From: biyani@isoc.org
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: hall@isoc.org, frautschy@isoc.org, singh@isoc.org
Sent: Thursday, August 17, 2023 3:13:09 PM
Subject: Internet Society comments on TRAI consultation: Regulatory Mechanism for OTT Communication Services & Selective Banning of OTT Services

To,

Shri Akhilesh Kumar Trivedi
Advisor (Networks, Spectrum and Licensing)
Telecom Regulatory Authority of India (TRAI)
Government of India
New Delhi

Sir,

At the outset, please allow me to introduce myself, I'm Neeti Biyani and I am Senior Advisor, Policy and Advocacy with the Internet Society, a global nonprofit organization that works to ensure the Internet remains a force for good for everyone: open, globally connected, secure, and trustworthy.

In response to the TRAI Consultation Paper on '**Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services**', please find the Internet Society's comments in the attached.

I want to thank TRAI for hosting this consultation and giving relevant stakeholders a chance to engage with this process.

I hope our suggestions help in our collective endeavour to strengthen the national economy, and uphold the open, global Internet.

Please reach out to me via email at biyani@isoc.org if I can provide any further information, or if we can be of further assistance.

Thank you,
Neeti Biyani

Neeti Biyani
Senior Advisor, Policy and Advocacy
New Delhi, India
biyani@isoc.org

Internet Society

internetsociety.org

17 August 2023

Internet Society's comments on the TRAI Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Q1: What should be the definition of over-the-top (OTT) services? Kindly provide a detailed response with justification.

The term 'over-the-top' or OTT is a misnomer. The term 'over-the-top' originally comes from the telecommunications industry, where it was used to describe the routing of voice calls over the traditional telephone network, bypassing the conventional telephone company's voice call infrastructure. In this context, the term made sense as the calls were 'over-the-top' of the existing telephone network.

However, when the term is intended to refer to Internet-based services, ***it is irrelevant***. Content delivered over the Internet is not literally passing 'over-the-top' of any existing infrastructure. Instead, it is being transmitted through the same networks and data channels that are used for various Internet services. The delivery of content and services through the Internet has become a standard practice, making the term 'over-the-top' irrelevant. This also includes the telecom companies own voice call system which today runs on an IP (Internet Protocol) core.

The term 'over-the-top' also begs the question—over the top of what? Telecom companies are service providers of and gatekeepers to the Internet's infrastructure, but they don't have sole proprietorship over the Internet. ***The Internet is a network of networks***, composed of about 75,000 voluntary networks that choose to connect with one another. Open standards are what enable this network of Internet networks to communicate. And they're what make it possible for anyone to create content, offer services, and sell products without requiring permission from a central authority. The Internet is not like a telephone network. Part of the overwhelming utility of the Internet is in how it differs from telephone networks: designed to be general purpose with low barriers to entry, ***not single purpose with gatekeepers who decide what services can best meet the needs of the people***.

In this sense, ***the Internet belongs to no one—and it belongs to everyone***.

The appropriate term to use in this context would be ***Internet-based services***.

Q2: What could be the reasonable classification of OTT services based on an intelligible differentia? Please provide a list of the categories of OTT services based on such classification. Kindly provide a detailed response with justification.

While the Department of Telecom regulates the telecommunications sector, the Ministry of Electronics and IT and the Ministry of Information and Broadcasting govern Internet-based services. The IT Act, 2000 already creates categories of Internet-based services: including social media and significant social media intermediaries based on user threshold; and social media and gaming intermediaries on the basis of functionality. In fact, this consultation too, begins with the assumption that "OTT communication services" form a category of Internet-based services, before stakeholders have had a chance to respond to the consultation paper.

There is already a ***pre-existing, clear, and indeed intelligible differentia between the telecom and Internet ecosystems***—justified by their separate regulation by different ministries. This not only makes it an ***unnecessary exercise for TRAI to undertake***, but indeed risks regulatory disharmony. Such a bifurcation must continue, as any attempt to regulate or govern Internet-based services as a telecom service would be a colorable exercise of power, i.e. under the doctrine of colorable legislation in the country, TRAI transgressing its powers and indirectly attempting to do something that it could not have done directly.

Q3: What should be the definition of OTT communication services? Please provide a list of features which may comprehensively characterize OTT communication services. Kindly provide a detailed response with justification.

As highlighted in our response to Question 2, Internet-based services are already regulated under the IT Act, 2000 by Ministry of Electronics and IT. This includes those providing communication services. Any attempt by TRAI towards defining and then regulating them as telecom services is unnecessary, risks regulatory disharmony, and would be a colorable exercise of power.

Q4: What could be the reasonable classification of OTT communication services based on an intelligible differentia? Please provide a list of the categories of OTT communication services based on such classification. Kindly provide a detailed response with justification.

As highlighted in our response to Question 2, there is already a pre-existing, clear, and indeed intelligible differentia between the telecom and Internet ecosystems—justified by their separate regulation by different ministries. Any attempt by TRAI towards classifying such Internet-based services and then regulating them as telecom services is unnecessary, risks regulatory disharmony, and would be a colorable exercise of power.

Q5. Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:

(a) regulatory aspects
(b) economic aspects
(c) security aspects
(d) privacy aspects
(e) safety aspects
(f) quality of service aspects
(g) consumer grievance redressal aspects
(h) any other aspects (please specify).

Kindly provide a detailed response with justification.

(a) **Regulatory aspects**: Internet-based services are regulated under the Information Technology Act 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the CERT-In Cybersecurity Directions 2022, and will continue to be regulated under the forthcoming Digital India Bill.

The concern that Internet-based services are not regulated is unfounded, and indeed incorrect.

Given the ***inherently different nature of service*** between telecom service providers and Internet-based services, it is imperative that they are treated as two distinct groups of entities and regulated accordingly. More comments on the 'same service, same rules' argument are in the following response to Question 7.

(c) **Security aspects** and (d) **Privacy aspects**: Please see our response to 'Lawful interception of messages and Privacy and security' as part of Question 7.

(e) **Safety aspects**: Billions of people around the world use encrypted services to protect their privacy and data when communicating with others. However, the concerns of law enforcement agencies regained prominence in the last decade. Such positions tend to focus encryption policy on law enforcement and intelligence agencies' claims that they need to be able to access encrypted communications. But encryption is not just a law enforcement issue. The availability of secure encrypted communication services is central to privacy, free expression, and the security of today's online commerce and financial services.

Q6. Whether there is a need to bring OTT communication services under any licensing/regulatory framework to promote a competitive landscape for the benefit of consumers and service innovation? Kindly provide a detailed response with justification.

The Internet Society continues to maintain its position that there is *no need for a licensing framework for Internet-based services*, including modern communication services.

Any licensing framework for Internet-based services will do the exact opposite by harming the thriving digital environment in the country, *impacting the national economy*, stifling innovation and growth, and raising significant barriers to entry—especially for homegrown start-ups and apps.

Such a requirement will 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 this requirement will risk large-scale harm to this sector. The consequences of requiring Internet-based services to engage in licensing will disproportionately impact smaller, cash-strapped platforms and start-ups which would need to spend crucial resources in complying with this requirement.

This lays an extremely heavy, onerous compliance burden on Internet-based 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. This will create an uncertain regulatory environment for Internet-based services, and will only stifle and inhibit innovation. While bigger players may have the resources to comply, any licensing requirement will impact national start-ups and smaller ventures.

Further, the International Telecommunication Union (ITU) encourages voluntary agreements between telecom service providers and Internet-based service providers to nurture commercial cooperation. Licensing requirements 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 Internet-based services is an unnecessary compliance requirement, thwarting easy and unrestricted access to an open Internet.

Q7. In case it is decided to bring OTT communication services under a licensing / regulatory framework, what licensing / regulatory framework(s) would be appropriate for the various classes of OTT communication services as envisaged in the question number 4 above? Specifically, what should be the provisions in the licensing / regulatory framework(s) for OTT Communication services in respect of the following aspects:

(a) lawful interception
(b) privacy and security
(c) emergency services
(d) unsolicited commercial communication
(e) customer verification
(f) quality of service
(g) consumer grievance redressal
(h) eligibility conditions
(i) financial conditions (such as application processing fee, entry fee, license fee, bank guarantees etc.
(j) any other aspects (please specify).

Kindly provide a detailed response in respect of each class of OTT communication services with justification.

As highlighted in our response to Question 6, there is *no need for a licensing framework for Internet-based services*.

This move towards regulating Internet-based services in a manner similar to telecom service providers has been a persistent demand by telecom companies. They argue that the lack of regulation of Internet-based services 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 is popularly known as 'same service, same rules'.

The 'same service, same rules' argument is flawed and misleading. This was also reaffirmed in a submission made by the Broadband India Forum (BIF) to TRAI in 2017. 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. Telecom services' own customers pay telecoms directly to access the Internet.

Internet-based services 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. This consultation paper, on page 12, highlights ***telecom companies' revenue from data usage has increased tenfold between June 2013 and December 2022***.

In fact, many Internet-based services make huge investments in networks and telecom infrastructure, such as data centers, content delivery networks, cache servers, undersea cables, etc. ***Between 2011 and 2021, Internet-based services invested $883 billion in digital infrastructure*** including hosting, transport, and delivery networks, leading to positive impacts on end users, and broader economic benefits.

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 traditional voice calls and text messaging services, and foster innovation along a number of axes that simply don't exist in specialized networks. Regulation of Internet-based services in a manner similar to telecom services would lead to significant curbs on innovation and the proliferation of new services, and would have a ***direct impact on pricing for consumers***.

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 privileges not 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. ***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 limited 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 services, would not only harm innovation, but also stifle the voices and labor of the already disadvantaged.

(a) **Lawful interception of messages** and (b) **Privacy and security**:

Lawful interception of messages on end-to-end encrypted (e2ee) communication services will compel messaging platforms to weaken security afforded to users by strong encryption and would be ***detrimental to the safety, security, privacy and livelihood of users, businesses and governments worldwide***. It would also result in severe financial losses 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—or indeed giving vast swaths of government officials keys to everyone's 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 that could be used for financial, emotional, or bodily harm.

E2ee communication 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. 'Lawful interception' of messages is not only impossible on e2ee platforms—we cannot create a backdoor that only lets "good guys" through—but is also 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 cease to offer e2ee entirely.

A complete withdrawal of e2ee communication platforms will not be a surprising move considering the withdrawal of several Virtual Private Networks (VPNs) from India following the onerous CERT-In Cybersecurity Directions released in 2022. 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.

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. 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.

Moreover, *criminals will just switch to using other non-compliant services or building their own services* from scratch, easily possible in this day and age given the relative commodification of encryption—for instance, building a working e2ee system is a typical task of early computer science students in secondary school and university.

Furthermore, compelling business communications platforms 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*.

Q8. Whether there is a need for a collaborative framework between OTT communication service providers and the licensed telecommunication service providers? If yes, what should be the provisions of such a collaborative framework? Kindly provide a detailed response with justification.

Telecommunication service providers and Internet-based services are *inter-dependent*. While telecom service providers enable users to access the Internet's infrastructure, Internet-based services drive demand for data, high-speed Internet, and more bandwidth. Thus, both groups of businesses *complement each other* in the digital economy — they need each other to continue to remain functional, viable, and profitable.

Neither can survive without the other any longer. *Mutual cooperation and complementarity* is necessary instead of competition and conflict. Further, *no mandatory collaborative framework* should be implemented between telecom operators and Internet-based services.

Q9. What could be the potential challenges arising out of the collaborative framework between OTT communication service providers and the licensed telecommunication service providers? How will it impact the aspects of net neutrality, consumer access and consumer choice etc.? What measures can be taken to address such challenges? Kindly provide a detailed response with justification.

A collaborative framework between telecommunication service providers and Internet-based services ***should not include a cost-share or sending party network pays model***, i.e. telecom operators should not compel Internet-based services to make mandatory payments in exchange for transmitting traffic requested from them.

The TRAI consultation paper of January 2023 [Regulating Converged Digital Technologies and Services: Enabling Convergence of Carriage of Broadcasting and Telecommunication Services] is of the position: "*The recent increase in OTT media consumption has challenged telecom service providers to support more content, more devices, and more users with limited infrastructure resources.*" (1.22)

This is not accurate. The Internet model of networking is agile, scalable, and has the potential to offer virtually infinite opportunities to users. Over the last three years of the Covid19 pandemic, the Internet was able to support many more users who were dependent on the Internet for more and more functions — all without any severe disruptions.

This assertion is based on a long standing demand by telecom operators to have Internet-based services share network expansion costs.

The following are ***some of the harms such a proposal can cause***:

- Increased costs for consumers: If telecom companies are allowed to charge Internet-based services for access to their networks, those costs may be passed on to consumers through higher prices for availing those Internet services. This could make Internet access less affordable for many users, hinder innovation, disrupt the model of networking that the Internet relies on, and disrupt the country's digital economy.
- Reduced innovation and competition: If smaller Internet services, including smaller Internet service providers, are unable to afford the fees charged by telecom companies, they may be forced out of the market, reducing innovation and competition in the industry. This could lead to fewer choices for consumers and less incentive for companies to invest in new technologies.
- Threats to Net Neutrality: If telecom companies are able to charge Internet-based services for access to their networks, they will give preferential treatment to certain services over others. This could threaten the principle of net neutrality, which holds that

all Internet traffic should be treated equally. *In 2017, TRAI itself recommended Net Neutrality principles,* including non-discriminatory access to content, application and services on the Internet.

- Limited access to information: If Internet-based services are forced to pay fees to telecom companies for access to their networks, this could result in some information and services being prioritized over others. This could limit access to important information and resources, particularly for those who cannot afford to pay for premium services.

Overall, the proposal to introduce new obligations to ensure payments from Internet-based services to telecom operators is in ***direct conflict with the model of networking the Internet depends on***. This model implies that a network that wants to get connected to the Internet has to make just one agreement with another network that has already achieved it. By this means, it will be automatically reachable by every Internet user in the world.

Changing this model by introducing ***obligations to negotiate one-by-one contracts*** (thus replicating the telephone way of networking) is a step backwards, will dramatically alter the fabric of the Internet and will cause an ***irreversible fragmentation or splintering of the Internet***. This is a real threat to the Internet and the success it has brought about in the country, and we urge you to guard against this.

Q10. What are the technical challenges in selective banning of specific OTT services and websites in specific regions of the country for a specific period? Please elaborate your response and suggest technical solutions to mitigate the challenges.

Because of how the Internet works, top-down interference with specific services and technologies on the Internet will *damage interoperation and tend to splinter the Internet into smaller, less-connected islands*.

National and regional bans can also have the ironic effect of *undermining security online for people*. The Internet is designed to be extremely flexible and provide multiple ways to achieve a goal. People who depend on a service may circumvent barriers to access that service, or worse, fall for scams that pretend to restore access. This can expose those and other people to fake sites and other sources of malware.

It is also important to recognize second order effects of such a move. More and more platforms depend on login and authentication provided by other services. Selective banning of certain Internet-based services would have a knock-on effect and impede the ability of people to use services that have not been restricted. Services deployed over the Internet are themselves a network of networked functionalities that could be damaged.

The impact goes beyond a country's borders. The more governments block or ban each other's online services, the more it fragments the Internet by making user experiences insular and inconsistent from country to country. The global economy will suffer, and many will be left without easy access to cross-border resources that are critical to their daily lives. Furthermore, people in one country or region can end up with less access to valuable information than is available elsewhere on the Internet, thereby exacerbating global inequity.

Policymakers may claim such actions to block or ban certain apps and services are necessary for maintenance of law and order or national security—when citizen use of some applications or services could lead to wide scale theft of personal data, exposure of national security assets, or creation of numerous in-country landing points for a widespread cybersecurity attack, among other risks.

The idea that these risks are somehow unique to a particular application or service is poorly founded: the same attacks could be as easily embedded in another permitted application. Since the Internet is such a flexible technology, any necessary defense of national security has to come from preventing the attacks no matter what. *Law and order and national security that supposedly come from banning a particular app or service is a security blanket made entirely of holes*.

The Government of India should avoid service or applications specific bans, which undermine security and access to opportunities. Instead of banning a particular platform or application based on non-technical criteria like country of origin or ownership, countries should be transparent about risks and raise the privacy and security standards for all online services to mitigate broader potential threats from end-user devices.

Q11. Whether there is a need to put in place a regulatory framework for selective banning of OTT services under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force? Please provide a detailed response with justification.

A selective banning of Internet-based services under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force, especially services named in the consultation paper—Facebook, WhatsApp, Telegram—is *not needed*.

Such a move is in fact harmful to people (especially women and marginalized people), society, and the national economy.

The investigation into the Internet shutdown in Manipur in effect since May 2023 shows that people rely on communication services deployed over the Internet to stay in touch with their family; access information, news, and healthcare services; report crime and abuse; and share personal details such as their geo-location in case they are in danger, and need assistance or protection.

Modern communication services deployed over the Internet are also used as marketplaces for small businesses and entrepreneurs. In fact, banning of services also presents a risk for businesses and investors, including those building infrastructure and developing services. Such a move sends the ***signal that a country's business environment is not resilient or reliable***, and that the country's government is willing and able to shut down operations arbitrarily. This economic uncertainty is cumulative, causing disincentives to invest in infrastructure and driving existing customers away to other, more stable business markets.

The Internet Society has developed a ***Pulse NetLoss calculator to estimate the economic impact of an Internet shutdown and app bans***.

The NetLoss calculator uses an economic framework to estimate the impact of Internet shutdowns and app bans on a range of economic, social, and other outcomes. It uses econometric tools to provide a rigorous and precise estimate of the economic impact of Internet shutdowns and app bans. The methodology relies on publicly available datasets, thus making the methodology reproducible as well as transparent.

Unlike other existing estimation tools, the NetLoss calculator also estimates the impact on unemployment and loss of foreign direct investment (FDI). The data used in the NetLoss calculator is refreshed quarterly as the primary data on economic indicators is used at an annual level. The source of the data is the World Bank's World Development Indicators, which typically corrects for minor statistical changes.

Additionally, there is little to no evidence to prove that Internet-based services are used primarily by terrorists, criminals, or miscreants. As the Internet and Internet-based services become more ubiquitous, people increasingly depend on them. Bans of Internet-based services can have a negative effect because these services and apps form an important part of people's lives. Some online services provide people with their income or networks of support. Others provide essential information for healthcare and education. Part of the safety and security of citizens is their freedom to interact with others in the ways they wish, and banning such applications inherently takes away that freedom.

Q12. In case it is decided to put in place a regulatory framework for selective banning of OTT services in the country -

(a) Which class(es) of OTT services should be covered under selective banning of OTT services? Please provide a detailed response with justification and illustrations.

(b) What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

There should be *no banning* of any Internet-based services. The Internet—and the services, apps, websites, and platforms deployed over it—should remain on and strong, no matter what.

If India is to achieve its ambition of *$1 trillion digital economy*, realize its dream of *Digital India*, and become a world leader in global supply chains, it must give up arbitrary bans of Internet-based services, disruptions to the Internet, and ensure that Internet access only increases for more and more people to get connected.

Q13. Whether there is a need to selectively ban specific websites apart from OTT services to meet the purposes? If yes, which class(es) of websites should be included for this purpose? Kindly provide a detailed response with justification.

No.

Q14. Are there any other relevant issues or suggestions related to regulatory mechanism for OTT communication services, and selective banning of OTT services? Please provide a detailed explanation and justification for any such concerns or suggestions.

N/A