Internet Impact Brief

Draft Indian Telecommunication Bill, 2022

Neeti Biyani, Pranav Bhaskar Tiwari, Akriti Bopanna, Internet Society
Prateek Waghre, Anushka Jain, Internet Freedom Foundation
Contributors: Rajnesh D. Singh, Joseph Lorenzo Hall, Carl Gahnberg, Ryan Polk, Susannah Gray, Internet Society
9 November 2022

Abstract

In September 2022, the Government of India's Department of Telecommunications released a draft of the Indian Telecommunication Bill, 2022 for public consultation. The Bill aims to create a comprehensive and contemporary framework for the regulation of telecommunications in the country.

The Bill expands several legal definitions, including that of a 'telecommunication service,' and presents a number of onerous regulatory requirements for Internet-based service providers and users alike. The Bill threatens the open, globally connected, secure and trustworthy Internet several ways. Of most concern are requirements on the part of Internet-based service providers to obtain licenses to continue offering services in India; extensive Know-Your-Customer (KYC) requirements for users to verify their identity on service platforms; threats against encryption, especially end-to-end encryption; and the government's move to unilaterally cement its powers to order Internet shutdowns.

This Internet Impact Brief analyzes various aspects of the Bill from the point of view of what the Internet needs to exist and thrive. We find that the Bill's provisions undermine the critical properties of the Internet as well as the enablers of an open and trustworthy Internet. It places unnecessary barriers and burdens on businesses and users alike, and harms user privacy.

Ultimately, the Telecom Bill is unlikely to achieve its aims of efficiently regulating the telecommunications sector in India. Competing legislation and rules from other ministries and bodies such as the Ministry of Electronics and Information Technology (MeitY) as well as the Computer Emergency Response Team – India (CERT-In), also pose jurisdictional issues. Instead, this legislative proposal is likely to severely impact the digital economy and the GDP of the country, subject millions of users to greater risk of harm, and jeopardize the security of individuals and businesses.

An open, globally connected, secure and trustworthy Internet is a force for good for everyone—and the Government of India must ensure that laws and regulations uphold the properties that enable the Internet to exist and thrive.

Methodology

The Internet owes a great deal of its strength and success to a series of critical properties that, combined, represent the Internet Way of Networking (IWN): an accessible Infrastructure with a common protocol, a layered architecture of interoperable and reusable building blocks, decentralized management and distributed routing, a common global identifier system, and technology-neutral general-purpose network.

In order to assess whether the proposed actions have an impact on the Internet, this report will examine their impact on the IWN foundation the Internet needs to thrive as an open, globally connected, secure and trustworthy resource.

Context

The Draft Indian Telecommunication Bill, 2022 is an attempt by the Department of Telecommunications (DoT), under the Ministry of Communications, to consolidate various laws that currently govern the provision, operation and development of telecommunications in India. The Bill repeals the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and The Telegraph Wire (Unlawful Protection) Act, 1950—two of which were enacted before the country asserted its status as an independent republic.

The Government of India has stressed that it is considering a complete overhaul[1] of cyber laws—the Telecommunication Bill, 2022 should not be considered in isolation, but as part of a larger digital framework, and is going to be followed by a Digital Personal Data Protection Act and the Digital India Act.

The Bill empowers the Union Government to govern three crucial aspects of telecommunications:

- Telecommunication equipment and infrastructure;
- Telecommunication services and networks; and
- Spectrum.

[1] 'IT Ministry Will Soon Come Up with New Version of Data Protection Bill, Says Union Minister Ashwini Vaishnaw', The Times of India, September 5, 2022. https://timesofindia.indiatimes.com/india/it-ministry-will-soon-come-up-with-new-version-of-data-protection-bill-says-union-minister-ashwini-vaishnaw/articleshow/94010672.cms

The Bill therefore applies to any entity or body that provides telecommunication services, operates telecommunications networks, owns telecommunications equipment or infrastructure, or has been assigned or seeks spectrum.

Given the broad approach of the Bill, this Internet Impact Brief will analyze the following aspects of the proposed legislation from the perspective of the Bill's impact on the open, globally connected, secure and trustworthy Internet.

Expanded Definitions

The most far-reaching impact the Bill has is through widely expanded legal definitions. The Bill expands the definition of 'telecommunications services' to include several new services within Clause 2(21), including:

- Broadcasting services
    - Direct to Home (DTH) services such as Tata Sky, Airtel Digital TV, Videocon DTH
    - Community radio such as Radio Dehradun, Radio Rajasthan, Radio Bulbul
    - FM radio broadcasting services through private agencies such as Big FM, Red FM
    - Internet Protocol Television Services such as Bharti Airtel, MTNL, BSNL
    - Television channels
- Electronic mail such as Yahoo, Hotmail, Gmail
- Voice mail such as Vodafone, Airtel
- Voice call services such as Vodafone, Airtel
- Video communication services such as Skype
- Data communication services
- Audiotex services
- Videotex services
- Fixed and mobile services such as MTNL, BSNL, Jio
- Internet and broadband services such as Airtel, Spectra, Excitel
- Satellite based communication services
- Internet based communication services such as WhatsApp, Gmail, Zoom, Microsoft Teams
- In-flight and maritime connectivity services
- Interpersonal communications services such as Signal, Telegram, WhatsApp
- Machine-to-machine communications services such as smart cars, smart TVs, smartwatches, industrial sensors
- Over-the-top or Internet-based communications services such as Zoom, Facetime, Google Duo, Instagram, Twitter

It is important to note that most terms and services have not been defined, and the examples included against each are based on our interpretation. This creates significant scope for ambiguity, overreach and overlap. A number of service providers serve multiple functions and offer a wide variety of services,

thus creating uncertainty about the application of the law - what pieces of the law will apply, in which cases and to what degree.

The Bill also defines the term 'telecom' as a "transmission, emission, or reception of any message by wire, radio, optical or other electro-magnetic system" and the term 'message' as "any sign, signal, writing, image, sound, video, data stream or information intended for telecom".

The inclusion of potentially every communication system available, whether it uses spectrum or cable, or is Internet-based, has significant impact on the open, global, interoperable Internet.

Licensing, Registration, Authorization and Assignment

The provisions contained under Clause 3 of the Bill give the government the exclusive privilege to provide telecommunication services, and the power to exercise its privilege by granting a license to entities providing telecommunication services. Thus, every entity within the ambit of a 'telecommunications service' including Google Meet, Signal, Gmail, Instagram, Zoom, Microsoft Teams etc. will be required to obtain a license from the Government of India to be able to continue providing services in India.

The Bill's following clauses also specify that the procedure for the government exercising this 'privilege' may be prescribed through rules at a later date, including license and registration fees, payment of entry fees, or any other charges and fees.

This move towards regulating Internet-based services has been a persistent demand by traditional telecom companies. They argue that the lack of regulation of Internet-based platforms such as WhatsApp and Zoom creates an uneven playing field, resulting in a loss of revenue for telecom companies and creates the need to compensate telecom companies for their losses. This argument, popularly known as "same service, same rules", has surfaced over the last few years in several jurisdictions across the world.

In a submission[2] made to the Telecom Regulatory Authority of India (TRAI) in 2017, the Broadband India Forum (BIF) asserted that the "same service, same rules" argument is flawed and misleading. BIF is of the opinion that telecom companies control the underlying Internet access infrastructure, and are the gatekeepers to Internet access. Anybody looking to access Internet-based services cannot do so without paying a subscription fee to a telecom company. Thus, even the argument that Internet-based services "free-ride" on telecom services is unfounded. In fact, many Internet-based services make huge investments in networks and telecom infrastructure, such as data centers, content delivery networks,

[2] 'Counter Comments from BIF on TRAI Consultation Paper on Net Neutrality', Broadband India Forum, https://trai.gov.in/sites/default/files/BIF_27_04_17.pdf

cache servers, undersea cables, etc. They are also responsible for creating demand for bandwidth for easier consumption of content, and in doing so, creating opportunities for telecom operators to profit from providing higher speed and enhanced access subscription offerings.

Further, a telecommunication service operates as an application that is intrinsically linked to a specialized network (e.g. SMS over the traditional phone network), while Internet-based services are applications deployed over the general-purpose Internet. Internet-based services are also qualitatively distinct from telecom service providers as they provide a richer communications environment than voice calls and traditional text messaging services, and foster innovation along a number of axes. Regulation of Internet-based services in the manner prescribed in the Bill would lead to significant curbs in innovation and the proliferation of new services.

Telecom service providers also enjoy exclusive rights conferred upon them through their licenses, such as the right to acquire a scarce natural resource like spectrum, the right to obtain telecom numbering resources, and the right of way to set up infrastructure - all of which are not privileges enjoyed by Internet-based services.

The utilization of public resources such as spectrum and right of way by telecom operators affords them an economic advantage.[3] Telecom operators are often provided crucial infrastructural assets, essential facilities, state subsidies, concessions and territories necessary for their functioning. Telecom markets therefore have high barriers to entry and are inclined to concentration and lack of competition. Meanwhile, the Internet is a neutral, general-purpose space which encourages the entry of new actors and players by presenting minimal barriers to entry. By virtue of these characteristics, the Internet has been crucial for the founding and flourishing of numerous micro- and small-businesses and endeavors, and has given a voice to vulnerable and marginalized sections of society. Thus, regulating Internet-based services and applications as if they were a traditional telecommunications service, would not only harm innovation, but also stifle the voices and labor of the already disadvantaged.

User Privacy

The Telecom Bill, 2022 mandates that every entity receiving a license must "unequivocally identify the person to whom it provides services, through a verifiable mode of identification as may be prescribed." While the mode of identification is ambiguous in the current text of the Bill, service providers will need to ascertain the identity of each user. The Bill also lays emphasis on the need to prevent cyber fraud, and establishes the need to make the identity of a person placing calls or sending a message using telecommunication services.

[3] Chima, R.J.S., and Palero, J., 'Internet vs. Telecommunications services: differences that matter for users' rights', Access Now, May 22, 2017. https://www.accessnow.org/ott-vs-telecom-services/

The need to prevent cyber fraud is important, but excessive data collection and retention by several entities in the absence of a data protection framework in the country is concerning. These provisions take away the right of a person to stay anonymous while communicating. Anonymity is not a secondary concern, but central to our security and privacy in the information age. In his report[4] to the Human Rights Council, Special Rapporteur on freedom of opinion and expression, David Kaye notes that "encryption and anonymity in digital communications deserve strong protection to safeguard individuals' right to exercise their freedom of opinion and expression."

This would also have a negative impact on addressing cyber fraud. People's data will be more susceptible to theft, fraud will be easier to pull off, blackmail and other crimes will be easier—simply because data will be linked to people's identity.

There is also little clarity about the ability users will have to delist themselves in case they don't want their details to be shared with receivers of messages, or the ability of users to have their data erased and forgotten.

Encryption

Billions of people across the world rely on encryption–often without realizing–to secure their lives online, whether they are making bank transactions, buying something online, working, learning or sharing personal thoughts with loved ones. It is the best digital tool available to keep ourselves safe from criminals, eavesdroppers and malicious actors online. End-to-end encryption (e2ee) is the strongest form of encryption available, which ensures nobody apart from the sender and receiver of information has access to it, not even the service provider.

Despite encryption's crucial role online and offline, the Bill has significantly adverse impacts on encryption, especially e2ee messaging platforms like WhatsApp and Signal, e2ee email platforms, or zero-knowledge cloud service providers. Clause 24(2) empowers the government at the Union and state levels to block the transmission of, intercept or disclose a "message or class of messages," "to or from any person or class of persons," or "relating to any particular subject." This can be done if the government feels it is necessary, expedient, in the interest of the country's sovereignty, integrity or security, friendly relations with other countries, public order, or to prevent incitement to an offence.

This essentially means that e2ee platforms, in order to comply with the Bill, will be compelled to:

- Weaken security by providing backdoor or exceptional access to end-to-end encrypted content in order to grant government access;

[4] Kaye, D., 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', May 22, 2015. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

- Bypass e2ee entirely by getting access to content before or after the encryption process, through methods such as client-side scanning[5] or storing a copy of every message sent; or
- Not offer e2ee at all.

The negative consequences of forcing platforms to weaken security afforded to users by strong encryption would be detrimental to the safety, security, privacy and livelihood of users, businesses and governments worldwide. It would also result in severe financial losses[6] due to erosion of trust in secure, private communications. Strong encryption, especially e2ee keeps all of us safe online and offline, especially children, the elderly and vulnerable sections of the population. Preventing people from locking the doors to their house makes the owner more vulnerable to criminals and intruders, and that's exactly the result of weakening encryption. Criminals and malicious actors could gain access to sensitive and personal information.

Previously, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Draft Encryption Policy, 2015, as well as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also contain clauses that severely undermine encryption. The Government of India must uphold and continue to protect strong encryption, not simply for the sake of individual privacy, but to promote the national economy and national security.

Internet Shutdowns

The Government of India, through Clauses 24(2)(b) and 25(1)(f) of the Telecom Bill, 2022, cements its power to suspend Internet services. Similar to clauses on encryption, the Bill specifies that the communications or telecommunications networks may be suspended if the government finds it necessary, expedient, in the interest of the country's sovereignty, integrity or security, friendly relations with other countries, public order, or to prevent incitement to an offence.

According to Top10VPN, India shut down the Internet for 1,157 hours in 2021, resulting in economic losses in the bracket of $583 million.[7] Over the last three years, the Internet was shut down in India for a cumulative 14,280 hours, costing the national economy $4.7 billion.[8]

---

[5] 'Client-Side Scanning: What It Is and Why It Threatens Trustworthy, Private Communications', Internet Society, September 2, 2022. https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

[6] 'New Study Finds Australia's TOLA Law Poses Long-term Risks to Australian Economy', Internet Society, June 1, 2021. https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

[7] Woodhams, S., and Migliano, S., 'Government Internet Shutdowns Have Cost $35.5 Billion Since 2019', Top10VPN, October 11, 2022. https://www.top10vpn.com/research/cost-of-internet-shutdowns/

[8] 'IFF provides inputs to UN on Internet Shutdowns', Internet Freedom Foundation, February 11, 2022. https://internetfreedom.in/ohchr-internet-shutdowns-submission/

The Internet is a key driver of the national economy, and indeed the global economy. The Government of India has itself recognized the increasing contribution of the digital economy to the national GDP, and has launched public programmes to increase digital literacy, digital reach, and reliance on digital platforms for the delivery of public services. Further, the government is also aware of India's competitive edge in the digital sector. The Internet is crucial to these national aspirations, the national economy, the government's public service delivery programmes as well as countless citizens' livelihoods and self-expression.

The Parliamentary Standing Committee on Communications and Information Technology, in its 26th report, 'Suspension of Telecom Services/Internet and its Impact',[9] elaborated the impact and misuse of Internet shutdowns in the country, and how grounds of 'public emergency' and 'public safety' are thrown around to legitimize Internet shutdowns. The report also recommended that the government avoids the frequent suspension of the Internet on "flimsy grounds" in this day and age of ubiquitous digitization.

The Supreme Court of India, while hearing Anuradha Bhasin vs. Union of India (2020),[10] also expressed its displeasure at the frequent Internet shutdowns and opined that Internet shutdowns should only be ordered in case they are absolutely necessary and only after carrying out balancing tests as a restrictive step. Further, in January 2020, the Supreme Court ruled[11] that the right to access the Internet is a fundamental right under Article 19 of the Constitution - that accessing the Internet to express speech and carry out trade is a fundamental right.

The provisions in the Telecom Bill, 2022 go against these observations and recommendations, essentially cementing the ability of Union and state governments to shut the Internet down on arbitrary and unjust grounds, under the guise of public emergency and safety.

How does the India Telecom Bill, 2022 Affect the Realization of the Full Potential of the Internet?

What the Internet Needs to Exist

[9] 'Twenty-Sixth Report: Suspension of Telecom Services/Internet and its Impact', Standing Committee on Communications and Information Technology, December 1, 2021. https://eparlib.nic.in/bitstream/123456789/820699/1/17_Communications_and_Information_Technology_26.pdf

[10] Anuradha Bhasin vs. Union of India, (2020) 3 SCC 637.

[11] Krishnan, M. 'Access to Internet Is a Fundamental Right, Says Supreme Court.' Hindustan Times, January 11, 2020. https://www.hindustantimes.com/india-news/access-to-internet-is-a-fundamental-right-says-supreme-court/story-miomQARGJTy7Cz1WPazENI.html

The Internet owes its success not only to the technology that makes it work, but to the unique way it operates and evolves. The Internet Way of Networking[12] describes a foundation of critical properties that, all together, are what the Internet needs to exist and work for everyone. The Internet's unprecedented growth and success is a direct result of people and organizations committed to protecting this foundation as the Internet has expanded worldwide. This section examines how the Indian Telecommunication Bill, 2022 would impact certain critical properties that the Internet requires to exist and function.

Critical Property 1: An Accessible Infrastructure with a Common Protocol

You don't need permission from a central authority to connect to the Internet. You find a point nearby, make arrangements to connect, and you're on the Internet. The network is extended by the many different kinds of organizations that connect to it. There is no international policy on who can connect or what they should pay; these factors are largely driven by the market, not a centralized authority.

The Telecom Bill, in expanding the definition of a telecommunication service as well as mandating every telecommunication service to seek a license to continue operating in the country, fundamentally undermining this Critical Property of the Internet. The Bill also says that license and registration fees, payment of entry fees, or any other charges and fees may be notified by the government at a later date.

These requirements impact user accessibility and could potentially cause disruption of services, thereby resulting in significant economic losses and a fractured business environment in India. The digital economy is a large contributor to the country's GDP, and the government risks large-scale harm to this thriving sector due to this requirement. The consequences of requiring Internet-based services to engage in licensing, registration and fee payment will disproportionately impact smaller, cash-strapped platforms and start-ups which would need to spend crucial resources in complying with the Bill.

The Bill in Schedule 3, lays out a penalty for providing telecommunication services or establishing a telecommunication network without obtaining a license - imprisonment up to one year, or a fine up to INR 5 million, or both. Additionally, a person or entity may be fined up to INR 100,000 for using an unlicensed telecommunication network, infrastructure, or network, either knowingly or having reason to believe it to be unlicensed.

This lays an extremely heavy, onerous compliance burden on all entities under the broadened ambit of 'telecommunication services' to ensure that their licenses are in place, up to date, and maintained. They will also need to keep a keen, vigilant eye on any changes in the licensing regime. However, the fines

[12] 'The Internet Way of Networking: Defining the critical properties of the Internet', Internet Society, September 9, 2020. https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

proposed for users availing services that do not have a license is highly unwarranted. It is simply not possible for all users, regardless of age, literacy, background, access, etc. to be aware of the status of every service provider's license.

Critical Property 5: A Technology Neutral, General-Purpose Network

The Internet is designed as a general-purpose network—not optimized for voice, particular usage patterns, or special traffic characteristics. The Internet is completely agnostic about the type of content that flows through it, guaranteeing neither quality nor connectivity, yet delivering enough of both to be a base layer for information services, commerce, communications, recreation, and more.

The requirement for a telecommunication network to block, intercept, detain or disclose a message has repercussions for the technology neutral, and general-purpose character of the Internet. The Internet was designed as a general-purpose network - in simple words, the Internet was built for doing many things and not for a specific purpose.

Clause 24(2) of the Bill authorizes the Union and state governments to direct that "any message or class of messages, to or from any person or class of persons, or relating to any particular subject" being transmitted or received by telecommunication services or telecommunication networks can be blocked, intercepted, detained, or disclosed. The requirement for telecommunication services to enable this has an impact on encryption, but when applied to a telecommunication network, this requirement has serious adverse impacts on the open architecture and interoperability of the Internet.

The network layer of the Internet is where network-to-network connections are made, enabling devices connected on different networks to communicate with one another. The network layer, being a part of the Internet's infrastructure is responsible for sending packets of data back and forth between different networks. The network layer is agnostic about the data being passed back and forth and often has little if no insight into what any given piece of data pertains to. In other words, this layer of the Internet does not and should not have the ability to gauge or filter data. This is not its function to play, and instrumenting it to do so would begin to collapse core parts of why the Internet works as well as it does to deliver information and services.

Clause 24(2), in requiring telecommunication networks to identify and subsequently filter data the government finds objectionable, will fundamentally disrupt the Internet's functioning. It will compel networks to invest in expensive data and content filtering mechanisms, delay data transmission and make interoperability nearly impossible. Without the technology-neutral, general-purpose approach, innovation over the Internet and the digital economy would suffer.

What the Internet Needs to Thrive

In addition to the critical properties the Internet needs to exist, there are additional characteristics, or 'enablers', that it needs to thrive. The Enablers of an Open, Globally Connected, Secure and Trustworthy

Internet[13] can help us get closer to the kind of Internet we want, and that many countries and organizations worldwide have committed to supporting, now and in the future. The following section analyzes how the Indian Telecommunication Bill, 2022 would impact these enablers, preventing the Internet and everyone that uses it from benefiting from its full potential.

Easy and Unrestricted Access

It is easy to become part of the Internet, for networks and users alike. Network operators can easily add themselves to the Internet's infrastructure without unnecessary regulatory or commercial barriers. Responsive Internet infrastructure creates an Internet that is affordable for users and that has accessible services, empowering users to connect and use the Internet with minimal barriers.

The Internet was built and developed in a voluntary, decentralized, and permissionless manner. This permissionless model that the Internet is predicated upon, presents lowest possible technical barriers to new actors when they choose to enter, connect to, or innovate on the Internet. This implies that there are no unnecessary barriers for connecting to and building services on top of the Internet's infrastructure. The Telecom Bill counters this principle via its mandates for licensing, Know-Your-Customer (KYC) registers, and interception. The Bill's provisions for Internet shutdowns without requisite checks and balances also impinges upon the unrestricted access to the Internet.

The Bill grants the Union Government the exclusive privilege to provide telecommunications services and require every entity under the ambit of a 'telecommunications service' to obtain a license to continue operating in the country. The International Telecommunication Union (ITU) encourages voluntary agreements between telecom service providers and Internet-based service providers to nurture commercial cooperation.[14] The provisions pertaining to licensing under the Bill are in stark contrast to the international practices envisaged at the ITU. The ITU does not prescribe any regulatory mechanism for Internet-based service providers, except for certain standards for consumer and data protection. Thus, the extension of licensing requirements for all Internet-based services, apps, and platforms as contained within the Bill is an unnecessary compliance thwarting easy and unrestricted access to an open Internet.

Clause 48 of the Bill lays down that if an offence is committed by a company, its employees, who at the time were responsible for conducting business related to the 'offence', shall be liable and punished accordingly. The Bill states further that if a service provider like Telegram or Signal continues to provide services in India without a license from the Union Government, their officers may be criminally

[13] 'Enablers of an Open, Globally Connected, Secure and Trustworthy Internet', Internet Society, November 8, 2021. https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

[14] 'Enabling environment for voluntary commercial arrangements between telecommunication network operators and OTT providers', International Telecommunications Union, September 28, 2020. https://www.itu.int/rec/T-REC-D.1101-202008-I/en

prosecuted. On an even more concerning note, if a user continues to use such unlicensed services, they may be fined a hefty amount of 100,000 INR.

This part of the Bill is one that is perhaps most divorced from the stated aims of the Bill - protecting user rights. In effect, the government is requiring each and every user, regardless of age, literacy, background, access, etc. to be aware of the status of every service provider's license - an impossible requirement. The grounds "having reason to believe so" may be misused and may put the user at a disadvantage as it appears to place the burden on them to prove lack of knowledge about the license status of any service provider.

Further, the Bill requires licensed telecommunication services to unequivocally identify the person(s) using the service through a verifiable mode of identification. Given the ambiguity in the bill, it can be assumed that a verifiable mode of identification would include a government-issued identification or a biometric signature. This requirement undermines this Critical Property of the Internet, by breaking the permissionless model of the Internet, and creating barriers of entry for people.

This is especially harmful and disadvantageous for sections of the population which struggle with literacy and digital literacy, do not possess the means and resources to obtain or maintain government-issued identification, people living in remote areas including tribal groups, and groups which engage in hard labor or do not have 'verifiable' or 'reliable' biometric information.

Finally, in cementing the government's power to order Internet shutdowns, the Telecom Bill impacts easy and unrestricted access to the Internet. Right to free speech, right to information, and freedom of the press are facets of freedom of speech and expression as envisaged under Article 19(1)(a) of the Constitution of India. In the digital age, these facets are conjoined with one's right to uninterrupted access to the Internet.

In light of these realities, the Kerala High Court in Faheema Shirin R.K. v State of Kerala[15] declared that the right to the Internet is an inherent part of the right to education under Article 21A and right to privacy under Article 21. Despite these precedents, Internet shutdowns continue to be ordered on arbitrary grounds in the country.[16]

Unrestricted Use and Deployment of Internet Technologies

The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, OS vendor, or network

[15] Faheema Shirin R.K. vs. State Of Kerala (2019) SCC OnLine Ker 2976.

[16] 'The internet cannot be suspended in entire districts to prevent cheating in exams - IFF writes to the Rajasthan Government', Internet Freedom Foundation, September 27, 2021. https://internetfreedom.in/the-internet-cannot-be-suspended-in-entire-districts-to-prevent-cheating-in-exams-iff-writes-to-the-rajasthan-government/

provider. The Internet's infrastructure is available as a resource to anyone who wishes to use it in a responsible and equitable way. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities.

The requirement to detain, intercept or disclose messages under Clause 24 of the Bill restricts how end-to-end encryption (e2ee) can be used or deployed. The policy prescription to intercept messages on the ground of public emergency or public safety fails to appreciate the fundamental nature of e2ee - only the sender and receiver can see the information exchanged. No third party, whether it is law enforcement, non-state actors or the platform itself can view the message. Mandating interception of messages in such a scenario is against the unrestricted use and deployment of e2ee technology. With the traceability provision envisaged under Rule 4(2) of the IT Rules, 2021 being disputed before the Delhi High Court, the overarching mandate under Clause 24 of the Bill is unwarranted.

Unrestricted Reachability

Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves, contributing to the Internet's role as a resource of global knowledge production. Once a resource has been made available in some way by its owner, there is no blocking of use and access to that resource by third parties.

The Telecom Bill, via Clause 24(2)(b), empowers the government to restrict access to the Internet and may restrict it to only any communication or class of communications, person or class of person or pertaining to any particular subject. Clause 25(1)(f) empowers the government with carte blanche power to take over control and management of, or suspend the operation of, telecom services. These powers are triggered if the Government deems it is 'necessary or expedient' to do so in the interest of public emergency or public safety and national security, external relations, or war.

The United Nations considers cutting off users from Internet access, regardless of the justification provided, to be disproportionate and thus a violation of Article 19(3) of the International Covenant on Civil and Political Rights.[17] It also calls upon all States to ensure that Internet access is maintained at all times, including during times of political unrest.

Internet shutdowns remain a disproportionate reaction that often only hides - instead of solving - a perceived problem, and can result in significant collateral damage. We believe Internet shutdowns harm societies, economies, and the global Internet infrastructure. We are therefore of the position that the Internet must remain on and strong, no matter what, in order to build strong economies and give people an opportunity for a prosperous future.

[17] 'UN Human Rights Council Resolution A/HRC/17/27', May 16, 2011. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

At a time when governments of the world have committed to leveraging the power of the Internet and Information and Communications Technology (ICTs) to fulfil the Sustainable Development Goals in areas such as education, health, and economic growth, cutting off entire populations from the Internet is extremely counterproductive.

Further, the licensing regime proposed by the Bill will not only create unnecessary barriers in operations and disrupt the digital economy, but also risk making certain services, applications, and platforms unavailable and unreachable to users. This will also disproportionately impact smaller services, platforms, and start-ups, who will have to expend crucial resources in complying with these requirements to ensure their continued availability.

Available Capacity

The capacity of the Internet is sufficient to meet user demand. No one expects the capacity of the Internet to be infinite, but there is enough connection capacity – ports, bandwidth, services – to meet the demands of the users.

The Bill enhances the scope of the existing Universal Service Obligation Fund which was previously restricted to universal service in remote areas. The proposed Telecom Development Fund would extend universal service to underserved rural, remote, and urban areas; R&D of new technologies, products, and services; support for skill development and training; support for pilot projects; and introduction of new telecom services, technologies, and products. These efforts will increase the availability of Internet resources for users.

While the scope of use of the Telecom Development Fund has been enhanced to further increase the availability of Internet resources, the Bill missed the opportunity to foster collaboration between the Union, state, and district authorities for the maintenance of the existing telecom infrastructure.[18] After twenty years of its introduction, about 50% of the Universal Service Obligation Fund remains unutilized. Despite the availability of funds there exists a stark rural-urban digital divide.[19]

According to the 2021 National Family Health Survey, 72.5 per cent of urban males and 51.8 per cent of urban females have used the Internet, against 48.7 per cent of rural males and 24.6 per cent rural females.[20] In the Twenty-Eighth Report of the Standing Committee on Rural Development and Panchayati Raj (2021-2022), the Standing Committee noted that the despite appraising the Ministry of

[18] Muldiar, P., 'A Reality Check on India's Search for Digital Utopia', The Hindu Centre, August 24, 2022. https://www.thehinducentre.com/the-arena/current-issues/a-reality-check-on-indias-search-for-digital-utopia/article64931311.ece#eleven11

[19] Tejpal, R., 'Why the government must suspend the USO levy, leave expansion of rural telephony to private telcos', The Economic Times, August 13, 2020. https://economictimes.indiatimes.com/prime/media-and-communications/why-the-government-must-suspend-the-uso-levy-leave-expansion-of-rural-telephony-to-private-telcos/primearticleshow/77514006.cms?from=mdr

[20] 'National Family Health Survey 2019-21, India Fact Sheet', International Institute for Population Sciences, http://rchiips.org/nfhs/NFHS-5_FCTS/India.pdf

Panchayati Raj (MoPR) about the dismal ground reality observed by the Committee during its study visits to various parts of the country, so far no corrective action has been taken by the Ministry pertaining to 'Digitization of Gram Panchayats'.[21] Given the urban-rural digital divide, the Telecommunications Development Fund should prioritize bridging it.

The proposed provisions in the Bill that give powers to the government to order Internet shutdowns restrict the capacity of the Internet available to the users, leading to numerous challenges. For instance, during the year-long denial to 4G services to the citizens of Jammu and Kashmir, numerous small businesses were not able to sustain themselves with access to just 2G services and many had to close their shops, while some went into debt.[22] About half a million people lost their job, education and learning were impacted, and crucial health services were inaccessible during a global pandemic.

The proposed Bill vests sweeping powers for the government to shut down the Internet without requisite checks and balances, impacting the availability of the Internet for the entire population.

Data Confidentiality of Information, Devices, and Applications

Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications and on devices. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet)

End-to-end encryption ensures what people share with each other online stays confidential between the two of them, i.e., the sender and the receiver of the information. The Telecom Bill, in authorizing the government to direct certain messages to be blocked, intercepted, detained, or disclosed, jeopardizes the security of people and businesses in India and across the world.

This is incompatible with e2ee since service providers themselves cannot access the communication between sending and receiving parties. Hence, platforms offering e2ee will be compelled to weaken security by providing backdoor or exceptional access to the government, or bypass e2ee entirely by getting access to content before or after the encryption process by methods such as client-side scanning, or not offer e2ee at all.

A complete withdrawal of e2ee communication platforms will not be a surprising move considering the withdrawal of Virtual Private Networks (VPNs) from India such as Nord, Proton, Surfshark etc. following

[21] 'Twenty-eight Report: Action taken on the Observations/Recommendations contained in Twenty Fourth Report on 'Demands for Grants' (2022-23) pertaining to Ministry of Panchayati Raj', Standing Committee on Rural Development and Panchayati Raj, August 3, 2022. http://164.100.47.193/lsscommittee/Rural%20Development%20and%20Panchayati%20Raj/17_Rural_Development_and_Panchayati_Raj_28.pdf

[22] Biyani, N., 'Internet Access Should Not be Disrupted to Serve Political Goals: Shutdowns in Jammu & Kashmir, India' Internet Society, Pulse, March 18, 2022. https://pulse.internetsociety.org/blog/internet-access-should-not-be-disrupted-to-serve-political-goals-shutdowns-in-jammu-kashmir-india

the onerous CERT-In Directions released earlier in 2022.[23] It is simply not possible for e2ee services to create backdoors, provide the Government of India with exceptional access and establish mechanisms for client-side scanning in the country without jeopardizing the safety, security, privacy, and communication of all their other customers globally.[24]

Several businesses in India are built upon services like WhatsApp and use them to carry out business transactions. Health services also use these platforms to collect patient information, share appointment details and medical reports, and update patients about progress and logistical details through the course of their medical care. Thus, an undermining of e2ee will have a ripple effect on the growth of e-commerce and digital healthcare, two significant priorities for the Government of India.

A recent study of the economic impact of laws that threaten or undermine encryption found Australia's TOLA Act to have a significant impact on local industry.[25] One company told researchers that they estimated the effect of weakening encryption to cause losses in the range of approximately US $700 million. When extrapolated for the digital economy in India, the losses could be immense.

Undermining or an effective prohibition of e2ee will not make people safer. On the contrary, it will make people, especially children, the elderly, and vulnerable sections of the population as well as their data less secure. It will make individuals and businesses extremely susceptible to large-scale data breaches and eavesdropping attacks. These breaches will result in financial and reputational damage to companies. Weakened protocols have also proven to be exploited by foreign governments, for instance, to access critical national infrastructure.[26]

Furthermore, compelling business communications platforms like Microsoft Teams, Slack etc. to intercept and disclose messages will create huge risks for businesses. Businesses and corporations need to maintain absolute privacy and confidentiality of their communications, and the Bill risks the possibility of commercial espionage and violations of intellectual property rights.

Finally, Clause 51 states that if the government (at the Union, state, or union territory level) is satisfied that a licensed or registered entity possesses any information, document, or record that is necessary to be furnished in relation to a pending or apprehended civil or criminal proceeding, the government can

[23] CERT-In Direction No. 20(3)/2022-CERT-In, April 28, 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[24] 'International coalition calls for withdrawal of Draft Indian Telco Bill: provisions threaten end-to-end encryption', Access Now October 27, 2022. https://www.accessnow.org/india-telecommunications-bill-encryption/

[25] Barker, G., Lehr, W., Loney, M., and Sicker, D., 'The Economic Impact of Laws that Weaken Encryption', June 1, 2021. https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/

[26] Zetter, K., 'Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA', Wired, December 22, 2015. https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

request such information. Subsequently, the concerned entity will have to comply with the direction of such officer.

The ambiguity in the Clause opens it for misuse. There is an absence of clear parameters of information which may be revealed and the specific circumstances in which the government may request it to be furnished, as the Bill allows requests to be made even in situations where illegal activity is apprehended. This vagueness may lead to overbroad requests for disclosure which could result in the violation of the right to privacy of users.

Integrity of Information, Applications, and Services

The integrity of data sent over the Internet, and stored in applications, is not compromised. That is, information sent over the Internet shouldn't be modified in transit, unless directed by the communicating parties (e.g., a captioning bot may be useful to turn spoken words into text). Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties.

Strong encryption keeps data safe and secure and prevents manipulations or attacks on the data at rest or in transit. Weakened encryption, a direct result of the Telecom Bill, will negatively impact integrity of data and information by making it much easier for a third party or malicious actors to manipulate the content of communication.

It also makes the possibility of and avenues for hacking easier since backdoors created for law enforcement can and will be discovered by malicious actors to access information. This could also lead to more machine-in-the-middle attacks, where a third party is secretly placed in the middle of a data exchange, intercepting messages and either reading or altering them before passing them along.[27]

Such attacks and manipulation of data could also lead to physical harm. With more and more devices and objects getting connected to the Internet, and each other, weakening encryption in one area will lead to negative consequences in another. Weakened encryption protocols will especially impact the Internet of Things (IoT), and in turn put people in dangerous situations. For instance, an IoT security breach due to lax security measures allowed cybercriminals to hack into several families' connected doorbell and home monitoring systems.[28]

Reliability, Resilience, and Availability

[27] Voge, C., and Wilton, R., 'Internet Impact Brief: End-to-end Encryption under the UK's draft Online Safety Bill', Internet Society and Internet Society UK England Chapter. January, 2022. https://www.internetsociety.org/wp-content/uploads/2022/01/IIB_Encryption_UK_Online_Safety_Bill_EN-1.pdf

[28] Paul, K., 'Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs', The Guardian, December 23, 2020. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats

The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations.

The consistency of our experience on the Internet relies on the predictability of its infrastructure, processes, and the services and applications we use - all of which ensure delivery of services to its users.

The Internet is a resource like no other. It facilitates countless opportunities for everyone who has access to it. For the Internet to continue to be a force for good, it is essential that it continues to be on and strong. By way of the Telecom Bill, the government assumes the right to shut the Internet down on ill-defined grounds of 'public safety' and 'public emergency'. This impacts the availability of Internet services, which in turn reduces trust in the Internet. If businesses are to host their service in India, and the service is unavailable to users frequently due to repeated Internet shutdowns in the country, this will impact users and businesses in equal measure.

Another key issue with the Telecom Bill is the widely expanded definitions of services included in its scope, leading to ambiguity and overlap. The Parliamentary Standing Committee on Communications and Information Technology met in the last week of October 2022 and expressed their concern about the lack of clarity in the definition of Internet-based (or over-the-top) services, data safety, and the privacy provisions in the proposed legislation.[29]

There is little precedence for the sort of licensing and registration regime proposed by the Telecom Bill. The Bill thus creates an uncertain regulatory environment for Internet-based services, which are currently facing onerous compliance requirements presented by the 2021 IT Rules, the 2022 CERT-In Cybersecurity Directions, and now the 2022 Telecom Bill. There is further confusion about which law to follow in case of an overlap, what law takes precedence, and how they co-exist.

For the sake of reliability, resilience, and availability, it is of utmost necessity that this over-regulation and regulatory overlap be addressed. Legislation and regulation need to be specific, comprehensive, and balanced. If this issue is not addressed, some services could simply withdraw from the Indian market - severely harming the digital economy, causing financial and job losses.

Clause 24 of the Bill lays out several actions permissible by the government in the event of public safety or public emergency, such as taking temporary possession of all telecommunication services, network or infrastructure from a licensee or registered entity. This clause does not mention a time limit

[29] 'Parliamentary panel members raise apprehensions about some provisions of draft telecom bill', The Economic Times, October 28, 2022. https://economictimes.indiatimes.com/news/india/parliamentary-panel-members-raise-apprehensions-about-some-provisions-of-draft-telecom-bill/articleshow/95151117.cms

for such temporary possession, implying an indefinite ownership is possible - even if it exceeds the circumstance of the emergency itself.

The Bill further includes all Internet-based services within the definition of a 'telecommunication service', and how Clause 24 will interact with their temporary possession is unclear. In practical terms, most Internet-based services span multiple jurisdictions, and can simply not handover themselves for temporary possession by the government.

Finally, the reliability and security of communication is eroded through weakened encryption, as it leads to reduced trust in the service as well as the Internet. The Global Encryption Coalition has multiple human stories and accounts of how the availability of strong encryption and their reliability on the technology kept them safe from harm in various dangerous and harmful situations - these should serve as a reminder that making a technology like e2ee or a service relying on e2ee less secure, less reliable, and less resilient stands to damage us all.[30]

Accountability

Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.

The Telecom Bill significantly overreaches by including Internet-based services within its scope. The consultation paper does not explicitly include either the reasoning or the indication for including substantive changes such as the expansion of definition of telecommunication services. Although the explanatory note mentions the "need for updating the nomenclature and definitions of relevant terms in the telecommunication legal framework" as a key theme emerging from the consultation responses, it is unfortunate to note that the responses received by Department of Telecommunication (DoT) were not made public. DoT, in compliance with the Pre-Legislative Consultation Policy, at the very least must release a summary of these submissions.

In response to an RTI application, DoT noted that roughly 500 pages worth of responses were submitted on a consultation paper titled 'Need for a new legal framework governing Telecommunication in India'.[31] However, none of these responses were made publicly available. Additionally, it is worth noting that the Telecom Bill was released just three weeks after the submission deadline for the consultation paper. Overall, the consultative process has not been in line with the

[30] Global Encryption Coalition https://www.globalencryption.org/events/ged/encryption-kept-me-safe/

[31] 'Response from Department of Telecommunications on RTI application DOTEL/R/T/22/00785', Internet Freedom Foundation, October 12, 2022. https://drive.google.com/file/d/1UiIz2ZF1AISZI1ItMUR6DH2BYJfKIw5J/view?usp=sharing.

stated ambitious goal of establishing a modern legal framework for the Indian telecommunications sector.

The definition of a telecommunication service should be limited in scope to the transmission of services between or among points using wire, radio, optical, visual, or other electro-magnetic means or systems.

Internet-based service applications and services that run on top of the Internet should not fall under this definition as these are agnostic to the telecommunication service medium being used. Such services are already covered under multiple legislations from the Ministry of Electronics and Information Technology (MeitY) and CERT-In. Regulatory overlap will only serve to create an uncertain environment for users and service providers alike.

Further, the Telecom Bill reserves a range of powers referred to throughout this document as an 'exclusive privilege' of the Union Government, therefore leading to a cementing of discretionary, arbitrary powers. The Bill essentially dilutes the regulatory powers that have so far resided with the Telecom Regulatory Authority of India (TRAI).

Currently the Union Government can seek the non-binding recommendation of the TRAI under Section 11(1) of the TRAI Act. The relevant section of the TRAI Act has been deleted via Clause 46(f) of the Telecom Bill. The Bill also grants the government absolute powers to issue licenses to telecommunication services. The requirement of minimum qualification of being appointed as TRAI chairman has also been diluted in the Bill. Collectively, it appears that there is active effort being made to limit the mandate of TRAI. Similarly, the wide grounds for exercising the powers to order interception of communications and Internet shutdowns are the sole prerogative of the Union and state governments without provisions for independent review or oversight.

With regard to Internet shutdowns, Clauses 24(2)(b) and 25(1)(f) of the Bill empower the Union and state governments to suspend Internet services. However, the lack of any independent review or oversight on these suspension powers raises serious concern. The Bill also fails to fix any of the concerns in the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 under Section 7 of the Indian Telegraph Act.[32] Further, the powers of the review committee under the Rules have also not been strengthened. Except for a single review committee, that comprises members of the Executive, there is no independent and impartial body or committee to check the justness of the shutdowns, creating a conflict of interest. Moreover, except for envisaging the powers

[32] Department of Telecommunications, Ministry of Communication, Government of India, 'Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017'. https://dot.gov.in/circulars/temporary-suspension-telecom-services-public-emergency-or-public-safety-rules-2017

to order shutdown, the Bill does not mention the procedure for lifting the blockade after any specific time.

The Telecom Bill is quite heavy-handed in its approach, and does not include specific, nuanced, and comprehensive limitations, checks and balances, reviews, or oversight mechanisms.

Privacy

Privacy on the Internet is the ability of individuals and groups to be able to understand and control what information about them is being collected and how, and to control how this is used and shared. Privacy often includes aspects of anonymity, removing linkages between data, devices, and communications sessions and the identities of the people to which they pertain.

Users choosing to rely on services offering e2ee expect their information and communications to be kept private and secure. As mentioned above, there are many reasons law-abiding citizens and businesses rely on privacy for personal security. The Telecom Bill must not weaken strong encryption, especially e2ee, limit its availability, or reduce its reliance and resilience. Any attempt to do so will result in self-censorship as users will be reticent in their communication for the fear of being watched. This also extends to fear of trade secrets, commercial and financial communication and privileged communication being surveilled.

Clause 4 asks for identification of the user availing the telecom service for the purpose of mitigating cyber fraud. However, mandating verification of users does not necessarily prevent virtual fraud. For example, in the Philippines, a new law requires phone users to submit personal identification before purchasing a SIM card.[33] Two weeks later, GCash, an e-wallet reported increased instances of SIM fraud though it is a digital platform. This was because users were selling their accounts (registered to their mobile number post presenting identification) to scammers or conducting scams themselves.[34] It has been observed that collecting personal data does not prevent frauds like SIM card swaps and virtual takeovers either.[35]

In another instance, nearly half of Australia's population (including visitors who obtained a SIM as a tourist), had their personal information breached. The breach took place when the country's second

[33] 'Marcos signs SIM registration law' CNN Philippines, October 10, 2022. https://www.cnnphilippines.com/news/2022/10/10/Marcos-signs-SIM-Card-Registration-Act.html

[34] 'GCash says users selling SIM with verified account to scammers may face jail time' ABS CBN News, October 25, 2022. https://news.abs-cbn.com/business/10/25/22/gcash-users-selling-accounts-may-face-jail-time

[35] 'What is SIM swapping? SIM swap fraud explained and how to help protect yourself', Norton, August 15, 2022. https://us.norton.com/blog/mobile/sim-swap-fraud#

largest telecom operator, Optus, had their KYC data leaked. It has since become a major issue as identity theft was rife within days.[36]

According to Clause 4(7) of the Bill, VPN providers must collect user data via mandatory KYC. VPN providers and zero-knowledge systems do not collect additional user data by design and should not have to collect data that is not relevant to their operations only to comply with the Telecom Bill, just as private spaces cannot be mandated to carry out surveillance to aid law enforcement purposes. It further creates a situation where data that could not be breached before now must be collected and protected against breaches and rogue uses of such data. The provisions on mandatory KYC are higher risk as India does not have a data privacy or a data protection law. Therefore, citizens in the country do not have the surety that their data will be safeguarded against overuse, abuse, profiling, or surveillance. This restriction on use of VPN technology has severe business implications on VPN providers as well as corporate and individual users. Notably, neither the mandate for KYC nor that of interception fulfil the triple test of legality, necessity and proportionality as envisaged in the Puttaswamy judgement and are thus unreasonable restriction on users' fundamental right to privacy.[37]

Internet service providers have been known to collect and share user data beyond need or purpose for further improving their advertisement targeting services or for other business purposes such as selling user data to third party advertising entities.[38] This, coupled with the continued absence of a comprehensive data protection framework in the country, puts users at great risk - and the Telecom Bill does little to protect users from such practices.

Concerns around data localization requirements also arise as a result of the move towards licensing Internet-based services. The government may now ask these services to store data, including personal and sensitive information such as private conversations, locally. Such a licensing requirement would confer excessive discretion to the government, and adversely affect individual privacy by potentially giving the government and law enforcement agencies greater access to user data.

Recommendations

- Withdraw the Telecom Bill, 2022, and start the consultation process afresh, in compliance with the Pre-Legislative Consultation Policy. The DoT should publish a paper with justifications and reasoning for introducing any changes, and set up an institutionalized

[36] Turnbull, T. 'Optus: How a Massive Data Breach Has Exposed Australia', BBC, September 29, 2022. https://www.bbc.com/news/world-australia-63056838

[37] K.S. Puttaswamy and Anr. vs. Union of India (2017) 10 SCC 1.

[38] 'A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers', Federal Trade Commission. October 21, 2021. https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf

system of broad, multi-city, in-person stakeholder consultation. We also urge the Union Government to appoint a Law Commission and/or an independent Standing Committee or expert body to look into reforms for the telecommunications sector.

- Narrow the scope of overbroad definitions like 'telecommunication service' to only include businesses and entities that use spectrum for their operations. Exclude Internet-based services and applications from the ambit of a 'telecommunication service'. Withdraw the licensing requirement for Internet-based service providers, applications, and platforms. The requirement frustrates the permissionless model of the Internet and raises entry barriers, especially when such entities are already complying with the provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

- Withdraw KYC requirements, as it will lead to digital exclusion of underprivileged sections of society and raise privacy and safety concerns for users. Anonymity is crucial for many Internet users, especially journalists, women, activists, whistleblowers, members of LGBTQ+ community and other marginalized groups. The KYC requirements will have deleterious impact on their privacy, safety, and security offline.

- Withdraw the mandate for interception of messages envisaged in Clause 24(2)(a) of the Bill. The provision also fails to appreciate the technical architecture of e2ee messaging platforms. To mandate interception powers in an e2ee platform is equivalent to outlawing strong encryption in India, a technology which is crucial for user safety and national security. This provision would also not hold up against the Puttaswamy judgement[39] nor stand the test of proportionality.

- Remove the provision granting the government authority to order an Internet shutdown. The Internet must remain on and strong, no matter what. If this is simply not possible, amend the provisions for Internet shutdown to include checks and balances. This includes removing the grounds of expedience, and instilling principles of due process of law, proportionality, and necessity. Reforming the provisions of the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 by diversifying the membership of the Review Committee and institutionalizing parliamentary or judicial oversight would go a long way in establishing a resilient telecommunications architecture in India and foster the growth of the Indian digital economy.

[39] K.S. Puttaswamy and Anr. vs. Union of India (2017) 10 SCC 1.