based services that provide access to services independent of a legacy network or facility dedicated to its distribution or provision. These services, *inter alia*, include content streaming services (contrasted with traditional broadcasting) and communication services (contrasted with telecommunication voice and messaging).

Categorisation of OTT Services

OTT services, as noted in the Consultation Paper, consist of a wide variety of online services including communication, media, e-commerce, social media, cloud storage, etc. These services may be classified based on their functionality to end-users. The 2015 Department of Telecommunications (DoT) Report on Net Neutrality ("**DoT Report**") classifies OTT services into two groups, viz., (i) OTT Communication Services and (ii) OTT Application Services. According to the DoT Report, OTT Communication Services are classified as distinct from other OTT Application Services as the latter use the network infrastructure created by TSPs but do not directly compete with the service offerings for which the TSPs have obtained a licence under applicable laws.

However, classifying OTT services into distinct categories poses challenges due to their dynamic and evolving nature. Many OTT applications now offer multiple distinct services within a single platform, blurring the lines between communication, media, and e-commerce functionalities. For instance, an OTT application might provide a social media feed, voice calling, and messaging features, making it difficult to pinpoint its core function and ancillary functions. Moreover, some OTT applications that primarily engage in e-commerce, food delivery, or cab aggregation also integrate communication functionalities, further complicating the classification process. This integration of communication features within various service offerings challenges the clear identification and isolation of the core communication function of OTT services. The constantly evolving landscape of OTT services necessitates the need for a flexible approach in regulating and classifying them.

Further, with the introduction of more than one core feature in apps, it becomes difficult to classify exactly what constitutes a communication app. For instance, the rise of "Super Apps" which are used for communication, payments and e-commerce with each feature being capable of used standalone complicates this categorisation.

[23] OTT Consultation Paper, pg 21-22.

In this context, we can place some reliance on the EU wherein the ECC reformed the framework for the regulation of electronic communications services and networks across the European Economic Area. The ECC defines 'interpersonal communications service' ("**ICS**") as a service that is normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Sub-categorisation of OTT services into communication services (i.e., IBCS) while not straightforward as noted above, can be based on some common factors such as assessing the core-functionality of a feature in an application. The following two-fold test may be employed in order to assess the core functionality:

(i) the OTT service should be same or similar to communication services provided by TSPs; and
(ii) the OTT service should be capable of being used on a stand-alone basis, not to facilitate the provision of a separate service that does not qualify as a communication service.

However, any regulation that specifically applies to a class of such services must showcase a reasonable nexus between the classification and the objective sought to be achieved by the regulation.[24] In addition to strict functionality, any potential regulation should also be mindful of the inherent technological differences underlying a service.[25]

Question 5: Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:
(a) regulatory aspects;
(b) economic aspects;
(c) security aspects;
(d) privacy aspects;
(e) safety aspects;
(f) quality of service aspects;
(g) consumer grievance redressal aspects; and
(h) any other aspects (please specify).

Kindly provide a detailed response with justification.

Question 6: Whether there is a need to bring OTT communication services under any licensing/regulatory framework to promote a competitive landscape for the benefit of consumers and service innovation? Kindly provide a detailed response with justification.

Question 7: In case it is decided to bring OTT communication services under a licensing/ regulatory framework, what licensing/ regulatory framework(s) would be appropriate for the various classes of OTT communication services as envisaged in the question number 4 above? Specifically, what should be the provisions in the licensing/ regulatory framework(s) for OTT Communication services in respect of the following aspects:
(a) lawful interception;

[24] Ajay Hasia v. Khalid Mujib, (1981) 1 SCC 722.
[25] GSMA, 'A new regulatory framework for the digital ecosystem' (2016), available here.

(b) privacy and security;
(c) emergency services;
(d) unsolicited commercial communication;
(e) customer verification;
(f) quality of service;
(g) consumer grievance redressal;
(h) eligibility conditions;
(i) financial conditions (such as application processing fee, entry fee, license fee, bank guarantees etc.); and
(j) any other aspects (please specify).
Kindly provide a detailed response in respect of each class of OTT communication services with justification.

INDUSLAW's Response: Please refer to our analysis and conclusions on regulating IBCS under paragraphs 1.7 to 1.11 above. In accordance with our observations above, adoption of the 'same service same rules' approach by the application of traditional regulatory and licensing requirements to OTT Services will be a huge step backwards. The fundamental technical differences between TSPs and OTT services do not necessitate any licensing requirements for the latter as they do not deploy critical network infrastructure.

Additionally, we would also like to highlight that there are some obligations imposed on IBCS under the IT Act, akin to those imposed on TSPs under the ULA and other applicable laws, the same is captured in the table below. That said, it is suggested that IBCS that are functionally similar to the services of a TSP (such as voice calling and SMS) may be brought under limited regulatory parity – regulatory intervention may be required in certain critical areas of concern such as privacy, security and key areas of consumer concern. We believe that IBCS offered in a competitive market with low barriers to entry may be subjected to a light-touch regulatory framework, to allow the industry to self-regulate based on market forces. While some of our responses may imply changes to the IT Act, our overall view remains that these issues may be taken up in consultations for the Digital India Act.

No.	Aspect	TSPs	IBCS	IndusLaw's Response
(a)	Security and Lawful interception	TSPs are required to comply with lawful interception orders received from the government under the Indian Telegraph Act, 1885.[26] The ULA also requires TSPs to provide requisite interception facilities in accordance with the requirements.[27]	IBCS are required to comply with interception and decryption requirements under the IT Act.	Legal requirements relating to lawful interception have already been provided for both TSPs and IBCS. The requirements for interception for TSPs under the Telegraph Act, 1885 and IBCS under the IT Act are akin to each other, giving the government similar powers under both statutes.

[26] Section 5 of the Telegraph Act, 1885.
[27] Clause 23.1 of the ULA.

				However, the implementation of interception provisions would be more effective in case of TSPs as the ULA mandates that the TSP should have the requisite technical facilities for interception. The same is not the case with IBCS as there are no such prerequisites. The DPDP Act also obligates 'data fiduciaries' to implement reasonable security safeguards targeted towards preventing data breaches.[28] This compliance would have to be undertaken in addition to the obligations prescribed under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Interception Rules**"), such as providing assistance to the authorised agencies for the purpose of interception,[29] and instituting effective internal checks against unauthorised interception.[30] Similar obligations, including one on maintenance of accurate records has also been prescribed under the CERT-In directions.[31] In this regard, it is recommended that IBCS should be required to have in place requisite technology infrastructure to honour interception and decryption requests. This may be achieved through suitable amendments to the IT Act and the Interception Rules.

[28] Section 8(5) of the DPDP Act.
[29] Rule 19 of the Interception Rules.
[30] Rule 20 of the Interception Rules.
[31] MeitY, Indian Computer Emergency Response Team (CERT-In), Notification No. 20(3)/2022-CERT-In, pg 4.

(b)	Privacy and Cybersecurity	The ULA requires TSPs to ensure protection of privacy of communication and to ensure that unauthorized interception of messages does not take place.[32] However, the ULA prohibits TSPs from employing bulk encryption on their networks.[33]	IBCS are required to ensure privacy of any sensitive personal data or information in terms of Section 43A (and the rules notified thereunder) of the IT Act. They are required to take all reasonable measures to secure their computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.[34]	The enactment of the Digital Personal Data Protection Act, 2023 will overhaul the data protection regime in India for all entities that collect personal data of individuals. Both TSPs and IBCS will be subject to requirements for protecting personal data of individuals by implementing reasonable security safeguards to prevent breach.[35] It must be noted that end-to-end encryption is a commonly seen feature of all communications on IBCS apps; bulk encryption is prohibited for TSPs under the ULA. Thus, TSP services pose a greater privacy and cybersecurity risk to individuals. There may be no need for any regulatory intervention as users of IBCS enjoy better privacy and cybersecurity than their TSP counterparts.
(c)	Emergency Services	TSPs are required to provide access to all public utility services as well as emergency services including toll-free services like police, fire, ambulance.[36]	None	The effectiveness of emergency communication services should be assessed on interoperability, ubiquity and ease of access. IBCS operate on closed clouds and cannot be used to communicate with other services unless technically enabled to do so by cooperation between TSPs

[32] Clause 39.4 of the ULA.
[33] Clause 37.1 of the ULA.
[34] Rule 3(1)(i) of the of the Information Technology (Guidelines For Intermediaries and Digital Media Ethics Code) Rules, 2021.
[35] Section 8(5) of the DPDP Act.
[36] Clause 7.1 of the ULA.

				and IBCS. Moreover, only the largest IBCS would be effective in terms of ubiquity and ease of access. Hence, as most IBCS do not offer interconnection with a public-switched telephone network, it would be redundant to impose such obligations on the former since users continue to rely on traditional TSPs for accessing these services.
(d)	Quality of Service	TSPs are required to comply with the service standards notified by the TRAI and in terms of the ULA.	None	Quality of service for IBCS varies, to a large extent, on the underlying network coverage. Given the dependence of IBCS on TSPs' network coverage, there may not be a need for regulatory intervention.
(e)	Consumer Grievance Redressal	TSPs are required to be responsive to complaints filed by the subscribers in accordance with the ULA.[37] Further, in accordance with Telecom Consumers Complaint Redressal Regulations, 2012, each TSP is required to have a complaint resolution centre which must resolve complaints within a specified timeframe.	IBCS being intermediaries are required to appoint a Grievance Officer and comply with grievance redressal obligations in line with the IT Act (read with the rules framed thereunder).[38] Further, in case of SSMIs, the consumer grievance requirements are much more elaborate.[39]	The requirements of Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 are sufficient to address any consumer grievances that may arise on IBCS. Accordingly, there is no requirement of regulatory intervention. Any shortcomings in the current regime may be more suitably addressed in the consultations for the upcoming Digital India Act.
(f)	Unsolicited Commercial Communic	TSPs have several obligations under Telecom Commercial Communications	None	Section 66A of the IT Act, would have covered the issue of spamming on IBCS but the same has been struck down by the

[37] Clause 29.3 of the ULA.
[38] Rule 3(2) of the Information Technology (Guidelines For Intermediaries and Digital Media Ethics Code) Rules, 2021.
[39] Rule 4(1)(c) of the of the Information Technology (Guidelines For Intermediaries and Digital Media Ethics Code) Rules, 2021.

	ations and Spam	Customer Preference Regulations, 2018 to keep spam and unsolicited commercial communications under control.		Supreme Court as being unconstitutional. Hence, regulatory intervention on this ground is justified. An anti-spamming provision may be added to the existing IT Act.
(g)	Customer Verification	TSPs are required to ensure verification of customers before onboarding them on as subscribers in accordance with instructions issued by the government.[40]	None	Customer verification is an area of significant imbalance between IBCS and TSPs. However, mandating customer verification for IBCS is not feasible as it would be too onerous for small scale and homegrown applications. Such a move would effectively drive such smaller players out of the market given their lack of financial and technical capabilities to implement customer verification. Only restricting customer verification to large online platforms (such as those classified as SSMIs) would also not achieve the intended security outcomes as it would drive user traffic to those applications that do not have such a requirement. Hence, it would be prudent to not disturb the *status quo* at this stage.
(h)	Roll-out Obligations	TSPs are required to comply with timelines in relation to roll out of frequencies allotted to a TSP.	None	No regulatory intervention required on these aspects given the inherently distinct nature of services provided by TSPs as operating in the network layer.
(i)	Interconnection	TSPs are required to maintain interconnectivity with other TSPs' networks in accordance with the	None	

[40] Clause 39.17 of the ULA.

		ULA and Telecom Interconnection Regulations, 2018.		
(j)	Universal Service Obligation	The Universal Service Obligation (USO) fund has been established with objective of providing access to basic telecom services to people in remote and rural areas at affordable and reasonable prices. TSPs are required to contribute to the USO fund as part of their license fees.[41]	None	

Q11. Whether there is a need to put in place a regulatory framework for selective banning of OTT services under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force? Please provide a detailed response with justification.

Q12. In case it is decided to put in place a regulatory framework for selective banning of OTT services in the country, -
(a) Which class(es) of OTT services should be covered under selective banning of OTT services? Please provide a detailed response with justification and illustrations.
(b) What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

Q13. Whether there is a need to selectively ban specific websites apart from OTT services to meet the purposes? If yes, which class(es) of websites should be included for this purpose? Kindly provide a detailed response with justification.

Q14. Are there any other relevant issues or suggestions related to regulatory mechanism for OTT communication services, and selective banning of OTT services? Please provide a detailed explanation and justification for any such concerns or suggestions.

Answer:

Section 5(2) of the Telegraph Act, 1885 allows the Central government or the State Government to temporarily suspend telecommunications services in areas affected by unrest on grounds of public emergency or public safety. This power can only be exercised in the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, maintenance of public order or for preventing incitement to the commission of an offence. The rules notified in furtherance of this power, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ("**Internet Suspension Rules**") do not offer any further guidance on the exceptionally wide powers granted to the Central and State Governments.

[41] Clause 18.2.1 of the ULA.

In 2020, the Supreme Court declared that access to the internet is constitutionally protected as part of citizens' right to freedom of free speech and expression and freedom to carry on one's occupation. Further, the Supreme Court also issued directions for imposing internet suspension orders, noting that restrictions on fundamental rights must adhere to constitutional safeguards.[42]

The Parliament's Standing Committee on Communication and Information Technology in its Twenty-Sixth Report noted the need to be able to selectively ban OTT applications in affected areas instead of imposing outright ban on telecom services. As noted in paragraph 2.1 above, we have only provided our recommendation with regards to IBCS as we believe that providing recommendations for OTT services in general is not within the regulatory ambit of TRAI.

As further noted above in paragraph 2.2, Section 69A of the IT Act may be utilised by the Central Government to ban applications, whereby it can direct not only TSPs but also app store providers to block access to information hosted on a computer resource.[43] The provision, akin to Section 5(2) of the Telegraph Act, 1885, is widely worded allowing the Central Government to direct any intermediary (which includes IBCS) to block any information generated, transmitted, received, stored or hosted in any computer resource from access by the public. Further, powers under Section 69A are to be exercised in accordance with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Blocking Rules**").

Basis our analysis of Section 69A of the IT Act, we note that the circumstances in which the power to block can be utilised mirrors the allowance made for reasonable restrictions on freedom of speech in Article 19(2). Accordingly, there is already a framework in place under the IT Act read with the Blocking Rules to act as a check vis-à-vis concerns pertaining to the maintenance of public order, *inter alia*, which could be relied upon to undertake blocking of any information hosted on a computer resource. The banning of applications through Section 69A is a powerful and an effective tool and we are of the humble view that any desired changes to the blocking regime under Section 69A may be taken up during the consultation process for the upcoming Digital India Act, where such issues may be addressed more holistically.

Your Sincerely,
For **INDUSLAW**

Avimukt Dar
Founding Partner
M: +91 9818577632
E: avimukt.dar@induslaw.com

[42] Anuradha Bhasin v. Union of India, WP (Civil) No. 1031 of 2019; the directions issued by the Supreme Court include: (1) suspension orders must be published to enable legal challenge before courts; (2) suspension orders must adhere to the principle of proportionality and must not extend beyond the necessary duration; (3) and a review committee must review the internet suspension order within 5 days of its issuance, with a periodic review within every 7 working days thereafter.
[43] Please refer: https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206.