From: biyani@isoc.org
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: voge@isoc.org, bernardi@isoc.org, gnojeim@cdt.org, sheetal@gp-digital.org, prateek@internetfreedom.in, utiwari@mozilla.com
Sent: Thursday, August 17, 2023 3:26:45 PM
Subject: Global Encryption Coalition Steering Committee's comments on TRAI consultation: Regulatory Mechanism for OTT Communication Services & Selective Banning of OTT Services

To,

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

Sir,

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 comments from the Steering Committee of the Global Encryption Coalition in the attached.

The Global Encryption Coalition promotes and defends encryption in key countries and multilateral fora where it is under threat. The GEC also supports efforts by companies to offer encrypted services to their users. The Coalition has over 350 members across the world.

This is a statement of the Steering Committee of the Global Encryption Coalition. While Steering Committee members may have additional concerns about the Consultation, this statement focuses on the Steering Committee's shared encryption concerns.

We 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 and protect encryption.

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

Global Encryption Coalition Steering Committee’s submission to the Telecom Regulatory Authority of India’s consultation: **Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services**

August 17, 2023

The Steering Committee of the Global Encryption Coalition submits this statement to the Telecom Regulatory Authority of India (TRAI) to encourage it to refrain from introducing a licensing framework for Internet-based services and undermining encryption in the context of the current ‘Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services’ (henceforth “Consultation”).

The Global Encryption Coalition promotes and defends encryption in key countries and multilateral fora where it is under threat. The GEC also supports efforts by companies to offer encrypted services to their users. The Coalition has over 350 members across the world.

This is a statement of the Steering Committee of the Global Encryption Coalition, which consists of Center for Democracy & Technology, Global Partners Digital, Internet Freedom Foundation, Internet Society, and Mozilla. While Steering Committee members may have additional concerns about the Consultation, this statement focuses on the Steering Committee’s shared encryption concerns.

We are concerned with the requirements to introduce a licensing or registration framework for Internet-based services in India. We believe there is no need for a licensing framework for Internet-based services, including modern communication services.

Any licensing framework for Internet-based services will stifle innovation and growth, and raise significant barriers to entry—especially for startups and independent 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.

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. This will create an uncertain regulatory environment for Internet-based services, and will only stifle and inhibit innovation.

Further, platforms that offer encrypted communication services, particularly end-to-end encrypted services (e2ee services) provide distinct services and serve separate purposes from telecommunication services, and as a result, should not be regulated in the same way. Providers of e2ee services cannot decrypt and access the contents of the communications they carry.

Question 7 in the Consultation asks what licensing or regulatory framework would be appropriate for different classes of OTT services, including the framework that would be applicable to matters of lawful interception, as well as privacy and security. We believe it critically important that regulatory requirements related to lawful interception of messages on e2ee communication services should not compel messaging platforms to weaken security afforded to users by strong encryption, nor should they encourage services to abandon e2ee. Such an outcome 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 makes the owner more vulnerable to criminals and intruders, and that’s the physical world equivalent of weakening encryption. Criminals and malicious actors could gain access to sensitive and personal information.

E2ee ensures that what people share with each other online stays confidential among them, i.e., the sender and intended recipients of the information. ‘Lawful interception’ of messages is not only impossible on e2ee platforms but is also incompatible with e2ee–since service providers themselves cannot access the communication between sending and receiving parties. Hence, unless the regulatory regime recognizes this reality, 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.

E2ee communication platforms could pull out of India if the regulatory regime does not protect this method of securing communications. It would not be a surprising result, considering the withdrawal of Virtual Private Networks (VPNs) from India such as Nord, Proton, Surfshark etc. following the onerous CERT-In 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 citizens of India, as well as their other customers globally.

Several businesses in India are built upon e2ee 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 effectively prohibiting 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 communication security protocols have also been exploited by hostile foreign governments, for instance, to access critical national infrastructure.

In conclusion, if the TRAI recommends any changes to the existing regulatory framework for Internet-based services, we urge it to ensure that the framework does not penalize—and indeed, that it supports—the offer of communication services that are encrypted end-to-end.