9 November 2022

Government of India
Ministry of Communications
Department of Telecommunications
New Delhi
Via Email

Subject: Indian Telecommunication Bill, 2022

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide feedback on the draft Indian Telecommunication Bill, 2022 (ITB), circulated for public comment on 21 September 2022.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services. Our members are unified in their support for policy measures that promote a robust, healthy digital ecosystem and information lifecycle worldwide.

SIIA has joined, and concurs in the recommendations set forth in, an industry letter submitted to the Ministry. We write separately to emphasize key concerns about the potential implications of the ITB, if enacted in its current form. We believe that ITB will create significant risks for businesses that will hurt investment into and innovation in India for a range of critical digital services. This will have ramifications for Indian consumers. It will also undermine India's national security by weakening cybersecurity protections in the digital ecosystem and working counter to the larger goal of democratic alignment on tech standards.

For the reasons set out below, our core recommendation is that the Ministry revise the ITB to exclude over the top (OTT) services and other services that are not telecommunications service providers (TSPs) and not traditionally considered within the ambit of telecommunications services.

Advancing Innovation, Investment, and the Health of the Indian Digital Ecosystem

The ITB represents a proposal to expand the scope of telecommunications regulation to virtually the entire landscape of digital communications. While we support the Indian government's interest in protecting its own digital ecosystem, we are concerned that the ITB would have significant, detrimental effects on the ability of companies to do business in India.

Telecommunications regulations have historically – in India as well as in virtually all countries around the world – focused on TSPs. In addition to being entitled to acquire spectrum, obtain numbering resources, and connect with the Public Switched Telephone Network, TSPs provide the physical infrastructure for the internet which is relied on by a host of digital service providers. The ITB would extend regulation well beyond this domain. It defines "telecommunication services," and related terms, in a broad manner that sweeps in virtually all digital communications services – including applications and OTT services that rely on the underlying control and access infrastructure that TSPs provide.[1]

The effect of this, as the Ministry is no doubt aware, is that the ITB would require virtually all digital services – not only hardware and spectrum providers – to comply with a range of regulatory requirements. These companies would need to seek government licenses and authorizations to conduct business and provide services to consumers, other businesses, and government agencies.

This approach will have significant consequences for the Indian digital economy and consumer and business welfare in India.

First, the ITB will generate significant uncertainty for companies doing business in India. India already regulates much of the non-TSP activity within the scope of the ITB under other laws, including the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.[2] These frameworks govern compliance and reporting, provide mechanisms for addressing national security needs of the Indian government, and include safeguards for Indian consumers.[3] The conflicting obligations of the ITB will create uncertainty and generate significant compliance costs that will likely be passed on to Indian consumers.

---

[1] Section 2(21) defines "telecommunication services" to mean "service of any description (including broadcasting services, electronic mail, voice mail, voice, video and data communication services, audiotex services, videotex services, fixed and mobile services, internet and broadband services, satellite based communication services, internet based communication services, in-flight and maritime connectivity services, interpersonal communications services, machine to machine communication services, over-the-top (OTT) communication services) which is made available to users by telecommunication, and includes any other service that the Central Government may notify to be telecommunication services."

[2] India also has in place a series of additional laws that focus on more discrete areas of concern, such as cybersecurity. These include the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, and the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

[3] India is also considering the Digital India Act, which would replace the Information Technology Act, 2000, and would be tailored to the digital services currently governed by that Act. The Digital India Act, rather than a broad expansion of telecommunications law as contemplated by the ITB, is a more appropriate vehicle to consider any gaps in the current legal structure.

Second, the expansive scope of the ITB and the regulatory requirements that extend to non-TSP services are likely to impede innovation in India. Companies in the OTT space will be hesitant to expand their footprint and introduce new digital services if that means that they will be subject to onerous restrictions common for TSPs but virtually unprecedented for internet-based applications. Moreover, the expansive authority the ITB would grant to the government (see below) would increase the risk and cost of doing business of doing business in India significant enough that some firms may opt to exit the market. This is likely to affect healthy competition and consumer choice in the long run and may also impinge on the ability of the tech sector to create job opportunities in India.

Third, the ITB will undoubtedly generate regulatory friction within the Indian government since many of the new services that would be covered under the ITB are overseen by different agencies in the Indian government (such as the Ministry of Electronics and Information Technology, and the Ministry of Information and Broadcasting). Increased regulatory friction will undermine business confidence and could decrease investment into the Indian digital ecosystem. This will necessarily have an impact on research and development and the development of products and services that are designed to address the needs of India and Indian consumers.

Fourth, by specifically including "communication-based" online services – such as communication-based OTT services within its ambit – ITB fails to recognize that there are many OTT services that offer overlapping functionalities. For example, several OTT services provide both communications based, as well as non-communication-based features. Since the ITB does not provide guidance on how a communication service ought to be distinguished from a non-communication service, the same will result in added regulatory uncertainty.

Fifth, by extrapolating a telecom licensing regime onto internet-based services, the ITB requires licensed entities to identify their users through a verifiable mode of identification and make available the identity of the sender to its receiver.[4] This may result in a scenario where service providers not only have to weaken their encryption mechanisms to ensure identification but also must collect additional personal information. This can have far-reaching consequences for users' right to privacy. Further, other requirements such as enabling a "priority call routing scheme"[5] may increase the compliance costs of OTT and other internet service providers as they may not have the necessary infrastructure in place to enable the same.

Sixth, certain undefined terms within the ITB raise concerns. For instance, the ITB allows the government to mandate licensed entities to obtain prior consent of users for receiving "specified messages," maintain "'do not disturb' registers," and enable reporting mechanisms. As "specified messages" are not defined, it is unclear whether messages that are merely

[4] ITB, Section 4(7) and 4(8).

[5] ITB, Section 24(1).

incidental to a service would be considered as "specified messages." This could cover push messages and in-app messages and notifications within the ambit of regulation and cause regulatory uncertainty. We also urge the Indian government to consider the existing regulation of unsolicited commercial communications (UCC) under the Telecom Commercial Communications Customer Preference Regulations, 2018 (UCC Regulations).

While the Ministry's objective in striving for a unified telecommunications regulation scheme is understandable, we encourage the Ministry to consider these and other risks. We do not believe that an expansion as broad as contemplated will have any net positive benefit on India and would recommend that any further regulation on OTT and other internet services be explored in separate, more targeted measures that address specific gaps in the existing regulatory fabric.

Balancing Democracy and National Security

SIIA also has concerns about the expansive powers that the ITB would give to the Indian government with respect to OTT services and other non-TSP services. Recognizing India's interest in securing its digital ecosystem, we fear that the ITB represents the kind of regulatory overreach that will curtail individual rights, undermine the safety of the digital ecosystem, and weaken India's national security.

The provisions of Chapter 6 of the ITB relating to government authority to intercept messages will almost certainly lead to weaker encryption and cybersecurity protections that expose the Indian digital ecosystem to heightened risks from bad actors and coordinated campaigns. Section 24, for example, would, among other things, allow the Indian government or any state government to intercept, detain, or disclose any message or group of communications or direct internet shutdowns for public interest or in case of a public emergency (with both terms being undefined) and if "it is necessary or expedient to do so, in the interest of the sovereignty, integrity or security of India, friendly relations with foreign states, public order, or preventing incitement to an offence."[6] Notwithstanding the Ministry's comment in its explanatory note that the provisions will "ensur[e] the rights of the citizens of India,"[7] we are concerned that this broad grant of authority – without any checks and balances or procedural safeguards in place – would undermine privacy and civil liberties and chill communications. We also note that the Information Technology Act, 2000 (the "IT Act"), read with the applicable rules, already addresses the information blocking, collection and surveillance needs of the government. In contrast to the approach taken by the ITB, however, that Act includes various safeguards (such as a 60-day review period) that protect individuals' rights and serve as guardrails against the potential abuse of authority or disproportionate government action.

---

[6] ITB, Section 24(2).

[7] *See* Explanatory Note, para. 51, available at https://dot.gov.in/sites/default/files/Explanatory%20Note%20to%20the%20draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf.

The grant of authority in Section 24 would also allow the government to "take temporary possession of any telecommunication services"[8] on the vague grounds of "public interest" or "public emergency." While the impact of this authority is difficult to quantify, the potential for confiscation, even on a temporary basis, creates an enormous business risk for companies. This risk is compounded by the lack of procedural safeguards as well. We have no doubt that this will factor into businesses' decisions to participate in the Indian economy.

Similarly, Section 25 permits the issuance of directions during times of war, etc. with respect to use of telecommunication services, telecommunication equipment, etc. It enables the government to, among other things, take over the control and management of telecommunications services. However, these powers of the Government are not limited to telecommunication services operated by regulated entities under the ITB. This may lead to a scenario where a whole host of digital or non-TSP services – regardless of whether they are regulated under the law – face government interference.

India is the world's largest democracy. In the past several years, India has made strides to engage with partner nations to further an international model for technology governance and standards that comport with a democratic rather than an authoritarian vision of digital governance through its increased engagement on the Council for the International Telecommunications Union, with various efforts of the Organisation for Economic Cooperation and Development, and as a member of the Global Partnership on Artificial Intelligence (GPAI) and other AI-focused projects that seek to build a framework for the development and use of advanced technologies that comport with democratic norms. This is also reflected by an increase in collaboration between India and the United States to further digital democracy.[9]

Moreover, the need for India to engage collaboratively to address digital threats has arguably never been greater. Cybersecurity and misinformation threats associated with authoritarian actors continue to grow. The private sector can be a critical collaborator in addressing these threats and helping the Indian government to improve the health of its digital ecosystem. We would caution the Ministry to avoid onerous regulation that may weaken this collaborative relationship.

The ITB appears to represent a turn away from the approach to multilateralism and collaboration that India has embraced on the digital front. We would encourage the Ministry, and the Indian government, to support measures that advance rather than undermine a global digital ecosystem that comports with the values and norms that citizens expect in democratic

[8] ITB, Section 24(1).

[9] *See, e.g.,* https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/u-s-india-joint-leaders-statement-a-partnership-for-global-good/; https://beta.nsf.gov/news/facilitating-us-india-bilateral-research; https://www.defense.gov/News/News-Stories/Article/Article/2996395/us-india-take-steps-to-increase-cooperation-ties-between-2-largest-democracies/; https://www.state.gov/the-united-states-and-india-deepening-our-strategic-partnership/.

nations. We believe the risk of creating a "splinternet" will ultimately be detrimental to Indian national security.

We urge the Indian government to introduce safeguards in the provisions pertaining to interception and suspension. Internet services that are governed under the IT Act, and allied rules, could be excluded from the ambit of the ITB. For the remaining part, the provisions described above should only come into effect under very limited circumstances, accompanied by sufficient procedural and judicial safeguards.

Further Considerations on Individuals' Data and Rights

The ITB requires licensed entities to unequivocally identify users to whom it provides services, through a verifiable mode of identification. We believe that collection of personal information of users for the purposes of verification may be unnecessary and may lead to collection and storage of personal data of individuals in large volumes. This could result in privacy concerns (including failure to prioritize user safety and security).

While we appreciate the intent of the government to ensure that users of telecommunication services are kept informed, this requirement could cause more problems than it attempts to solve. User verification for services such as email and video conferencing would also disrupt daily day-to-day business activities.

In addition, the ITB does not clarify the scope of the government's search and seizure powers under the same and could lead to exercise of wide powers by the Indian government without adequate statutory safeguards. As the definition of telecommunication services is wide and may also include encrypted services, cloud and software services, an unfettered power to seek information could raise user privacy and intellectual property concerns.

In this regard, however, safeguards are already provided under the framework of Criminal Procedure Code, 1973 (CrPC) and the IT Act, which adequately provide for information requests and search and seizure actions. While courts have held that law enforcement agencies can seek information under the CrPC only for the purpose of conducting investigations after filing a First Information Report, the ITB empowers the Government to seek information by meeting a lower threshold than this. Accordingly, existing mechanisms under existing law sufficiently aid search/seizure and information requests and do not require further enhancement under the ITB.

The ITB also empowers the government to impose penalties for non-compliance with its provisions. It also empowers the Indian government to decide upon the quantum of penalty or fine and compensation. Such penalties could cause impediments in innovation and ease of doing business and should be deleted.

Ensuring Interoperable Technical Standards

Under the ITB, the Indian government can prescribe technical standards for telecommunication services, networks, equipment, telecommunication infrastructure and for manufacturers,

importers, distributors and reliability of the provision of telecommunication services to the public. We urge the Indian government to consider mandating through statute, the requirement to align Indian technical standards with international standards. This would help in removing any conflict in standards, reduce the possibility of increased costs and ensure interoperability.

Conclusion

Thank you for the opportunity to share our views. We welcome further engagement with you on this legislation. Please directly inquiries to: Paul Lekas, SIIA's Senior Vice President for Global Public Policy, at plekas@siia.net.