॥न्यायस्तत्र प्रमाणं स्यात्॥
NLU DELHI

NATIONAL LAW UNIVERSITY, DELHI

November 09, 2022

Shri Naveen Kumar

Joint Secretary, Director (Restg.)

Ministry of Communications

Department of Telecommunications

Sanchar Bhawan

20, Ashoka Road, New Delhi - 110001

Subject: Submission of Comments on the proposed draft of the Indian Telecommunication Bill, 2022

Dear Shri Naveen Kumar,

The *National Law University Delhi* (NLU Delhi), established by 'The National Law University Delhi Act, 2007' (Act No. 1 of 2008 National Capital Territory of Delhi) is a public funded university established by the Government of NCT of Delhi on the initiative of the High Court of Delhi. The Chief Justice of India is a visitor of the University and the Chief Justice of the High Court of Delhi is the Chancellor of the University. The *Centre for Communication Governance* (CGG) was established by the University in 2013 to contribute to improved governance and policy making, and to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy. CCG is the only academic research centre dedicated to working on information technology law and policy in India.

CCG regularly engages with various institutions such as the Ministry of External Affairs, the Ministry of Law and Justice, the Ministry of Electronics and Information Technology, and the Competition Commission of India, and seeks to support the executive and judiciary with research on legal, technical and regulatory aspects in the course of their decision-making on issues relating to information technology law and policy.

As part of our work, and given how critical it is to provide policymakers with well-researched and useful material, we are submitting our response to the draft Indian

Telecommunication Bill, 2022. We are thankful to the DoT for giving us the opportunity to comment on this draft Bill and commend the DoT adopting a public and consultative approach to this amendment process.

For any further information or input please reach out to the Executive Director of the Centre for Communication Governance, NLUD - Jhalak M. Kakkar at jhalak.kakkar@nludelhi.ac.in

With best wishes,

Sincerely yours,

09/11/2022

Prof.(Dr.) Harpreet Kaur

Vice Chancellor (I/c)

Encl: Comments on the draft Indian Telecommunication Bill, 2022

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE DEPARTMENT OF TELECOMMUNICATIONS ON THE DRAFT INDIAN TELECOMMUNICATION BILL, 2022[1]

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in

[1] Authored by Aishwarya Giridhar, Priyanshi Dixit, and Sidharth Deb. Reviewed and Edited by Jhalak M. Kakkar, Shashank Mohan, and Sachin Dhawan. Research support provided by Shreenandini Mukhopadhyay and Shreya Parashar.

Introduction and Summary of Recommendations

The Centre for Communication Governance ("CCG") thanks the Department of Telecommunications ("DoT") and the Ministry of Communications ("MoC") for providing stakeholders with the opportunity to provide substantive inputs on the Draft Indian Telecommunication Bill, 2022 ("Bill"). We appreciate the DoT's decision to use a public consultative process in updating the existing legal framework on telecommunications in India and make it more adaptable for modern considerations. CCG is cognisant of the pressing need for legislative reform to modernise existing frameworks under the Indian Telegraph Act, 1885 ("Telegraph Act"), the Indian Wireless Telegraphy Act, 1933 and the Telegraph Wires (Unlawful Possession) Act, 1950.

Such reform should enable good governance, encourage cyberspace innovation, and protect users' interests. Legal systems must keep pace with the innovation trajectories of telecom and ICT ecosystems which are pushing towards 5G network environments. Our inputs highlight key challenges and opportunities which the DoT must address to strengthen India's legislative framework for telecommunications. In this spirit, our response highlights six key themes that the Government of India must address through the proposed telecom bill, namely: (a) Appropriate Jurisdiction; (b) Overbroad Definitions; (c) Licensing; (d) Interception and Monitoring; (e) Identity Verification; and (f) Suspension of Internet Services. Our submission relies on key principles of the rule of law, constitutional principles, relevant jurisprudence, and industry and international best practices. Our comments below expand on these issues and cumulatively form our response to the Bill that was released for public consultation on 21 September 2022. Our analysis and recommendations through the aforementioned six themes have been summarised below:

1. **Exclude digital/ internet based services from telecommunication regulation**: The Information Technology Act, 2000 ("IT Act") exclusively deals with issues pertaining to the internet and digital platforms, and provides

corresponding regulation and user safeguards. The Bill's proposed inclusion of digital services within telecommunications law may create a parallel legal regime and regulatory confusion that hinders innovation and the ease of doing business. Additionally, this Bill would likely subsist in parallel to the forthcoming Digital India Act which is under development at the Ministry of Electronics and Information Technology ("MeitY"). The Digital India Act is expected to be a comprehensive reform of India's digital and information and communications technology ("ICT") landscape and will likely replace the current IT Act. Therefore, we propose that the telecommunication regulation in India should not include digital services as it would create dual compliances for services which will negatively impact India's overall internet ecosystem.

2. **Revisit the premise of licensing internet based digital and software services**: Telecom Service Providers ("TSPs") require a license to operate in the market since their operations are dependent on the use of spectrum, which is a limited natural resource. It is based on this scarcity that the Government grants exclusive licenses to access and use spectrum to select service providers. The Government's privilege in this regard emerges from spectrum scarcity and the public trust doctrines. Conversely, internet based services do not function with the same scarcities and resource requirements as TSPs. Instead, they offer their services over the internet/ telecom network infrastructure. The internet is an ecosystem of abundance and thus digital service providers need not contend with the same infrastructural scarcities as network operators. Since over-the-top (services that are offered over the internet, hereafter "OTT") services do not require exclusive allocation of a scarce public resource like spectrum, imposing strict licensing requirements on them would hinder innovation, consumer choice and user accessibility. This would contradict Indian policy imperatives like the ease of doing business and inhibit development under flagship programmes like the Digital India campaign.

3. **The Bill should avoid one size fits all regulation**: The Bill in its current form deploys overbroad definitions for several terms including "telecommunication services" and "message". This particular definition will envelope all OTT

communication services, data communication services, email, and other digital platforms within a common licensing regime as all telecom services. Aside from compromising the principle of *legal certainty*, this overbroad definition contributes to a one size fits all regulatory approach for both carriage and content providers. Such a broad approach is antithetical to the internet's innate characteristics and heterogeneities across its network stack. It is also inconsistent with the growing international and domestic consensus that the internet requires differential regulations which are curated to the features and contextual harms which are native to specific types of platforms and services.

4. **The Bill's interception proposals are overbroad and may violate constitutional rights**: The Bill allows the State to order the interception of messages transmitted over telecommunication services or networks in specific situations. The broad definition in the Bill allows this provision to broadly apply to all messages communicated over all digital services, which may amount to a disproportionate restriction on users' right to privacy. Under Indian jurisprudence, measures restricting privacy must: (a) be provided by law; (b) pursue a legitimate aim and be necessary in a democratic society; (c) be proportionate to the need for the interference with the right to privacy; and (d) contain procedural safeguards to prevent against abuse. Existing provisions permitting interception must be re-examined for conformity with these standards and recent Supreme Court jurisprudence. Additionally, interception provisions in the Bill overlap with those in the IT Act and risks creating a parallel regulatory regime over digital services.

5. **The Bill's ID verification proposals may violate constitutional rights to privacy and free expression**: The Bill requires service providers to identify users of their services, and also requires the identity of persons sending messages over telecommunication services to be made available to the recipient. Although these measures may have sought to target cyber-fraud, they also remove anonymity in online communications. Online anonymity and encrypted services can however play a key role in protecting user privacy and the right to free

expression, and mandated identity verification systems can significantly restrict these rights, particularly for minorities and vulnerable populations.

6. **Provisions relating to the suspension of telecommunications services would restrict the right to free expression:** The Bill authorises the State to direct the suspension of communications transmitted or received by telecommunication networks. It allows for the suspension of 'telecommunication services', which would include all digital services, along with phone calls, text messaging, etc. This provision would expand the ambit of suspension powers to allow states to restrict or blacklist specific services, in addition to restricting access to the internet as a whole. The internet plays a key role in exercising fundamental rights such as free expression and education, and in accessing essential services. Wide powers to restrict access to the internet as a whole, as well as specific services can therefore significantly restrict the fundamental rights of users.

The rest of our submission provides detailed analysis for each of the themes and recommendations mentioned here.

1. Jurisdictional overlaps hinder specialised governance

We submit that the Bill's expansive definitions of "telecommunication services", "telecommunication equipment" and "telecommunication networks" will generate jurisdictional uncertainty for participants across India's digital and ICT economy. The Bill would undermine the Government of India's impetus towards specialised regulation for different layers of cyberspace, wherein:

- the MoC is entrusted with licensing and policymaking for carriage-linked infrastructure service providers like TSPs and internet service providers ("ISPs"); and

- MeitY is the nodal authority which administers and governs all other matters in cyberspace including electronic hardware, software, and wider digital platforms and services[2].

The Bill's definitions, enumerated above, empower the MoC and DoT to govern enterprises that offer: (a) digital services like email and "*OTT Communication Services*"; (b) video communication services; (c) "*data communication services*"; (d) internet based communication services; (d) software; and (e) internet-based equipment which fall within the domain of the *Internet of Things* (IoT).

As a result the Bill would undermine MeitY's exclusive and specialised powers (mentioned above) to oversee all policymaking matters relating to information technology, electronics and the internet – except for matters relating to the licensing of internet service providers, which rests with the MoC. Specifically, the Bill's definitions are inconsistent with deliberate amendments under the Allocation of Business Rules which bifurcated and created specialised ministries for telecom, and another for the broader digital environment.[3] In this regard, MeitY also serves as the nodal ministry for all cyber and IT related laws. To this end, MeitY oversees the IT Act, and will likely serve as the nodal Ministry supervising the forthcoming Digital India Act, which reportedly will replace the IT Act and regulate India's OTT and wider digital ecosystem.[4]

---

[2] Cabinet Secretariat, *The Government of India (Allocation of Business) Rules* (1961) 56 <https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_3190.pdf>.

[3] In July 2016, the Government split the erstwhile Ministry of Communications and Information Technology into two specialised ministries: the MoC and the Ministry of Electronics and Information Technology (MeitY). These ministries were meant to serve as specialised administrative institutions wherein:

(a) the MoC licences telecommunications and internet access service providers who own and operate the underlying network infrastructure; and
(b) MeitY could govern hardware/electronics infrastructures as well as services which operate on top of the infrastructure layer of the internet stack.

This change was reflected under the Government of India (Allocation of Business Rules), 1961 (AoB Rules), which operates under Article 77 of the Indian Constitution. This legal framework states that the MoC is responsible for policy making, coordination and licensing for matters like "*telegraphs, telephones, wireless, data, facsimile and telematic services and other like forms of communications.*" The Rules also restrict themselves to explicit references to telecommunications and similar network level infrastructure.

[4] 'Digital India Act to replace IT Rules soon' *Financial Express* (8 September 2022) <https://www.financialexpress.com/industry/digital-india-act-to-replace-it-act-soon/2658980/>; BigTech, 'OTT platforms stare at uncertainty as Centre plans to push through Digital India Act this Winter

The Bill's proposal to include certain software and equipment which fall under the ambit of IoT, contradicts the fact that MeitY has previously invested significant institutional resources in governing these emerging technologies. For instance, MeitY spearheads the regulation and governance of hardware and software elements of cyberspace. It executes such responsibilities through dedicated quality assurance frameworks like the Compulsory Registration Scheme (CRS) for Electronics and Information Technology Goods.[5] Moreover, it steers specialised institutions like the Standardisation, Testing and Quality Certification (STQC) Directorate, the National Institute for Smart Governance (NISG),[6] the National Institute of Electronics and Information Technology (NIELIT), and the Centre for Development of Advanced Computing.[7]

Keeping this overall context of institutional jurisdiction and expertise in mind, the Government of India should revisit its proposal to bring elements of digital services, software and hardware regulation and licensing within the ambit of the DoT and thereby the MoC. Aside from undercutting the clear specialisation and capacities which have been built up over time at MeitY, it will create parallel legal and compliance regimes for several operators within India's cyberspace. It will also compromise consumer choice by delaying citizens' access to cutting edge digital and ICT services from other parts of the globe. Finally, it creates the risk for regulatory arbitrage wherein companies will seek regulatory shelter from whichever authority they deem favourable– and this creates fertile ground for regulatory conflict. We have previously observed such regulatory arbitrage and jurisdictional conflict play out between the telecom regulator and the competition commission on issues like predatory pricing.[8] The Bill should avoid such pitfalls as India's digital economy matures.

Session' *Economic Times* (18 August 2022) <https://government.economictimes.indiatimes.com/news/digital-india/bigtech-ott-platforms-stare-at-uncertainty-as-centre-plans-to-push-through-digital-india-act-this-winter-session/93627140>.

[5] Ministry of Electronics & Information Technology, *Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order* (2021) <https://www.meity.gov.in/esdm/standards>.

[6] National Institute for Smart Governance <https://www.nisg.org/about>.

[7] Ministry of Electronics & Information Technology, MeitY Organisations <https://www.meity.gov.in/content/meity-organisations>.

[8] *Competition Commission of India vs Bharti Airtel &. Ors* Civil Appeal No(s). 11843 of 2018.

2. Overbroad definitions compromise legal certainty and risks one size fits all regulation

The Bill's current definitional approach for multiple concepts like "*telecommunication services*" and "*message*" lends itself to overbroad classification of heterogeneous products and services within the same umbrella category. Overbroad classification negatively impacts legal certainty for regulated subjects– and thus undercuts India's wider economic imperative of ease of doing business. It also creates risks of one size fits all regulation for different products and services across the internet's value chain. We submit that legal certainty is an essential condition when it comes to the democratic rule of law and is also an integral element for economic policymaking. Moreover, one size fits all regulation is inconsistent with the emergent understanding that the internet is better suited to differential regulation which is curated to specific service providers and native problems/ harms which they must contend with. Later in this section our analysis demonstrates the relevance of this thinking around differential regulation through MeitY's experience with regulating online intermediaries under the IT Act.

Telecommunication Services: The Bill's definition of "telecommunication services" is considerably broader than the definition of the same term under the Telecom Regulatory Authority of India Act, 1997. The Bill's definition of "telecommunication services", inter alia, includes electronic mail, video and data communication services, interpersonal communication services, machine-to-machine communication services (which fall within *IoT* services), and 'OTT communication services'.[9] Additionally, the definition does not qualify or explain the scope of any of these terms/ services, and as analysed later, leaves much room for subjective interpretation.

Message: The Bill also defines the term 'message' in an overbroad manner and includes "*any sign, signal, writing, image, sound, video, data stream or intelligence or information intended for telecommunication*", which would include virtually all content

[9] Clause 2(21), draft Indian Telecommunication Bill, 2022.

transmitted online.[10] This is a significant departure and update to the Telegraph Act's definition of the term which is also used within India's Unified Licensing Framework to regulate TSPs and ISPs.[11] The definition of "message" under the current legal framework does not explicitly mention online modes of communication like images, sound, video or data streams.[12] The Bill's proposed definition of "message" clubs traditional SMS in the same category as newer forms of online interactions/ messages like memes, gifs, currency, and other audio-visual messages. The proposed definition is unable to appreciate the dynamic nature of online interactions which differ from the static nature of SMS and other similar telephone services.

At a foundational level, the Bill's overbroad definitions of terms like "telecommunication services" and "message" raises issues of legal certainty and one size fits all regulation as referenced earlier.

A] <u>Undermines legal certainty</u>: The broadest possible interpretation of terms like "telecommunication services" and other related terms[13] means that most digital services and interactions could fall within the scope of telecommunications services. For instance "*OTT communication services*" (one of the categories enumerated within the definition of "telecommunication services") could be interpreted to include all platforms that provide product features which resemble messaging services, even where they are ancillary to their primary services. The unqualified breadth of this sub-category could potentially include the P2P chat features of online gaming platforms or online consumer dispute redressal chat features available on most e-commerce websites. Additionally, the Bill aims to empower the Central Government to notify *"any other service … to be telecommunication services*", further increasing the scope of discretionary application of the law. Such broad scope for interpretation and implementation creates risks of

[10] Clause 2(9), Draft Indian Telecommunication Bill, 2022.
[11] See General, Section 3(3), The Indian Telegraph Act, 1885 r/w License Agreement for Unified Agreement, Ministry of Communications, Government of India, https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf, Page 153.
[12] See generally, Section 3(3), The Indian Telegraph Act 1885.
[13] See Clause 2(18) "Telecommunication Equipment", Clause 2(20) "Telecommunication Network", draft Indian Telecommunications Bill, 2022.

uncertainty and confusion across most commercial and non-commercial participants in India's digital economy.

The potentially broad interpretation of these terms by implementation authorities also comes with substantial compliance requirements. For economic actors under this Bill, it could include terms and conditions prescribed under licensing,[14] registration[15] and/ or authorisation[16] frameworks. This is significant since India's universal licensing framework under current telecom laws is highly prescriptive and provides detailed compliance requirements for regulated subjects.[17] Given the country's historical approach to licensing, it is reasonable to anticipate that similar compliance requirements could arise for digital services, products and hardware manufacturers should they be brought within India's telecommunication regulatory/ licensing fold.

The compliance burden affiliated with broad definitions and unpredictable implementation could trigger unintended ecosystem-wide consequences. To begin with, it is inconsistent with the internet's core principle of permissionless innovation which has previously been endorsed within legal instruments by Indian authorities like the Telecom Regulatory Authority of India ("TRAI").[18] Moreover, the Bill's broad definition and subsequent compliance will act as barriers to entry and exit of services within the country's digital economy. This will have a negative impact on consumer choice and citizens' access to new products and services from the global digital and ICT economy. As a result we submit that the Bill is inconsistent with the Government of India's flagship Digital India programme since "*universal access*" and "*information for all*" are key pillars of the campaign.[19]

---

[14] Clause 3(2)(a), draft Indian Telecommunication Bill, 2022.
[15] Clause 3(2)(b), draft Indian Telecommunication Bill, 2022.
[16] Clause 3(2)(c), draft Indian Telecommunication Bill, 2022.
[17] See Generally: COAI Response to the TRAI Consultation Paper on "Ease of Doing Business in Telecom and Broadcasting Sector" <https://trai.gov.in/sites/default/files/COAI_11022022.pdf>, Consultation Paper On "Ease of Doing Business in Broadcasting Sector", Telecom Regulatory Authority of India, 31July, 2017 <https://www.trai.gov.in/sites/default/files/CP_ease_of_doing_31072017l.pdf>.
[18] Telecom Regulatory Authority Of India, Prohibition Of Discriminatory Tariffs For Data Services Regulations (2016, 9) para 15 <https://trai.gov.in/sites/default/files/Regulation_Data_Service.pdf>.
[19] Digital India, How Digital India will be realized: Pillars of Digital India <https://digitalindia.gov.in/content/programme-pillars>.

Learning from the "OSP" experience: Broad definitions will also lead to uneven and uncertain compliance environments. The Bill should avoid such an outcome since the telecom sector has prior experiences with broad definitions and discretionary implementation. For example, existing licensing and registration frameworks under the current telecom legal regime have been susceptible to inordinate discretion at the behest of administrative authorities.[20] Such discretion has generated legal and regulatory uncertainties for market participants. For example, Other Service Providers (OSPs), have been previously required to register with the DoT and comply with applicable terms and conditions. In this regard OSPs were defined broadly as '*application services*' and included '*tele-banking, tele-medicine, tele-education, tele-trading, e-commerce, call centres, network operation centres and other 'IT Enabled Services*'.[21] This overbroad definition affected market participants since the term had the scope to be potentially interpreted by authorities to require every digital/ IT enterprise to be providing "*IT Enabled Services*". This would have required market participants across India's digital landscape to register with the DoT. This open-ended definition yielded unexpected results since private enterprises were placed with the burden of interpretation and subsequently registering with the DoT. This legal regime had unexpected compliance outcomes wherein most commercial enterprises in the telecom regulatory landscape choose to interpret the definition of OSP in the narrowest possible terms and steer clear of compliance.[22] At the same time the OSP registration framework continued to perpetuate uncertainty. This is because the registration authority i.e. the DoT retained the lawful authority to exercise discretion and either implement the requirement or levy fines/ penalties on delinquent firms. Expert practitioners have previously opined that such regulatory and legal uncertainty makes compliance with Indian telecom laws excessively complex.[23] **We submit that the Bill should strive to evade such pitfalls since legal certainty**

[20] Rahul Matthan, "Telecom" in Regulation in India: Design, Capacity, Performance, Hart Studies in Comparative Public Law (Hart Publishing 2019).
[21] Department of Telecommunications, Revised "Terms and Conditions - Other Service Provider (OSP) Category" (2008) Annexure 1, ch 1(a) <https://dot.gov.in/sites/default/files/OSP%20registration070808.pdf>.
[22] Matthan, "Telecom" in Regulation in India: Design, Capacity, Performance, Hart Studies in Comparative Public Law (n 20).
[23] ibid.

is a key feature of the rule of law[24] and is an integral condition to attract economic investments.[25]

B] <u>Risk of one size fits all regulation</u>: The Bill's overbroad definition of "telecommunication services" could also enable a one size fits all regulation. Clause 3(2)(a) read with Clause 4 of the proposed Bill empowers the Central Government to govern telecommunication services under a licensing framework. Since the Bill does not provide for any differential classification and licensing framework based on the type of service provided, all entities that fall under the umbrella of "telecommunication services" are likely to deal with similar compliance through terms and conditions prescribed under a common licensing framework. This could lead to analogous compliances for fixed and mobile operators, email providers, data communication services and even OTT communication service providers.

We request the Government to revisit the risks associated with broad definitions enabling one size fits all regulatory frameworks since such regimes are inconsistent with the wide heterogeneity of internet markets and surrounding ecosystems. Moreover, the Bill's definitional proposals are a departure from the global understanding of differential regulation for different types of digital service providers which is evident within internet laws since the turn of the millennium.[26] Even in India various authorities like the Competition Commission of India's chairperson have already recognised the problems with one size fits all regulation for digital markets.[27] This position has advocated on the grounds that digital markets need to be regulated in a nuanced manner depending on the

[24] Hans Gribnau, 'Legal Certainty: A Matter of Principle' (2014) Tilburg Law School Research Paper (12) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447386>.
[25] Budiman Ginting, Rosnidar Sembiring, Mahmul Siregar, Afrita Abduh, "The Role of Law in Economic Development: To Develop a Special Economic Zone in Order to Build a National and Regional Economy" in Proceedings of MICoMS 2017 (Emerald Publishing Limited 2018) <https://www.emerald.com/insight/content/doi/10.1108/978-1-78756-793-1-00012/full/html>; Christiane Rudolph, "Facilitating investments", (Development and Cooperation, 2019) <https://www.dandc.eu/en/article/rule-law-essential-generating-employment-and-fostering-prosperity>.
[26] See Generally: Articles 12, 13 and 14 of EU E-Commerce Directive, 2000 which distinguishes between "mere conduit", "caching" and "hosting" service providers.
[27] "'One-size-fits-all approach' does not work for digital markets: CCI Chairperson' Economic Times, (3 January, 2022) <https://government.economictimes.indiatimes.com/news/digital-india/one-size-fits-all-approach-does-not-work-for-digital-markets-cci-chairperson/80081381>.

specific context.[28] Domestic digital regulation in other spheres is already grappling with similar challenges where broad definitions are leading to common compliance and liability regimes which are ill-suited for sub-category entities which are part of broader/ umbrella definitions. Consider section 2(1)(w) of India's IT Act which broadly defines "*intermediary*"[29] and then originally prescribed a common liability/ compliance regime for different types of digital operators like social networks, search engines, online payments sites, cloud service providers, web hosting service providers, and online marketplaces. This created regulatory and accountability challenges and consequently IT frameworks have begun efforts at remedying this problem by pushing for specialised legal regimes for entities classified as "social media intermediaries" which are distinct from other categories for intermediaries.[30] Based on this analysis we submit that the DoT revisit the Bill's issues with broad definitions leading to one size fits all requirements since they deviate from the consensus opinion that digital markets require specialised regulation.

Based on the above analysis we propose:

Nuanced classification of services: The classification of services under the Bill should appreciate the technical requirements of functionality rather than the end-user services offered. For instance, apart from traditional telephone calling and calls made over the open internet ("VoIP"), the sector has seen development through another type of service that allows VoIP to connect directly with a landline or a telephone number. One example of this type of service is offered by SkypeOut– a paid service which uses conveyance of signals over the internet and transmits these signals over to the traditional telecommunication service provider's infrastructure. In a landmark case the Court of Justice of the European Union ("CJEU") held that SkypeOut is an interconnected VoIP

[28]' ''One-size-fits-all approach' does not work for digital markets: CCI Chairperson' Economic Times, (3 January, 2022) <https://government.economictimes.indiatimes.com/news/digital-india/one-size-fits-all-approach-does-not-work-for-digital-markets-cci-chairperson/80081381>.
[29] Section 2(1)(w) defines 'intermediary' as ".. 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".
[30] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 <https://www.meity.gov.in/content/notification-dated-25th-february-2021-gsr-139e-information-technology-intermediary>.

service which should be classified as an electronic communication service. The rationale employed by the CJEU is that it (i) enables communication through VoIP using phone numbers and telecom networks, and (ii) for a remuneration paid by the customers. In a similar matter, the CJEU has also held that services like Gmail merely initiate conveyance of signals, and do not function 'wholly or mainly on signals on an electronic communication network' and thus should not be considered an electronic communication service. Thus, we observe that the European approach is able to distinguish between digital services like email which operate exclusively over the open internet and services like SkypeOut which may originate over the internet and directly interconnect with the telecom infrastructure.

We submit that the Indian Telecommunications Bill learns from such global precedent and recognises the distinction between digital services which operate exclusively over the content layer of the internet, and services like SkypeOut which operate in some form at the carriage layer of internet access networks. Thus, telecommunication regulation should exclude Gmail and other similar services which function entirely on top of the open internet. Instead, if it must, telecommunication regulation should restrict itself to focus only on services that primarily connect with telecom infrastructure as traditional telecommunication services.

Align Approach with TRAI's Recommendations and the International Telecommunication Union ("ITU"): Finally, under this theme we submit that the DoT consider prior recommendations from TRAI. In this regard after a comprehensive public consultation in 2018-19, TRAI has previously opposed the regulation of OTT services through telecommunications laws. It highlighted that the ITU is still studying the issue at a global scale and that there is a lack of consensus on international best practices around the subject.[31] Thus, concurring with the concerns of TRAI, it would be of best interest to await suggestions/ recommendations from the ITU on the inclusion of OTTs under global telecom regulation. This would ensure that the regulatory landscape is in

[31] 'Draft Telecom Bill: TRAI Not In Favour Of Regulating OTT Communication Apps' (Inc42, 22 October, 2022) <https://inc42.com/buzz/draft-telecom-bill-trai-not-in-favour-of-regulating-ott-communication-apps/>.

alignment with the evolving technology ecosystem and that the domestic framework is in conformity with the international best practices.

3. Licensing | Issues with the premise and the practical implications

At the outset we submit that the Bill has been unable to clearly demarcate between the terms and conditions applicable to the different licensing, registration authorisation regimes proposed under it. For instance, the manner in which the framework will differentiate between each of the compliance regimes is unclear. This lack of clarity will cause uncertainties about whether authorisation and registration frameworks will have simpler operational requirements for regulated entities, or onerous/ prescriptive compliance which is similar to existing licensing frameworks for service providers such as TSPs and ISPs. Keeping this in mind, we submit the following analysis on conceptual and practical challenges with licensing digital and internet services.

Premise of licensing digital services: Clause 3 of the Bill requires "telecommunication services" (which includes categories like email, data communication services and OTT communication services) to obtain licences in order to function in India. Specifically, Clause 3 would assign the Indian Government with an "exclusive privilege"e i.e. a monopoly to operate "telecommunication services" including internet-based services like OTT communication services, data communication services and email. The Bill envisions this privilege to be subsequently exercised through a licensing framework for telecommunications services which includes most digital service providers. The Indian Government must revisit this premise since such digital services do not operate with the same infrastructural scarcities as TSPs and ISPs. We submit that such a licensing regime for digital services does not serve the public interest.

The licensing framework in place for TSPs and ISPs under current telecom laws is premised on the fact that the State must allocate scarce public resources (like spectrum)[32]

[32] Shamika Ravi and Darrell M. West, 'Spectrum policy in India' (2015) Centre for Information Technology at Brookings <https://www.brookings.edu/wp-content/uploads/2017/05/spectrum-policy-

to operators fairly, efficiently and in public interest.[33] This responsibility stems from legal principles like the *public trust doctrine*.[34] This is why the Telegraph Act assigns the Central Government with an "exclusive privilege" i.e. a monopoly of operating "telegraphs" – with a power to delegate that privilege to commercial enterprises through a licensing regime.[35]

As mentioned above, digital services do not operate with the same infrastructural/resource scarcity as TSPs and ISPs. So there is no pressing imperative to efficiently allocate internet related resources for the provision of any OTT/ digital service. The internet is an ecosystem of abundance[36] which thrives on the ease of entry and exit of firms – which in turn allows for dynamic market competition, innovation, and abundant choice for consumers. The Bill should also avoid construing digital services as substitutes of traditional telecom services. Digital services differ from traditional network operators in terms of medium and infrastructure of delivery. They also have varied functionality and features that are much more dynamic and multi-purpose as compared to TSPs/ ISPs. The latter are concerned largely with providing mere carriage services. In this regard these licensed operators control the underlying network whereas the same privileges are not afforded to digital services providers who primarily deliver their services over the carriage network.[37] Given these clear distinctions, enforcing TSP style licensing requirements on OTTs would hinder innovation and create barriers to entry into the market. This would be contrary to India's focus on fostering ease of doing business[38] and its overall ethos of economic liberalisation since 1991.

---

in-india8515.pdf> ; *Union of India vs. CPIL*, Writ Petition (Civil) No. 423 Of 2010 <https://indiankanoon.org/doc/70191862/>.

[33] Hank Intven (ed) and McCarthy Tetrault (ed), *Telecommunications Regulations Handbook* (World Bank, 2000) <https://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/2_Licensing.pdf>.

[34] *CPIL* (n 32).

[35] Section 4, The Indian Telegraph Act 1885.

[36] Ben Thompson, 'Economic Power in the Age of Abundance' (24 June 2014) Stratechery <https://stratechery.com/2014/economic-power-age-abundance/>.

[37] Internet Freedom Foundation, 'A Public Brief On The Draft Indian Telecommunication Bill, 2022', p. 10, 4.2 - 4.4 <https://drive.google.com/file/d/13vSyFZY7mc5TMxTYsiueZ7051qt0-UK9/view>.

[38] 'Ease of doing business: Govt working on to reduce compliance issues, says official' Economic Times (6 July 2022) <https://economictimes.indiatimes.com/news/economy/policy/ease-of-doing-business-govt-working-on-to-reduce-compliance-issues-says-official/articleshow/92705974.cms>.

Navigating challenges with data collection and retention requirements: The licensing regime for TSPs, ISPs, and other similarly placed operators is centred on significant data collection and retention as directed by the DoT. Such data collection takes place for various purposes and at different points during an operator's life cycle. It can range from user verification and KYC for the issuance of a new connection, to real-time data collection of a person's one-to-one SMS and call interactions (CDR, UDR, IPDR, etc.)[39] using a telephone/ mobile subscription. In this context, we submit that extending licensing requirements to the internet/ cyberspace risks becoming a pre-emptive step towards imposing expansive data collection and open-ended retention requirements on OTT communication service providers and other digital service providers. Among other things this would be inconsistent with global trends where countries are enacting data protection laws which espouse certain core data protection principles like collection limitation, storage limitation, data minimisation and purpose limitation– principles which have even been endorsed within domestic data protection discussions.[40] Additionally, we submit that the Indian Governments must carefully evaluate the latent privacy and cybersecurity risks associated with transposing data collection and retention requirements onto digital service providers which are analogous to those imposed on TSPs and ISPs.

Privacy and consumer risks: If imposed upon OTT/ digital services, bulk data collection and retention requirements are inconsistent with privacy enhancing measures being

[39] Currently the Unified Licensing regime requires licensed operators to collect and retain Call Detail Records (CDR), Exchange Detail Records (EDR), IP Detail Records (IPDR) and Usage Data Records (UDR) of the communication exchanges on their respective networks. Although not explicitly defined, the nature of such information includes log-in/log-out details when accessing the internet, email and other internet/telecom related services. Licensing frameworks also require such information to be time stamped, and covers all information which is essential for LEAs for tracking/forensic purposes. The CDR/UDR must include extensive details including calling number, called number, date, start time, end time/duration, identity of the device used for making the call (MAC ID/Device Signature), user id initiating the session, soft-switch ID and trunk ID. Such records also extend to system log details and commands issued as well. Such CDR, IPDR, EDR, and UDR are expected to be retained by licensed service providers for a minimum period of two years, to allow law enforcement to pursue State security or public interest objectives.

[40] Article 5, General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians" ("Justice Srikrishna Committee Report") <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>.

adopted across the internet industry. Companies are increasingly building solutions that adhere to data protection principles like data minimisation[41] and purpose limitation.[42] Extensive data collection and retention requirements also contradict industry developments where even when data is collected it is destroyed by platforms within defined periods.[43] Moreover innovative end-to-end encrypted communication platforms like Signal[44] would become unavailable/inoperable for Indian users given its ethos of user privacy and security, and its institutional decision to limit the tracking of user interactions.

Information security risks: Finally, data collection and retention requirements (even for law enforcement purposes) must balance themselves against competing information security imperatives.[45] Practically, as more data is collected over extended periods of time such requirements increase the attack surfaces which can be exploited by malicious actors. Thus, policymakers should factor in data protection and information security risks affiliated with imposing data collection and retention requirements through licensing regimes.

Prescriptive prohibitions and standards on encryption: Finally, licensing requirements should avoid measures which limit the strength of encrypted solutions over

[41] Information Commissioner's Office, "Data Minimisation" in 'Guide to the General Data Protection Principles' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>.
[42] Information Commissioner's Office, "Purpose Limitation" in 'Guide to the General Data Protection Principles' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>
[43] For example *see* 'Data retention, deletion, and destruction in Microsoft 365' (2022) Microsoft 365 <https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview>.
[44] 'Signal Will Exit India Rather Than Comply With Laws That Weaken Encryption Medianama' (21 October 2022) <https://www.medianama.com/2022/10/223-signal-will-exit-india-laws-break-encryption/#:~:text=%22Let's%20be%20clear%2C%20we%20are,not%20going%20to%20do%20that>.
[45] Mark Lanterman, 'Cyber risk: Is your data retention policy helping or hurting?' (2022) Minnesota State Bar Association <https://www.mnbar.org/resources/publications/bench-bar/columns/2020/07/29/cyber-risk-is-your-data-retention-policy-helping-or-hurting>; Marcus Evans, Janine Regan, et al., 'Record Retention is a Key Component of Your Privacy and Cyber Compliance Program' (2019) Norton Rose Fulbright <https://www.dataprotectionreport.com/2019/12/record-retention-is-a-key-component-of-your-privacy-and-cyber-compliance-program/>; Bradley Freedman, 'Less is More – Data Minimization and Cyber Risk Management' (2017) BLG <https://www.blg.com/en/insights/2017/08/less-is-more-data-minimization-and-cyber-risk-management>.

the internet which help protect commercial and private communications. Strong encryption is considered an enabler of human rights over the internet[46] and is also viewed as a prerequisite for resilient and secure cyberspace.[47] Therefore, the Bill must avoid transposing existing standards from TSPs and ISPs to OTT and digital services. For example, the existing licensing regime prohibits TSPs from implementing "bulk encryption."[48] and places an obsolete 40 bit encryption limit for outbound voice and internet traffic over ISP networks.[49] Also, the Government's licensing regime should not require OTT and digital service providers to intentionally maintain decryption keys/ backdoor entries to people's commercial and private communications. Similarly, the licensing regime should not prohibit strong or "bulk" encryption nor should it mandate any key length limits which caps the strength of encryption. The risk with such mandates which may aim to promote law enforcement investigations and prosecutions, is that it creates vulnerabilities to people's and enterprises' communications. Given the volume of sensitive private and commercial interactions which take place in cyberspace, domestic limits on encryption could create national security risks wherein sophisticated State and non-State actors could compromise India's private and sensitive communications over modern digital services. Caps on encryption would also compromise people's right to informational privacy which is exercised through private messaging services like WhatsApp and Signal.

4. Interception powers under the Bill are overbroad and may violate constitutional rights

The Bill allows the state to order the interception of messages transmitted over telecommunication services or networks in certain situations. It is broadly analogous to Section 5(2) of the Telegraph Act, which authorises the interception of messages

[46] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015 <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32>.
[47] Privacy International, 'Securing Privacy: Privacy International on End-to-End Encryption', September 2022, <https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf>.
[48] The Unified License Agreement, Clause 37.1.
[49] The Unified License Agreement.

transmitted by telegraph. However, the Bill's definition of 'telecommunication services' substantially expands the scope of the provision to include messages communicated over broadly all digital services. Such a broad provision may amount to a disproportionate restriction on the right to privacy. Moreover, interception provisions in the Bill would overlap with the IT Act, which already regulates digital internet services and also contains interception provisions. Additionally, the Bill misses out on a timely opportunity for surveillance reform which is consistent with recent policy and jurisprudential developments. These include: (i) Supreme Court decisions in *KS Puttaswamy vs Union of India* (which reaffirmed the right to privacy as a fundamental right, hereafter "Puttaswamy")and *KS Puttaswamy vs Union of India* (which examined the constitutional validity of the Aadhaar Act, hereafter *Aadhaar)*; and (ii) the B.N Srikrishna Data Protection Committee report's extensive observations on the need for surveillance reform in line with what constitute reasonable restrictions to the fundamental right to privacy.

***Description of interception provisions in the Bill and overlaps with existing provisions*:** Clause 24(2)(a) of the Bill authorises the State or Central governments or authorised officers to direct the interception, disclosure, or detention of "any message or class of messages", which are "transmitted or received by any telecommunication services or telecommunication network" in the interest of public safety, or when a public emergency occurs.[50] This provision substantially draws from Section 5(2) of the Telegraph Act, which allows the state to direct the interception of messages transmitted by telegraph on similar grounds as the Bill. The definition of 'telegraph' in the Act includes any instruments used, or capable of being used to transmit images, sounds, or other information by "*wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means*".[51] However, the Bill substantially expands the scope of this provision. The broad definitions of 'message', 'telecommunication services', and 'telecommunication network' would bring virtually all digital communications within the ambit of this provision, ranging from messages

[50] Clause 24(2)(1), draft Indian Telecommunication Bill, 2022.
[51] Section 3(1), Indian Telegraph Act, 1885.

transmitted between devices as part of IoT systems to communication services that use end-to-end encryption.

Moreover, the IT Act also contains interception provisions - Section 69 allows the government to issue directions to monitor, intercept, or decrypt any information generated, transmitted, received, or stored on a computer resource.[52] Though similar, the IT Act extends the State's powers of interception by expanding the grounds on which such actions can be authorised, among other measures.[53] Section 69 of the IT Act does not contain the grounds of public emergency or public safety (as present in the Telegraph Act) for authorisation of interception orders.

The inclusion of interception provisions in the Bill would overlap with MeitY's policy-making powers for information technology, electronics and the internet, as discussed in section 1 above. Given that the IT Act already contains provisions that regulate the interception of messages over digital services, the Bill should refrain from creating a parallel regime of interception for digital services.

Background on the right to privacy and need to re-examine existing interception rules: The right to privacy was reaffirmed as a fundamental right by the Supreme Court in the landmark *Puttaswamy* judgement. The Court held that it was an intrinsic part of the right to life and personal liberty and the other fundamental rights. Measures restricting the right to privacy are required to conform to the requirements outlined in *Puttaswamy* (and subsequently further analysed in *Aadhaar*), and must: (a) be provided by law; (b) pursue a legitimate aim and be necessary in a democratic society; (c) be proportionate to the need for the interference with the right to privacy; and (d) contain procedural safeguards to prevent against abuse.[54]

[52] Rule 2(g), 2(l), 2(o), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 G.S.R. 780(E) (27 October 2009) ["Interception Rules"].
[53] *See* for example Section 69(1), 69(3) and 69(4 Information Technology Act, 2000; Ministry of Home Ministry (Cyber and Information Security Division) S.O. 6227(E) (20 December 2018).
[54] *K.S. Puttaswamy and Anr. vs. Union of India* (2017) 10 SCC 1.

The constitutionality of Section 5(2) of the Telegraph Act (which authorises the interception of messages transmitted by telegraph) was examined by the Supreme Court in 1997 in the landmark *PUCL vs Union of India* ("PUCL").[55] The Court upheld the constitutionality of the provision, but noted the lack of procedural safeguards for the exercise of the executive's surveillance powers and held that powers of interception were not to be exercised routinely and arbitrarily. It laid down detailed guidelines in this regard, and the Telegraph Rules were subsequently amended to introduce procedural safeguards in line with *PUCL*.[56] However, this decision, and the larger legislative framework relating to lawful interception must be revisited in light of the Supreme Court's decisions in *Puttaswamy* and *Aadhaar*. The provisions permitting interception in the Bill may amount to a disproportionate restriction on the right to privacy, as we discuss below.

Interception provisions in the Bill are disproportionate to the aim sought to be achieved: For measures restricting the right to privacy to be lawful, they must be proportionate to achieve the stated aim. Under the Bill, the State may order interception "*on the occurrence of any public emergency or in the interest of public safety*", where it is necessary or expedient to do so in the interest of specified grounds such as public order and the sovereignty of the country.[57] The wide definition of 'message', 'telecommunication services', and 'telecommunication networks' would mean that the scope of interception is broad enough to cover virtually all communication over digital services. Such a broad ambit could impose a disproportionate restriction on user privacy due to the vast range of services and number of individuals that interception orders would be able to target. The Bill allows interception measures to be aimed at *classes* of users or content - allowing the state to intercept messages of all residents of a particular community, for example, or all communications pertaining to a subject area, such as cricket. It is also unclear how one would be able to assess whether messages pertain to a particular issue or subject matter without screening all messages sent through particular telecommunication services or networks, which could adversely impact the privacy rights of unrelated users. Interception orders directed at services that use end-to-end encryption would potentially

[55] *PUCL v Union of India* (1997) 1 SCC 301.
[56] Rule 419A, The Telegraph Rules, 1951.
[57] Clause 24(2), Draft Telecommunications Bill, 2022.

undermine such encryption technology and compromise Indian users' ability to use such services.

Finally, these interception provisions must be looked at in the context of the existing licensing requirements under the Unified License frameworks. These licensing frameworks are currently applicable to specific types of service providers such as TSPs and ISPs, but it is unclear if a broader range of telecommunications service providers would be subject to licensing requirements under the Bill. Currently, licensing provisions require service providers to undertake various actions such as setting up monitoring and interception facilities and equipment, facilitating interception under Section 5(2) of the Telegraph Act, and maintaining various records of users.[58]

The Bill does not contain adequate procedural safeguards for interception: As discussed above, measures restricting the right to privacy must contain procedural safeguards to prevent misuse. One of the safeguards incorporated into the Telegraph Rules is the institution of a review committee, composed of members of the executive. This committee is meant to review every direction for interception and record its findings on whether the directions comply with requirements under the Telegraph Act.[59] However, as noted by the Srikrishna Committee Report, given the volume of interception orders and the frequency of the committee's meetings (which are bi-monthly), it was unrealistic for the committee to be able to provide effective oversight for each interception order.[60]

The need for judicial oversight for measures restricting the right to privacy was recognised by the Supreme Court in *Aadhaar*. The Court struck down a provision of the Aadhaar Act which authorised the disclosure of biometric information to the State, in the interest of national security, because the provision did not provide for independent oversight over the powers provided to the executive to protect the rights of individuals.[61] It highlighted

[58] See for instance Department of Telecommunications, "License Agreement for Unified License" <https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf> Clause 23.2, Clause 39.23 (ix), UL), 40.2, Clause 8.3, ULChapter VIII (Access Services).
[59] Telegraph Act, 1957.
[60] Srikrishna Committee Report (n 40).
[61] *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [513.6].

the importance of having a "*Judicial Officer (preferably a sitting High Court Judge)*" for the application of judicial mind to avoid misuse, and noted that such provisions are prevalent in other jurisdictions.[62] The requirement for judicial oversight for interception is also mirrored in international jurisprudence,[63] and should be incorporated as a safeguard into interception legal framework in India.

Additionally, in the absence of measures requiring the publication of interception orders or informing affected individuals, there is an especially pressing need for independent judicial oversight of interception orders. The Bill does not currently provide for interception orders to be published or for affected individuals to be informed of interception. The Srikrishna Committee Report notes that surveillance must not be carried out without a degree of transparency that would conform with *Puttaswamy,* to ensure oversight and enable public accountability.[64] The absence of the requirement to publish interception orders can make it extremely difficult for individuals to contest the legality of any order which they are affected by, and can impede their ability to avail of constitutional remedies provided under Articles 32 and 226.

5. ID verification requirements under the Bill may violate constitutional rights to privacy and free expression

The Bill requires service providers licensed under it to 'unequivocally identify' a person using such services through 'a verifiable mode of identification'.[65] It also requires the identity of persons sending messages using telecommunication services to be provided to the recipients.[66] Given the broad definition of service providers, this would mean that virtually all users of any digital services would be required to identify users on their services, and also make this information available to recipients. While this measure is ostensibly targeted at addressing spam calls and related issues,[67] such a provision would

[62] ibid.
[63] Srikrishna Committee Report (n 40) 125-128.
[64] Srikrishna Committee Report (n 40) 125.
[65] Clause 4(7), draft Telecommunication Bill, 2022.
[66] Clause 4(8), draft Telecommunication Bill, 2022.
[67] Media interaction on draft Telecom Bill 2022 by Union Minister Ashwini Vaishnaw, (YouTube September 23 2022) <https://www.youtube.com/watch?v=_FoRSdrB_zk>

have wider ramifications impacting the fundamental rights of all users. Measures aimed at removing anonymity in online communication can restrict the rights to privacy and free expression of users, and is likely to disproportionately affect marginalised and vulnerable communities.

For instance, the Special Rapporteur on freedom of opinion and expression noted that encryption and anonymity in communications played a key role in protecting the right to freedom of expression, noting that they are vital tools for journalists and other stakeholders to fully exercise their democratic rights.[68] They also noted that legitimate state access to encrypted or anonymous conversation must only be sought by judicial process, and cautioned against compelling entities to introduce vulnerabilities for government access both to protect rights as well as digital security. However, the Bill, in requiring "*the identity of a person sending a message using telecommunication services*" to be made available to the recipient, raises the risk of 'traceability' requirements, that is to identify the first originator of information. Such a provision was introduced through the Intermediary Guidelines in 2021. These Guidelines and various provisions, including those relating to traceability, are currently under challenge at the Supreme Court.[69]

The explanatory note of the Bill suggests that verifiability requirements are imposed under the Bill in order to tackle cyber-fraud.[70] However, such requirements should not be mandatory and must balance fundamental rights to privacy and free expression. Mandatory ID verification requirements would disallow users from being able to operate anonymously online, and online anonymity has been explicitly recognised by UN Special Rapporteurs as a key enabler for individuals in realising their international human

[68] Office of the High Commissioner for Human Rights, 'Human rights, encryption and anonymity in a digital age' UNHRC (1 July 2015) <https://www.ohchr.org/en/stories/2015/06/human-rights-encryption-and-anonymity-digital-age>.
[69] Stay on IT Rules Continues as SC Takes Up Centre's Transfer Plea, Restrains HCs in Matter' The Wire (9 May 2022) <https://thewire.in/law/supreme-court-it-rules-ott-transfer-plea>
[70] Ministry of Communications, Explanatory Note to The Draft Indian Telecommunication Bill, 2022, para 17 <https://dot.gov.in/sites/default/files/Explanatory%20Note%20to%20the%20draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf>

rights.[71] Moreover, online anonymity is viewed by experts as a catalyst in allowing minority and vulnerable groups to safely navigate cyberspace.[72] Mandatory ID verification requirements could also serve as a disincentive for users from accessing certain digital services - for instance, mandatory KYC/ ID verification requirements imposed by the RBI led to significant user-drop off across the digital wallet ("Prepaid Payment Instrument") industry.[73]

Open-ended and broad application of identification methods would also contradict established data protection principles such as data minimisation and purpose limitation.[74] These principles require those processing personal data to collect only the information that is necessary for specified purposes, and that personal data is collected only for specified, explicit, and legitimate purposes respectively. However, requiring OTT platforms to collect the government IDs of individuals in the absence of a data protection legislation, and without any resultant data protection safeguards would make it difficult to ensure the security of, and the proportionate use of such information.[75]

---

[71]UNHRC, Human rights, encryption and anonymity in a digital age, 01 July, 2015 <https://www.ohchr.org/en/stories/2015/06/human-rights-encryption-and-anonymity-digital-age>; Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015 <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32>

[72] International Network of Civil Liberties Organisation submission on The right to privacy in the digital age
Human Rights Council adopted resolution 34/7, 2018 <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/INCLO.pdf>; Article 19, 'Right to Online Anonymity', June 2015, p. 13, 25 < <https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf>.

[73] Amid Cash Crunch, Mobile Wallets Register Significant Drop As Users Shy Away From Full KYC, (inc42, 19 April 2018) < https://inc42.com/buzz/mobile-wallets-drop-users-full-kyc-rbi/>.

[74] Information Commissioner's Office, "Data Minimisation" in 'Guide to the General Data Protection Principles' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>; Information Commissioner's Office, "Purpose Limitation" in 'Guide to the General Data Protection Principles' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>.

[75] The consideration on verifiability was also seen in the IT Rules, however, it was solely introduced as a *voluntary* clause. Clause 4(7), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

6. Provisions relating to the suspension of telecommunication services restrict the right to free expression so they must be narrowly tailored and subject to procedural safeguards

Clause 24(2)(b) of the Bill authorises the State to direct the suspension of 'communication or class of communications', or 'relating to any particular subject' that is transmitted or received by any telecommunication network. This explicitly extends the ambit of suspension orders to internet based communications, and allows for the suspension of internet, phone call and messaging services, among other telecommunication services. The Telegraph Act currently allows for the temporary suspension of telecom services including the internet,[76] which means that the state has the power to temporarily restrict access to the internet as a whole. The Bill extends suspension powers to all internet and digital services, meaning that the state would have the ability to restrict access to or blacklist specific digital services, in addition to restrictions on access to the internet as a whole. This provision can significantly hamper the right to freedom of speech and expression on the internet in India.

The importance of access to the internet in exercising the right to freedom of speech and expression: Access to the internet is a core part of the exercise of many rights, particularly the rights to freedom of expression and information. These rights are protected in a variety of international instruments,[77] and many international organisations have noted that the right to internet access is protected under the right to freedom of speech and expression. For example, the United Nations considers internet access to be a basic human right,[78] and has noted that the suspension of services

[76] See Section 5, Indian Telegraph Act, 1885; Temporary Suspension of Telecom Services (Public Emergency or Public Service) Rules, 2017.
[77] Eg Article 19, Universal Declaration of Human Rights, UNGA 217 A (III), 1948; Article 19, International Covenant on Civil and Political Rights, United Nations, Treaty Series, vol. 999, p. 171, 1966.
[78] Marianne Franklin (ed), *The Charter of Human Rights and Principles for the Internet* (4th edn, UN Internet Governance Forum, 2014) <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>.

undermine a range of human rights, particularly the right to freedom of expression.[79] In accordance with settled international and domestic jurisprudence, measures restricting the right to freedom of expression must be: (i) provided by law; (ii) pursue a legitimate aim; and (iii) be necessary and proportional to achieve the aim. Consequently, measures suspending internet access must also conform to these requirements, since they undermine the freedom of expression. However, the UN Human Rights Office notes that this is often not the case, and that internet suspension orders very rarely meet these requirements.[80]

Jurisprudence around the freedom of speech and internet access has also been developing in India. In 2015, the Supreme Court in *Shreya Singhal v Union of India*[81] held that the right to freedom of speech and expression extends to the internet, and that any limitation on such right must conform to the requirements of Article 19(2) of the Constitution and must be proportionate to the goal it seeks to achieve.[82] Other judgments have also held that the freedom to practise any profession or trade over the internet are protected under Articles 19(1)(a) and 19(1)(g), and have noted the importance of access to the internet in ensuring the right to education.[83]

The Supreme Court specifically examined the constitutionality of communication suspensions in Jammu and Kashmir in *Anuradha Bhasin v Union of India* ("Anuradha Bhasin")[84] in 2019. In its judgement, the Court affirmed the proportionality standard in assessing the legality of restrictions to fundamental rights, and that proportionality would require "*a restriction to be tailored in accordance with the territorial extent of the restriction, the stage of emergency, nature of urgency, duration of such restrictive*

[79] Office of the High Commissioner for Human Rights, 'Activists: Internet shutdowns violate human rights', UNHRC (19 August 2022) <https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights>.
[80] Office of the High Commissioner for Human Rights, *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights*, (A/HRC/50/55, 19 August 2022) p 4 <https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts>.
[81] *Shreya Singhal v Union of India* (2013) 12 SCC 73.
[82] *Shreya Singhal*, para 86.
[83] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308, *Faheema Shirin.R.K vs State Of Kerala* on 19 September, 2019
[84] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308.

measure and nature of such restriction".[85] The Court also read procedural safeguards into the Suspension Rules formulated under the Telegraph Act, namely that: (a) all telecommunication suspension orders must be made publicly available pursuant to principles of natural justice; (b) orders must specify a time limit for operation and that indefinite suspensions are impermissible; and (c) the review committee constituted under the Suspension Rules must conduct periodic seven-day reviews to assess whether the suspensions continue to be proportionate and comply with the requirements of the Telegraph Act. However, subsequent reports indicate that these requirements are not being complied with.[86]

The report of the Standing Committee on the impact of internet suspensions[87] also notes the importance of the internet in the current era, noting that it "*is the lifeline which is propelling businesses and services, permitting students to enroll for important examination, and enabling home delivery of essentials*",[88] and that any interruptions to internet services should be avoided, and must be conducted with abundant caution where it is unavoidable.

Impact of telecom suspension provisions on the freedom of speech and expression: As noted above, the Bill enables the State to order the suspension of a wide range of services, including all internet and digital services. It does not incorporate any of the safeguards regarding publication of orders, specifying timelines of restricted services, or review/ oversight processes laid down in *Anuradha Bhasin*. Incorporating these

[85] *Anuradha Bhasin,* para 71.
[86] See Internet Freedom Foundation, RTI responses from MP and Meghalaya show compliance failure with the Anuradha Bhasin Internet Shutdown decision <https://internetfreedom.in/rti-responses-from-mp-and-meghalaya-show-compliance-failure-with-the-anuradha-bhasin-internet-shutdown-decision/>; Internet Freedom Foundation, RTI responses from Andhra Pradesh and Gujarat show compliance failure with the Anuradha Bhasin Internet Shutdown decision <https://internetfreedom.in/rti-responses-from-andhra-pradesh-and-gujarat-show-compliance-failure-with-the-anuradha-bhasin-internet-shutdown-decision/>; Internet Freedom Foundation, Revealed: Rajasthan's Review Committee does not meet or review internet suspension orders. #KeepItOn <https://internetfreedom.in/revealed-rajasthans-review-committee-does-not-meet-or-review-internet-suspension-orders-keepiton/>.
[87] Standing Committee on Communications and Information Technology, Suspension of Telecom Services/Internet and its Impact, Twenty- Sixth Report, December 2021 (Standing Committee Report) <http://164.100.47.193/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_26.pdf>.
[88] Standing Committee Report, p 31.

safeguards into legislation may be particularly important since states do not seem to be complying with these requirements, as discussed above. Moreover, measures such as publication of orders are integral to enable citizens to avail of constitutional remedies as noted in section 4 above, since users are unlikely to otherwise be able to challenge orders.

The Bill also allows for broad and wide-ranging suspensions on the basis of 'communications', persons, or subject matter. This does not incorporate the proportionality standard endorsed in the case, which would require restrictions on services to be tailored based on factors such as the extent of the restriction, nature of emergency, etc. The broad powers provided to the State by the Bill can therefore disproportionately impact users' fundamental rights and restrict their access to financial, educational, and other services that operate online. We urge that any restrictions on telecommunications services must be used only in the most exigent circumstances and be as narrowly targeted as possible to ensure compliance with existing legal standards, and the least impact on fundamental rights and freedoms.