Centre for Internet & Society

CIS's Comments to "The Telecommunications Bill, 2023"

22 December 2023

By **Isha Suri, Nishant Shankar, Shweta Mohandas, and Vipul Kharbanda** (in alphabetical order)

Reviewed by **Tanveer Hasan**

The Centre for Internet and Society, India

Key concerns

1. **Definition of Telecommunication Service**

The definition of the terms telecommunication (section 2(p) and telecommunication service (section 2(t)) is extremely broad and would effectively include transmission of any signal by any electromagnetic systems. This wide definition increases the scope of the Bill to include almost all kinds of means of communication used in modern times including messaging services, email, OTT services, among others. Even if one were to accept the argument that the scope of the Bill has been deliberately kept wide so that the government has the power to regulate all means of telecommunication in order to prevent mischief and illegal activities, the problem arises with the onerous language of section 3(1) which makes it compulsory to obtain an authorisation from the Central Government for any and all telecommunication services, unless specifically exempted under section 3(3).

In simpler words the Bill not only seeks to regulate all communication services, but requires government permission to provide such services in the first place. Such an approach has the very likely potential to hamper future telecom innovation especially in light of the fact that the penalty for not obtaining permission is imprisonment upto 3 years as well as fine of upto Rs. 2 crores.

Such a wide definition leads to ambiguity and lack of regulatory certainty to businesses as well as users participating in the ecosystem. This proposal triggers immediate concerns, particularly a confusing definition of telecommunication services which may also incorporate the provision of a broad range of digital and online services. Such a wide definition could lead to confusion and arbitrary implementation on one hand, and if made applicable to the content layer of the internet architecture stifle innovation in the digital ecosystem due to onerous licensing/registration requirements on the other hand. It is also pertinent to note that internet-based services are already regulated under the Information Technology (IT) Act 2000. For example, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 regulates intermediaries, including the significant social media intermediaries (SSMI) such as Facebook and Twitter. Putting an additional regulatory burden on these service layer companies will hamper innovation and competitiveness of the sector and also amount to regulatory overreach.

2. **Power of authorisation and assignment**

Section 3 (7) - *Any authorised entity which provides such telecommunication services as may be notified by the Central Government, shall identify the person to whom it provides telecommunication services through use of any verifiable biometric based identification as may be prescribed.*

All services do not require a biometric based identification of the person. While there is a legitimate need to verify a person in the case of financial transactions, however a similar level of scrutiny is not warranted for applications that a person might use once, or applications that do not pose a threat. For example the need to verify a person through Know Your Customer (KYC) or otherwise for an application to order food, or an application which is meant for communication can be excessive regulation. In addition to the enhanced burden of collecting and storing this data that will come on the telecommunication service, there will also be the added requirement to maintain strict data protection and security measures under the Digital Personal Data Protection Act 2023. Furthermore, as has been seen in multiple instances of data breaches and cyber security attacks such as the one at AIIMS[1], Justpay[2] demonstrate that both public and private organisations can be affected by cyber attacks. It is therefore advisable to reduce the number of entities that store and collect sensitive personal data such as biometric information in the interest of privacy as well as national security.

The Supreme Court while looking at the constitutionality of the Aadhaar Act upheld the need for banking and financial institutions to require an individual's Aadhaar number stating the legitimate aim of preventing money laundering; however, the Court struck down the provision that required any private entity to collect Aadhaar details. Justice Bhushan held that the collection by private entities violated the right to privacy, by failing the first prong of the test laid down in Puttaswamy judgement, the test of legality.[3]

More importantly, through the requirement of 'verifiable biometric based identification', the Bill is likely to nudge telecom service providers to incorporate Aadhar Based identification, even though the Indian Supreme Court in 2018 held that the mandatory linking of mobile connections with biometric identification is unlawful.

Standards, Public Safety, National Security And Protection Of Telecommunication Networks

1. **Power to notify standards**

[1]Business Today Desk, "Cyber attack at AIIMS Delhi: Hackers demand Rs 200 cr in crypto, says report" *Business Today,* 22 November 2022, https://www.businesstoday.in/latest/in-focus/story/cyber-attack-at-aiims-delhi-hackers-demand-rs-200-cr-in-crypto-says-report-354475-2022-11-28.
[2]Ashwin Manikandan, Anandi Chandrashekhar, "Juspay Data Leak fallout: RBI swings into action to curb cyberattacks", *The Economic Times,* 6 January 2021, https://economictimes.indiatimes.com/tech/technology/juspay-data-leak-fallout-rbi-swings-into-action-to-curb-cyberattacks/articleshow/80125430.cms
[3] "Judgement in Plain English Constitutionality of Aadhaar Act", "*Supreme Court Observer*, accessed 22 December 2023,https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/

Section 19 (f) The power to notify standards and conformity measures on encryption is a sweeping power that allows the central government to potentially request for backdoors on encryption, or ask for alternatives to end to end encryption such as client side scanning, which have been critiqued[4] as measures that undermine privacy for all users. If the objective is to provide recommendations for certain encryption techniques when dealing with sensitive government data, a more specific compliance certification can be issued to such firms. For example, the United States government mandates certain government agencies to comply with the Federal Information Processing Standards (FIPS)[5] which also apply to non-government firms holding government contracts. Standards like FIPS recommend specific cryptographic modules to ensure secure communication of sensitive data. Such conditions and cases must be explicitly scoped in defining the standard setting powers of government with regard to encryption, in consultation with the industry and civil society organisations.

2. Provisions for public emergency or public safety

Section 20(2) (a) - Messaging apps such as WhatsApp and Signal enable end to end encryption, where messages are encrypted on endpoints such as user devices. Service providers and intermediaries cannot decrypt messages. Requiring messages to be amenable to disclosure in an 'intelligible format' is technically impossible within the end to end paradigm of privacy engineering[6]. Technical means of disclosing the contents of messages can either reside on a user's device, in a middle-box that mediates communication, or on servers where some computation can occur. Restructuring end-to-end encrypted communication networks to facilitate these technical means of disclosure would result in the creation of potential points of vulnerability and encryption backdoors. These vulnerabilities can be exploited by malicious actors and backdoors act as 'intentional vulnerabilities'[7] that can be used for excessive surveillance of communication that users believe to be private.

Section 20 (2) states the grounds for which such information may be sought. These include sovereignty and integrity of India, defence and security of the State, friendly relations with foreign States, and public order. Prima facie, these may appear to be reasonable grounds for facilitating government access, however, the current phrasing is too wide and leaves room for an expansive interpretation. This is particularly true for maintenance of "public order" that is

---

[4] "Why Adding Client-Side Scanning Breaks End-To-End Encryption", *The Electronic Freedom Foundation*, accessed 22 December 2023,
https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.
[5] "Compliance FAQs: Federal Information Processing Standards (FIPS)", NIST, accessed December 22 2023.
https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips
[6] "Personal Data in the Cloud Is Under Siege. End-to-End Encryption Is Our Most Powerful Defense.", *Lawfare,* accessed 22 December 2023,
https://www.lawfaremedia.org/article/personal-data-in-the-cloud-is-under-siege.-end-to-end-encryption-is-our-most-powerful-defense
[7] "Breaking Encryption Myths", *Global Encryption Coalition,* accessed 22 December 2023,
https://www.globalencryption.org/2020/11/breaking-encryption-myths/

routinely invoked in a variety of situations.[8] According to research conducted in 2021 by Vrinda Bhandari and others on the "Use and Misuse of Section 144 found orders issued under the guise of public order restrictions to regulate a variety of activities, many of which would not qualify as illegal activities per se. For instance, orders were issued to prohibit flying of hot air balloons, unmanned aerial vehicles, unmanned aircraft systems, use of "special" or "metallic" manjhas to fly kites and carrying tiffin boxes inside cinemas.[9] And tracing encrypted messages to thwart such perceived public order threats would be excessive and disproportionate. The order to intercept, detain, disclose or suspend a communication made between private individuals, acts as a violation of privacy and provides extensive grounds to surveil people.[10]

These grounds may be used to intercept or monitor all communication where a particular word or set of words is used. And its implementation would require communication of all users to be monitored effectively leading to a lower degree of privacy for all users[11] - including internet communication based apps due to definitional ambiguity. The Supreme Court has held that any infringement of the right to privacy should be proportionate to the need for such interference.[12] The judgement in the Puttaswamy case provides some guidance to assess the limits and scope of the constitutional right to privacy in the form of the three prong test. The test requires the existence of a law, a legitimate state interest and the restriction (to privacy) should be 'proportionate'. This provision violates a user's fundamental right to privacy since it fails to meet the proportionality requirement as laid down by the Supreme Court.

Section 20 (2) (b) provides for suspension of telecommunication service or class of services on similar grounds. The Bill empowers the DoT to suspend telecommunication services and if applicable to internet based communication services such as WhatsApp, Signal, among others without the need for any judicial oversight or procedural safeguards as enunciated by the Supreme Court in Anuradha Bhasin vs Union Of India. The provision must incorporate an independent oversight mechanism for such orders and also incorporate safeguards laid down by the Supreme Court in the Anuradha Bhasin judgement[13] to prevent arbitrary, frequent, and prolonged suspension of telecommunication services in India.

---

[8] Smriti Parsheera "Political misinformation is a problem. But asking WhatsApp to risk user privacy is the wrong solution", *The Indian Express,* October 28 202 https://indianexpress.com/article/opinion/editorials/remedy-worse-than-malaise-9002600/.

[9] Vrinda Bhandari, *et al,* The Use and Misuse of Section 144 Cr.P.C, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4404496_code2801004.pdf?abstractid=4389147&mirid=1&type=2

[10] CIS' Comments to the (Draft) Indian Telecommunication Bill 2022 *"Centre for Internet and Society,* accessed 22 December 2023 https://cis-india.org/telecom/blog/cis-comments-to-draft-indian-telecom-bill-2022#:~:text=Comment%3A%20The%20draft%20bill%20attempts,power%20over%20the%20local%20government.

[11] The Telecommunications Bill, 2023, *PRS Legislative Research,* accessed 22 December 2023, https://prsindia.org/billtrack/the-telecommunication-bill-2023

[12] Justice K.S. Puttaswamy (Retd) vs Union of India, W.P.(Civil) No 494 of 2012, Supreme Court of India, September 26, 2018.

[13] Writ Petition (Civil) NO. 1031 OF 2019, accessed 22 Decmber 2023, https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf.

Protection of users

1. Measures for protection of users

Section 28 - This section should also provide mechanisms for de-registering from “specific messages” . While this section mentions the need for prior consent of users for receiving the specified messages/ class of specified messages, it should look at the full spectrum of rights the Digital Personal Data Protection Act 2023 provides, which includes the right to withdraw consent. Hence we suggest that Section 28(3) adds that the authorised entity providing telecommunication services shall establish an online mechanism for withdrawal of consent, in addition to grievance redressal.

2. Duty of users

Section 29 - While listing out the duties of the users the Act puts the onus on the user to furnish correct information. It fails to take into account instances where the information is fed into the system by third parties, due to issues of access and literacy on the part of the users. While the section heading states “duty of the user” the preceding text “no user shall” has the potential to penalise users for acts carried out without a malicious intent. Additionally, there is also a need to look at how notices and terms and conditions of most telecommunication services are primarily in English, making it even more difficult for a large number of Indian users to read and hence understand the requirements. Furthermore, the associated penalty for failing to comply with these provisions are, i.e. up to INR 25,000 for the first offence and for the second or subsequent offences, up to INR 50,000 for every day till the contravention continues. Considering the low digital literacy rates, the government would be well advised to reconsider imposition of such hefty fines.

If applicable on internet based services, this will also impact the ability of a user to retain anonymity over the internet. Individuals may choose to remain anonymous online for a number of reasons. It is important to understand that an individual may remain anonymous for a variety of legitimate purposes such as expressing opinions about their employers and whistleblowers, providing anonymous tips to newspapers or law enforcement, expressing political opinions and criticism that may be subject to persecution, or simply someone saying something that they may be embarrassed about. [14] In India, in particular, an individual’s caste can be identified from their name, and they may choose to remain anonymous or adopt a pseudonym to escape centuries of stigma and discrimination that their communities have faced. The broad definition of telecommunication services as elaborated above places

[14]Palme, Jacob, and Mikael Berglund. *"Anonymity on the Internet."* Accessed 22 December 2023: 2009.

restrictions on anonymity online and severely degrades an individual's ability to exercise their fundamental right to freedom of expression.