SFLC.IN
2nd Floor, K9
Birbal Road, K-Block
Jangpura Extension, Delhi – 110014
https://sflc.in | mail@sflc.in | +91-11-43587126

Comments on the Regulation Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services.

Executive Summary

Currently, OTT Services are regulated under the Information Technology Act, 2000 and subsequent rules that have been notified, and the TSPs are governed by numerous laws such as the Indian Telegraph Act, 1885, the Wireless Telegraphy Act, 1933, and the Telecom Regulatory Authority of India Act, 1997. The TRAI, which has been releasing public consultation papers and requesting comments since 2015, does not regulate OTT Services in India. The rationale behind TRAI's role in drafting a regulation is on the basis that the services provided by TSPs and OTTs are quite similar i.e. communication in written or oral form, therefore they should be guided by similar rules.

By internationally recognised definition, OTT services are the services provided over the internet, as opposed to traditional telecommunication channels. However, there is one stark difference between both, the TSPs are licensed service providers and OTTs provide their services over already-accessed services of TSPs. Because of this, We believe that the services provided by TSPs and OTT platforms should be subject to different privacy and security standards. A large part of a sustainable digital economy is based on trust that essentially comes from privacy and encryption. SFLC.in believes that the goal has to be to revisit and review the surveillance and interception provisions to ensure the right to free speech and expression. If a country requires weakening of encryption or any form of backdoors, then the encryption and security products originating from or taking place in that country cannot be trusted for undertaking any task that involves personal data. We at SFLC oppose any kind of licensing that requires breaking encryption or provides sweeping power of interception to the government.

The TSP is an oligopoly, working on limited resources, i.e. spectrum and OTT is polygopily, which is using the services provided by the TSPs to flourish. It becomes evidently clear that TSPs are essential for the existence of OTT and there is no scope for competition between both. With the IT Act and subsequent rules already governing OTT Services, along with the incoming Data Protection Bill, 2023, the TRAI Regulations become an impediment to OTT Services. TRAI does not have the requisite power to regulate or make recommendations to the DoT regarding OTT service providers, their regulations, including Internet shutdowns, selective banning of OTT apps. Selective bans are to be under the purview of separate laws and under separate ministries such as MeitY and MIB. If an action is required which is beyond the scope of what is permissible under the IT Act, then a new law is needed for this purpose.

SFLC.IN
2nd Floor, K9
Birbal Road, K-Block
Jangpura Extension, Delhi – 110014
https://sflc.in | mail@sflc.in | +91-11-43587126

We at SFLC.in oppose any kind of internet bans, surveillance or interception measures on any OTT Platforms. The proposal for selectively banning OTTs is based on the premise that it is useful in controlling law and order problems. However, there is no evidence to support the claim that shutting down the internet or banning specific content is useful in controlling the situation during the unrest or any other meaningful progress thus far.

Part – A: Regulation of OTT Services

Definitions

The report delves into the definitional aspects of OTT services, OTT Communication Services and how they may be reasonably classified in the event that an entirely new regulatory framework is going to be made in India. At present these services are regulated under the Information Technology Act, 2000 and subsequent rules that have been notified. At this time, the TRAI, which has been releasing public consultation papers and requesting comments since 2015, does not regulate OTT services in India.

To define OTT services, the starting point is to note the essential distinction, i.e., that they are services provided over the internet, as opposed to traditional telecommunication channels. This has been the lens through which international organs have also defined this set of services, as highlighted in the report. The other characteristics have been factual- the lack of regulation/ licensing requirements to operate services, especially services such as voice/video communication and messaging. A broader definition may open up confusion with respect to applicability of any regulations that may be envisaged; characterising such services on the basis of absence of licensing regimes would not be an appropriate distinction any further. With respect to the classification of these services, the report has discussed classification of OTT services as a whole, as well as further classification of OTT Communication Services, which would presumably be a subset of the overarching OTT services category. To further categorise communication services, categorisation on the basis of the nature of these services would be beneficial, as long as there are additional regulatory obligations that may be necessitated on this basis. In the absence of such requirements, there may not be a need to include further

classifications of OTT services. The classification of services, therefore, whether OTT services or OTT communication services, should be based on whether there are requirements in a proposed regulatory framework that require distinctive approaches towards licensing based on sub-categorisation of these services.

TSPs and OTTs: Difference in Regulation

Telecommunication services and OTT communication services, while providing similar end services, differ starkly in most other ways. At present, TSPs are licensed service providers, while OTT service providers are not. This regime should continue, as explained in detail in the next answer. TSPs operate differently than OTT service providers economically as well. TSPs operate in an oligopoly, while OTT services are provided in a market full of competition, a polyopoly. The reason that the OTT ecosystem has flourished is that it is not bound by the same restrictions and limitations as the TSPs. On the other hand, OTT service providers cannot sell access. They can only make their services available to those that already have access to the Internet, which is provided only by TSPs. Thus, economically as well, TSPs and OTT platforms merit different treatment.

The services provided by TSPs and OTT platforms should be subjected to different privacy and security standards. The telecommunication interception law in India (Sections 5 and 26 of the Telegraph Act) is extremely outdated. The lawful interception requirements under the License Agreements were made with the same assumptions regarding privacy and security as were prevalent during the British rule. To subject OTT platforms to similar standards would be immensely detrimental. Instead of requiring backdoors, weakening of encryption or increased surveillance on OTT platforms, we need to revisit and review the surveillance and interception provisions under the Telegraph Act, the Rules framed thereunder and the lawful interception requirements under the Licence Agreements for compliance with the Right to Privacy as per the Supreme Court's judgement. Further, OTT platforms are subjected to surveillance under the Information Technology Act, 2000, and the Intermediary Guidelines, 2021, along with the Interception Rules, and the Blocking Rules, 2009.

We recommend against any surveillance or interception measures on any OTT platform.

OTT Service Providers and TSPs: Standards of Licensing

OTT Service Providers should not be subjected to a similar standard of licensing/framework as TSPs. OTT providers and TSPs that provide the same or similar services (written and oral communication) exist and operate in entirely different realms. While the objective achieved through the use of these two might be the same – communication in written or oral form – TSPs and OTT providers are not in direct competition with each other. One of them has an oligopoly over the use of a limited natural resource in the form of spectrum, while the other faces unlimited competition. TSPs and OTT services cannot be seen to be competing with each other and do not require to be brought to the same playing field under the same restrictions and regulations, as the domains in which they are operating are not the same. We must not forget that TSPs are the sole gatekeepers of the Internet, with an ability to charge appropriately for that privilege.

OTT service providers are already regulated under the Information Technology Act, 2000 along with the Rules laid down under the said Act. TRAI has no power to regulate OTT services. We already have a draft data protection law as well which will be tabled in Parliament in the Monsoon Session of 2023. Further, the IT Rules, 2021 also govern the ways in which OTT platforms can operate. There is no non-level playing field between TSPs and OTT service providers as the two are not playing in the same field. OTT service providers can never run a TSP out of business, as an OTT service cannot exist without a TSP. Unfair regulation of a TSP is a concern that needs to be examined separately.

At the outset, it is important to state that OTT Service Providers should not be subjected to a similar standard of licensing/framework as TSPs. TSPs and OTT services cannot be seen to be competing with each other and do not require to be brought to the same playing field under the same restrictions and regulations, as the domains in which they are operating are not the same. If OTT Communication platforms are required to impose any form of surveillance or interception, then the right to privacy and freedom of speech and expression along with the entire digital economy of the country would be at high risk. Encryption now forms the backbone of the digital economy. A large part of a sustainable digital economy is based on trust. If a country requires weakening of encryption or any form of backdoors, then the encryption and security products originating from or taking place in that country cannot be trusted for undertaking any task that involves personal data.

a) Lawful Interception obligations: Section 69 of the IT Act gives the power to the Government to intercept, monitor or decrypt any computer resource. This provision also lays down a penalty of imprisonment up to seven years for an intermediary who does not assist the Government in interception or monitoring. Further Section 69B of the IT Act also empowers the Government to monitor and collect traffic data or information through any computer resource for cyber security. Interception of messages is a power that has consequences for the privacy of users, and is a power that must be used exceedingly carefully., If further regulation of OTT platforms is to take place, it is important that it does not increase surveillance of users. Licensing should not require encryption to be broken, and should not grant sweeping powers of interception to the Government.

b) Privacy and cybersecurity obligation: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 requires every service provider to outline a detailed privacy policy that is applicable to all users, that articulates nature of data collected, type of data that is collected and for what purpose including retention and further use. Additionally, India has consumer protection laws, financial regulations, competition law that ensures different aspects of user interest are protected. Further, Section 72 A of the IT Act provides for punishment for disclosure of information in breach of lawful contract. The Unified Licence mechanism mandates that bulk encryption should not be employed, and similar requirements should not be imposed on OTT Communication Platforms.

Part-B: Issues related to Selective Banning of OTT services

TRAI can regulate the use of the spectrum by TSPs, however TRAI has no power to regulate or even make recommendations to the Department of Telecommunications regarding OTT service providers. Their regulation can and does happen through a separate law – the Information Technology Act, 2000 along with certain sections in the Indian Penal Code, Criminal Procedure Code, and sectoral laws, amongst others. Intermediaries such as OTT service providers, including TSPs in their provision of OTT services, are required to abide by the Information Technology (Intermediaries Guidelines) Rules, 2021 under Section 87(2)(zg) read with Section 79(2) of the Information Technology Act, 2000.

SFLC.IN
2nd Floor, K9
Birbal Road, K-Block
Jangpura Extension, Delhi – 110014
https://sflc.in | mail@sflc.in | +91-11-43587126

Part 3 of the Information Technology Rules, 2021 classify its subjects into two categories namely i. Publishers of news and current affairs content; and ii. Publishers of online curated content. The rules are to be administered by the MIB. Currently there is a stay on the operation of Part 3 of the IL Rules, 2021. Additionally, "digital media" also falls under the jurisdiction and mandate of the I&B Ministry according to an amendment to the AoB Rules made in 2021 Therefore, the I&B Ministry should be the source of any legislation proposal to control such media. The purpose of the modification to the Business Rules was to have "platforms" (and subsequently the content on platforms) be governed by the MeitY while "publisher" content (and consequently the publishers of such content) be regulated by the I&B Ministry.

TRAI has no power to regulate OTT services. Instead, the power under the current laws rests with MeitY. If action is required beyond the scope of what is permissible under the Information Technology Act, 2000, then a new law would be needed for this purpose.
Surveillance of Internet networks is provisioned by Sections 69 and 69B of the Information Technology Act, 2000 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 as well as the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. These, along with Section 5 of the Indian Telegraph Act, 1885 read with Rule 419A of the Indian Telegraph Rules, 1951, lay down the substantive and procedural frameworks under which Law Enforcement Agencies may collect communications data and meta-data from communications service providers. The power to impose Internet Shutdowns is derived from Section 5(2) of the Indian Telegraph Act, 1859 along with the Temporary Suspension of Telecom Suspension Rules, 2017. Similarly the power to block websites lies with MEITY as well as MIB under the Information Technology Act, 2000. Section 69A of the IT act as well as Section 79 can be used by the executive and judiciary to block websites. Along with that websites can also be blocked under the Copyright Act 1957 as well as under the Civil Procedure Code, 1908. In the case of TSPs, their respective service licences contain clauses that further outline certain security conditions in support of the broader legislative framework.

Today, doctors and lawyers are conducting confidential communications with their clients over

end-to-end encrypted communication platforms such as WhatsApp. Journalists are using these platforms to communicate with their sources. Members of police and armed forces are sharing information internally through these platforms. Financial information is also shared by people over these platforms. If these platforms are required to function partially and selective banning of OTT service platforms takes place, it will gravely impact citizens. Many people use OTT Services such as Facebook Marketplace, Instagram ADs to run their business. Selectively banning these OTT services will gravely impact gig economy workers as well.

Encryption now forms the backbone of the digital economy. A large part of a sustainable digital economy is based on trust. If a country requires weakening of encryption or any form of backdoors, then the encryption and security products originating from or taking place in that country cannot be trusted for undertaking any task that involves personal data. Platforms that are required to implement such requirements would be faced with a choice to stop conducting business in India, weaken the security for their users across the globe, or to split their user base into (a) a global community except India with high security and (b) an isolated group of users in India that face high risk with weakened security. In such a situation, no OTT communication service originating in India would be trusted by the rest of the world. We recommend against any surveillance or interception measures on any OTT platform.

While Section 43 of the Information Technology Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 protecting only sensitive personal data or information, India is currently in the process of formulating a new data protection law. This law would impose restrictions and requirements upon OTT platforms for the collection, use, storage, transmission, sale and other activities related to personal data. It would be prudent for TRAI to take a wait-and-watch approach towards further developments in this area instead of attempting or recommending any regulation of OTT platforms at this juncture. Instead, it would be prudent to revisit the existing surveillance and interception requirements in light of the Supreme Court's judgement of the Right to Privacy.

The proposal for selectively banning OTTs is based on the premise that it is useful to shut down the internet or certain services in specific scenarios, such as during law and order problems.

We have witnessed internet shutdowns in India, even to prevent cheating in examinations. However, there is no evidence to support the claim that shutting down the internet is useful in controlling the situation during unrest. Often, shutdowns are resorted to as knee-jerk reactions to prevent protests by the people against the government.

As noted in the earlier part of our response, we believe OTT services should not be subject to any licensing or regulatory framework similar to TSPs. In the context of selective bans, we recommend that a regulatory framework for the same not be implemented either. Banning the internet has not resulted in any meaningful progress thus far, and have concurrently been found to be detrimental to parties involved. Seeking to regulate such action, selective as it may be, may therefore not show any positive results. Regulators of OTT services, if at all, regulate VoIP services and communication services- as seen in Germany, Austria and even then in limited ways, such as in relation to security and integrity provisions, interoperability provisions, and service quality provisions (Austria). Countries in the EU, under the European Electronic Communications Code (2018) have regulated only "number independent interpersonal communications services", which require them to provide information, submit security audits and be subject to investigations in case they do not comply with competent authorities. Modern democracies have not been implementing provisions that permit selective banning, even for restrictions as listed under Article 19 (2) of our Indian Constitution. In the absence of any evidence to suggest that selective banning of OTT services would not result in the disruption of critical services such as healthcare and education at all (which has been evidenced with internet shutdowns), seeking to implement such a framework may continue to invite harmful risks to the people subject to such selective bans.

Conclusive Remarks:

In conclusion, Internet Shutdowns, even partial ones, have a disproportionate human cost. Selective banning of OTT services should not be a way ahead to regulate the internet. Access to the Internet is emerging as a fundamental right and modern democracies should not be looking at blocking it even in a selective manner. Moreover, OTT services cannot be regulated by TRAI. Instead, MeitY is in charge under the current legal framework. A new law would be required for this purpose if the desired action seeks to go beyond what is allowed by the

Information Technology Act of 2000.

About SFLC.in:

SFLC.IN is a donor supported legal services organization that brings together lawyers, policy analysts, students, and technologists to protect freedom in the digital world. SFLC.IN promotes innovation and open access to knowledge by helping developers make great Free and Open Source Software, protect privacy and civil liberties for citizens in the digital world by educating and providing free legal advice and help policy makers make informed and just decisions with the use and adoption of technology. SFLC.in has been granted Consultative Status with the Economic and Social Council of the United Nations (ECOSOC).