October 30, 2022

To:

Mr Naveen Kumar
Hon'ble Joint Secretary, Telecom,
Government of India
naveen.kumar71@gov.in

Submission to the Ministry of Communications, Department of Telecommunications, on the Draft Indian Telecommunication Bill, 2022

We thank the Ministry of Communications (MoC) for the opportunity to submit comments on the Draft Indian Telecommunication Bill, 2022.

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.

Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations.[1]

Access Now has consistently engaged with multiple stakeholders around the world, including governments and regulatory authorities, and in India, on matters pertaining to digital rights, including intermediary liability, content governance, cybersecurity, data protection, internet

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.

shutdowns, surveillance and digital security. We write to you to provide our comments based on our expertise working on digital rights in various regions across the world, including the Asia Pacific.

Submissions on the Draft Indian Telecommunication Bill, 2022

At the outset, we acknowledge the need for legislation/s governing telecommunications to evolve, in keeping with changing technologies, and continuing development of a nuanced understanding of their impact on individuals' rights and freedoms, economy, and democracy. However, we humbly submit that the Draft Indian Telecommunication Bill, 2022 ("Draft Bill") will adversely impact each of these, and must be withdrawn. A new bill should be prepared, with meaningful, in-depth and sustained stakeholder consultation. The country has long been in need of a legal framework that strengthens human rights in the digital age, including drastic and meaningful surveillance reform. The Draft Bill, however, aggravates the issues with India's surveillance regime, instead of paving the way towards reforms.

As the world's largest democracy, with the second largest internet user base, and a notable market for innovation, India has a unique opportunity to be a global leader, and devise an exemplary legislative framework for telecommunications in a manner that strengthens access, connectivity, privacy, security, and free expression.

In addition to the comments in our present submission, we also submit as attachments to this document (a) a copy of the "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" as Annexure I[2]; and (b) a copy of Access Now's "Policy Brief: 10 facts to counter encryption myths" as Annexure II[3]. We request that these documents may please be perused as forming part of our substantive feedback on the creation of a rights-respecting data protection framework.

Our initial comments and recommendations, in anticipation of further opportunities to engage, on certain specific provisions and issues within the Bill are below.

---

[2] Access Now, *Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance*, https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf

[3] Access Now, *Policy Brief: 10 facts to counter encryption myths*, https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf

October 30, 2022

Communications surveillance: Safeguards must be embedded to protect fundamental rights

The current framework governing communications surveillance in India, including the Indian Telegraph Act, 1885, is archaic and derives much of its context from the repressive colonial regime prevalent at that time. Therefore, it is imperative to replace this framework with one that is in keeping with the changing context, technological advances, rights jurisprudence and democratic principles. We humbly submit that the Bill fails to take this opportunity and achieve this goal.

The Bill perpetuates the rights violations and concerns arising from unrestricted, centralised and opaque surveillance powers granted to the government, including through Chapter 6, and Clauses 24 and 25 in particular. The government is conferred with excessive and arbitrary powers to intercept, access and retain communications content, and issue directions to telecommunication service providers in this regard, on overbroad grounds including sovereignty, security and integrity of the country, and public order. This is without clear restrictions on application on the grounds of necessity and proportionality, and adequate safeguards to prevent potential rights violations. As has been contended by civil society, privacy advocates, human rights defenders and others, and observed by the Indian Supreme Court, national security cannot be invoked as a blanket shield against accountability.

The Bill is devoid of any meaningful safeguards, limitations, checks and balances, including in the form of independent and judicial oversight to prevent the arbitrary use or misuse of surveillance powers in violation of people's rights. Further, no robust mechanism has been established for transparency and reporting of use of surveillance measures, notification requirements to those who have been affected, avenues for independent scrutiny and review, and remedy and redress for affected individuals.

In order to protect freedom of expression, the right to privacy, and other fundamental human rights in the current digital context, surveillance frameworks ought to be shaped by the principles of necessity and proportionality, which have been recognised in international human rights law, as well as the Indian Supreme Court.[4]

Our annexed Implementation Guide for the Necessary and Proportionate Principles provides a detailed, step-by-step guide focusing on a four-part process: the initiation of the

[4] Necessary and Proportionate Principles, https://necessaryandproportionate.org/principles/

surveillance request, the court order authorising such surveillance, the communication providers response, and the execution of the surveillance order. We note that additional context-specific steps and safeguards may be necessary to strengthen rights and freedoms, and reproduce the checklist version of this below for the benefit of the Department – please note that capitalised terms have been defined in the Implementation Guide:

I. **The Request**

- Based on publicly available, discernable law;
- Applicable to only a single Target;
- Narrowly tailored to minimize the impact on Protected Information;
- Written and signed by a Government Agent and Approved by an independent and competent Judicial Authority, who evaluates the Request based on both the content and the sufficiency;
- Describes the Account, Device, or Repository subject to Communications Surveillance, the Necessary Information sought, any Protected Information that may be incidentally accessed, the methodology to be used, and the specific timetable for the Communications Surveillance;
- Establishes that the Necessary Information sought is contained in the Account, Device, or Repository identified for Communications Surveillance;
- Demonstrates a sufficient nexus between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information sought;
- Where emergency procedures are used, a formal application is filed within 24-72 hours after the initiation of the Search.

II. The Court Order

- Issued and signed by an impartial, competent, and independent Judicial Authority;
- Pursuant to public and transparent proceedings;
- Based on credible, lawfully acquired information;
- In writing, identifying all underlying legal authorities and with the Request attached;
- Describes the full scope of the authorization, including the Accounts, Devices, or Repositories to be subject to Communications Surveillance, as well as the scope, timeline, and methodology for the Communications Surveillance;
- Narrowed to ensure minimal incidental access to Protected Information;

• Limits the retention time for all Protected Information to a reasonable time, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance;
• Includes a written opinion explaining the issues and the rationale for the decision in all cases of novel or unique factual or legal issues;
• Requires reporting on all Protected Information acquired during the Search, including collection, access, retention, and eventual destruction; and
• In the case of emergency procedures, limits the authorization to the time reasonably necessary for the Government Agent to complete a proper Request.

III. The Provider's Response

• Responds only to Requests in writing and including the identify of the Government Agent making the Request as well as a clear description of the scope, duration, and methodology of the Communications Surveillance to be conducted;
• Formally challenges all Requests outside the scope of domestic or international laws that should be formally challenged;
• Unless legally prohibited from doing so, requires notification to the user of the Request;
• Limits the Search precisely to the bounds of the Request and provides no more information than the most narrow construction requires; and
• Provides regular transparency reports to document all Requests.

IV. Execution of the Court Order

• Notifies the Target of the Court Order and provides an adequate opportunity to challenge the validity of the Search unless there is a demonstration that a delay is necessary;
• Regularly reports back to the Judicial Authority all of the Protected Information acquired during the Search;
• Segregates relevant information, promptly discards irrelevant information, and destroys evidence at the conclusion of the case or when it is no longer required;
• Respects Formal International Channels for any Request to or from an international jurisdiction;
• Prevents the use of any Protected Information that was not legally obtained from being used in any judicial proceeding or as the basis for further investigations;
• Reimburses all costs to Providers within a reasonable time; and
• Compiled within regularly published transparency reports on the usage of

October 30, 2022

Communications Surveillance authorities and practices.

With respect to safeguards and oversight, we share the following overarching and non-exhaustive list of recommendations that must inform changes to the surveillance regime in India, including any framework governing telecommunications, in a human rights-centric manner:

- Require oversight and approval of all surveillance requests by an independent judicial authority;
- Impose strict limitations on the scope, duration and form of authorised surveillance, and storage, retention and disclosure of data between authorities;
- Impose strict notification requirements for affected individuals;
- Implement a robust redressal and remedy mechanism to enable individuals to enforce their rights;
- Impose reporting and record-keeping requirements, to enable periodic review and independent scrutiny, for all agencies conferred with surveillance powers;
- Limit ability to invoke the authorities on behalf of foreign governments;
- Substantially limit the surveillance regime's overall potential to be used in harmful and dangerous ways by limiting the justifications and objectives for its use;
- Prohibit any requirement to enable access to data that would undermine privacy and cybersecurity, including backdoors to encrypted channels;
- Other amendments necessary in order to ensure protection of human rights.

Access Now recommends that safeguards and oversight mechanisms be implemented in recognition of the four-part process outlined above, in accordance with the Necessity and Proportionality Principles, and in alignment with the Supreme Court's jurisprudence on the right to privacy as well as international human rights principles. The goal of a surveillance regime in a democratic and digital society should be to strengthen fundamental human rights.

Encryption is crucial for human rights, the economy and national security, and must be protected

In addition to conferring unrestricted powers of communications surveillance on the

government as submitted above, Clause 24 of the Draft Bill threatens end-to-end encryption ("E2EE"), which is a crucial tool for online privacy and security, and protects free expression.

Clause 24(2)(a) in the Bill authorises the government to "direct that any message or class of messages, to or from any person or class of persons, or relating to any particular subject, brought for transmission by, or transmitted or received by any telecommunication services or telecommunication network, shall not be transmitted, or shall be intercepted or detained or disclosed to the officer mentioned in such order. This provision authorising sweeping surveillance, fails to carve out an exemption for E2EE services, and could easily be misused to break the security offered by E2EE services.

Content on E2EE on platforms cannot be accessed by anyone other than the sender and intended recipient/s, not even the service provider. If service providers of E2EE channels are compelled to comply with this clause, it will be an effective ban on E2EE services. This will inevitably have a debilitating effect on the right to privacy, freedom of expression and online safety. It must be noted that even if the clause is not invoked in context of E2EE services, but retained in its current form, its mere existence, and the uncertainty it engenders, will still result in a negative effect on rights and freedoms, and weaker cybersecurity infrastructure as service providers.

Encryption is inalienable in a democratic and digital society that seeks to meaningfully bolster human rights, the economy and national security. It protects fundamental rights and helps people stay safe online – particularly vulnerable groups, such as journalists, activists, members of the LGBTQ+ community, and dissidents. As encryption facilitates data security, many rely on this tool to perform their daily duties, such as medical and legal professionals, and obtain essential services, including healthcare and education – particularly since the drastic shift to online spaces during and after the pandemic.

Encryption is a critical component of a country's resilient cybersecurity infrastructure. Weakening it in any manner, whether direct or indirect, would result in the degradation of cybersecurity more broadly, and jeopardise national security. Once a vulnerability, or workaround, is introduced within an E2EE system, it can easily be misused by malicious state and non-state actors.

Technological innovations, including security measures such as encryption amid rapidly evolving technological and digital landscapes, and increasing online presence – for

communication, digital payments, information exchange etc. – in India and around the world, are integral to the growth of the economy. Legislative frameworks with the scope of adversely impacting encryption have been proven to have a negative impact on the economy. They stifle innovation, and place tech developers at a disadvantage in respect of the domestic market. For instance, an Australian legislation authorising law enforcement access to compel decryption and access communication is known to have had a noticeable detrimental impact on the market.[5]

Additionally, we are also concerned by Clause 25, which grants extremely broad discretionary powers to the government. The government is authorised to issue directions on standards to be adopted by licensees, registered entities or assignees. The clause lacks any explanation or limitation as to the precise subject matter, and scope and effect of such standards. Clear limitations and prohibitions must be incorporated in order to ensure that the standards do not have the effect, whether direct or indirect, of weakening or circumventing security tools such as encryption.

We strongly believe that measures to explicitly protect and strengthen encryption, and other security features, are essential to achieve the government's goal of creating a open, safe, trusted and accountable internet, and will also serve as a strong pillar on which a meaningful "Digital India" as envisioned by the government, and in a way that benefits people's rights, freedoms and ambitions, can be built.

Access Now recommends that any language that would have the effect of weakening, circumventing, or breaking encryption should be eliminated, and provisions must be incorporated to protect and strengthen this privacy and security enhancing tool.

Suspension or limitation of telecommunication services/internet shutdowns have a profoundly negative impact on rights and the economy

In 2016, the United Nations recognised access to the internet as a basic human right.[6] The Indian Supreme Court, in 2019, has also highlighted the importance of internet access for the fundamental rights protected by the Indian Constitution in *Anuradha Bhasin v. Union of India*.

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

[6] Brookings, *The internet as a human right*, https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/

Even the Parliamentary Standing Committee on Information Technology published a report in December 2021, noting the misuse of internet shutdowns, and the impact on people's rights and freedoms, with a list of recommendations for the government.[7]

However, in solidifying the government's powers to suspend or limit telecommunication services, and impose internet shutdowns, the Bill disregards the express guidance from the Supreme Court and the parliament, the Indian Constitution, and international human rights frameworks, authorities in India continue to impose internet shutdowns in violation of people's rights. Clauses 24 and 25 of the Bill empower the government to suspend communications, issue directions on a broad range of matters, including the use of telecommunication services, network and equipment. These provisions are devoid of any meaningful safeguards and limitations to ensure transparency and accountability, and will only serve to perpetuate the ongoing injustices stemming from the rampant imposition of shutdowns across the country.

In 2021, Access Now and the #KeepItOn coalition documented at least 106 shutdowns in India[8], and as of October 11, 2022, SFLC.in's internet shutdowns tracker has already identified at least 67 shutdowns in the country[9]. Hundreds of shutdown orders have been issued on the grounds of public safety and security in Jammu & Kashmir. Authorities continue to impose shutdowns in various states, including Rajasthan, Assam, West Bengal, Uttar Pradesh and Haryana, under orders that are either not made public, or carry vague, unjustifiable grounds such as prevention of cheating in exams, and containing protests.

Internet shutdowns also carry immense economic costs.[10] As the Indian Council for Research on International Economic Research noted in April 2018, frequent internet shutdowns are detrimental to sectors primarily dependent on digital technologies such as e-commerce, IT services, tourism; and also to healthcare and education.[11] As per Brookings, between July

---

[7] Standing Committee on Information Technology, *Suspension of Telecom Services/Internet and its Impact*, https://www.medianama.com/wp-content/uploads/2021/12/17_Communications_and_Information_Technology_26.pdf

[8] Access Now, *The Return of Digital Authoritarianism: Internet Shutdowns in 2021*, from https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf

[9] SFLC.in, *Internet Shutdowns Tracker*, https://internetshutdowns.in/

[10] Rest of World, *"As important as water is to life": How internet blackouts stifled Kashmir's digital economy*, https://restofworld.org/2022/blackouts-kashmir-digital-economy/

[11] Indian Council for Research on International Economic Relations, *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India*, https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf

2015 and June 2016, 1,692 hours of internet shutdowns in India cost the economy US$968 million.[12] This amount has already increased substantially. In 2020, Top 10 VPN reported in 2020 that internet shutdowns for 8,927 hours in India cost the country over US$ 2.8 billion (Rs. 20,973 crore). The average cost of an internet shutdown in India in 2020, was therefore over Rs 2.34 crore per hour.[13]

It must be noted that while the costs, both human and economic, of internet shutdowns are well documented, the benefits remain hypothetical, and there is no research to support claims that internet shutdowns help maintain public order.

The need of the hour is to ensure transparency and accountability from the government, prevent the misuse of shutdown orders, and uphold human rights – including freedom of expression, access to information, and freedom of peaceful assembly – and recognise, and therefore prevent, the economic costs. However, the Bill, in its current form, will have the opposite effect.

Access Now recommends that legislative frameworks reflect that internet access is crucial to protecting and strengthening fundamental rights, and bolstering the economy, in the digital age. Accountability and transparency measures must be embedded to ensure the prevention of misuse and abuse of internet shutdowns. Additionally, a robust mechanism must be established to ensure avenues for enforcement of rights and remedies.

Excessive government control, through "exclusive privilege" and licensing requirements, has an adverse impact on rights, democracy and innovation

The breadth of the proposed law, and the extent of government control it would enable, is deeply problematic. For instance, the broad definitions of "telecommunication" and "telecommunication services" in the Bill are effectively all-encompassing. The Bill in effect clubs together a swathe of different services, including various layers of the internet stack, with varying objectives and underlying technical capabilities, and seeks to govern them all in the same manner. This will prove to be regulatorily uncertain, ineffective, cumbersome; and is inconsistent with the need for nuanced analysis and rulemaking today. Further, allowing

[12] Center for Technology Innovation at Brookings, *Internet shutdowns cost countries $2.4 billion last year,* https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf
[13] The Indian Express, *Decoding India's dubious distinction as world's 'internet shutdown capital'*, https://indianexpress.com/article/technology/tech-news-technology/india-ranks-highest-in-internet-suspensions-7654773/

effectively unrestricted government control on all these services will inevitably hurt human rights and the economy.

Clause 3 of the Bill states that the Central Government shall have exclusive privilege to provide telecommunication services; establish, operate, maintain and expand telecommunication network and telecommunication infrastructure; and use, allocate, and assign spectrum. Further, the clause empowers the government to exercise its privilege through licensing, registration, authorisation and assignment pertaining to telecommunication services, network, infrastructure, and equipment. This clause enables regulatory overreach, and its problematic nature of this provision is exacerbated by the fact that there is no explanation or limitation as to the grounds on which the government would make assessments on these matters, or any safeguards to prevent or challenge arbitrary decisions. Additionally, it must be noted that regulatory uncertainty, and excessive licensing and compliance burdens are ultimately detrimental to the end users as they result in a lack of choice in the market, and the compliance costs are eventually passed on by the service providers to the consumers.

The internet has served as a democratising tool – making it possible for more people to broadcast, share, and access information; to use it as a platform to exercise their fundamental rights, including the rights to freedom of expression and privacy; and to avail essential services. OTT platforms facilitating news exchange, communication, and entertainment, have become a vital component of a free and open internet. This has, for instance, facilitated the growth of digital news media and journalism in a manner that encourages free expression, and the development of a more diverse news ecosystem; and encrypted communication channels that are relied on for private and secure communications.

Further, it has also opened up the market to newer and smaller players, fuelling competition, innovation and the economy. The cumbersome, all-encompassing, and uncertain licensing requirements will be a deterrent for new entrants, negatively impact investments and deprive the market and the people of diverse services, innovations and competition.

In broadening the definition of telecommunication services such that a vast majority of services and platforms on the internet, if not all, are subject to the “exclusive privilege” of the government and cannot operate, except with the government’s permission, and in terms of standards prescribed by the government, the Bill threatens the existence of the internet as we know it, jeopardises people’s rights and freedoms, undermines democracy and stifles

innovation.

Such extensive government control, and licensing requirements, are incompatible with a democratic society, and a free, open and secure internet. They also stand in stark contrast with international human rights principles and global best practices.

Access Now recommends that the exclusive privilege and excessive powers granted to the government, including through licensing requirements, be strictly limited, in recognition of the impact on human rights; the free, open, and secure nature of the internet; democracy; and the economy.

Need for limitations on personal data collection, including identification proof

Under the Draft Bill, license holders have an obligation to identify the users of its service through a verifiable mode of identification. As set out above, given the sweeping scope of the Draft Bill, license holders would include nearly each and every provider that utilises the internet to provide a service.

This would enable an appalling number of service providers, including private sector entities, to gather an enormous amount of personal data. This would be inconsistent with the internationally recognised principles and best practices pertaining to data governance, including necessity, proportionality, and data minimisation, and would jeopardise people's rights. Further, it would place hurdles to access of services. For instance, people should not be required to submit identification proof, containing personal information, to use communications platforms.

Such an obligation also runs contrary to efforts, including by the government, to hold companies' accountable, and the goal of curbing surveillance by the private sector. The country lacks robust data protection legislation, and the amplification of data collection mandates and opportunities under the Bill will further exacerbate the risks to people's right to privacy and other fundamental rights.

Further, submission of identification proof must by no means be a prerequisite for accessing online services – especially communication platforms. This would severely undermine privacy and anonymity, which are inalienable features of a free, open, safe and trustworthy internet,

and integral to the protection of human rights in the digital age.[14]

Access Now recommends that the government must restrict, and not enhance, mandates and opportunities for personal data collection that are not in alignment with strict principles of necessity, proportionality, data minimisation and purpose limitation, as they violate people's rights. The risks to people's rights that such obligations pose are exponentially exacerbated by the absence of a robust data protection framework in the country. Submission of identification proof must not be made necessary for accessing online services as privacy and anonymity are key components of a safe internet that protects fundamental rights.

Need for clarity, clear definitions and narrowing down of scope

An issue that runs through many provisions in the Bill is the absence of safeguards, lack of clarity and clear demarcation of scope in a narrowly defined manner.

For instance, Clauses 25 and 26 authorise the government to prescribe standards and issue directions on a broad, all-inclusive, range of issues pertaining to telecommunication services, network, and equipment, on vague grounds such as "national security" and "public interest". Such sweeping powers, without clear definitions, narrow scopes, limitations and safeguards, will result in arbitrary decisions and violation of rights.

The Bill also fails to place limitations on data access and retention, including on the type and scope of data that may be accessed, the duration for which it may be retained, how and by whom it may be accessed, the manner in which it may be stored and kept secure, and the conditions under which it may be disclosed. Additionally, it does not provide safeguards for protection of personal and sensitive data amid investigations.

Particularly in the absence of a data protection legislation, it is crucial for any proposed law providing for data collection, access, retention, and storage, to prescribe limitations and safeguards that prioritise people's privacy and security, and consequently protect fundamental rights.

On a macro level, the Bill also contributes to a lack of clarity on how the overall ecosystem will

[14] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

function with several potential overlaps between different existing and upcoming legislations and regulators, such as the imminent data protection bill, the IT Rules of 2021, and the upcoming Digital India Act.

Access Now recommends the incorporation of clear definitions that effectively narrow down the application of each provision, and safeguards that protect fundamental rights at each stage of communication surveillance, particularly in context of the absence of a data protection legislation in India. Further, for regulatory certainty and clarity on the enforcement of rights, there needs to be clarity on how the various existing and upcoming frameworks governing data and internet and telecommunication service providers, as well as the various regulatory authorities involved, will interact.

October 30, 2022

In conclusion

We thank the DoT for initiating this important process of replacing the archaic framework governing telecommunications in India, and are grateful for the opportunity to provide inputs to the Draft Bill. We request to be included in any further meetings and stakeholder interactions that the Department may organise as part of its next steps in this process. We hope that the DoT will initiate a process of sustained, in-depth consultation with all stakeholders, including civil society and subject matter experts, to formulate a new draft that is in keeping with the goal of strengthening rights, democracy and innovation.

We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | **https://www.accessnow.org**