To,
Shri Baijayant Panda
Chairperson, Select Committee of Lok Sabha to Examine the Income Tax Bill, 2025
Lok Sabha Secretariat, New Delhi
Email: bj.panda@sansad.nic.in

Subject: Open Letter Regarding the Income Tax Bill, 2025 and its Implications for Encryption and Privacy

We, the undersigned civil society organizations, companies, and cybersecurity experts, including the members of the Global Encryption Coalition (GEC), are writing to express our significant concerns regarding specific provisions of the Income Tax Bill, 2025, particularly as they threaten end-to-end encryption, user privacy, and data security. The GEC, launched in 2020, has 434 members that includes civil society organisations, businesses and individual experts with a goal to promote and defend encryption for the security and privacy of individuals and nations.

The Income Tax Bill, 2025, particularly under Clause 247, significantly expands the powers of tax authorities to search and seize data in "virtual digital spaces," explicitly mandating disclosure of passwords and allowing forced access to encrypted information.[1] Clause 247(1)(ii) mandates disclosure of passwords, posing direct threats to privacy, while Clause 247(1)(iii) allows forced entry into encrypted digital spaces, effectively undermining end-to-end encryption technologies essential for secure communication. End-to-end encryption is crucial not only for personal privacy but also for protecting freedom of speech and maintaining secure digital communications globally. Any legal requirement that compels the disclosure of passwords or permits forced encryption breaking risks weakening the security infrastructure that protects citizens, businesses, and even government operations.

Further troubling is the expansive definition of "virtual digital space" under Clause 261(e)–(i), encompassing personal messaging platforms, cloud servers, and even IoT devices, which amplifies the scope of potential privacy violations. We urge the Government of India to reconsider and revise these provisions, aligning the legislation with international best practices and fundamental freedoms and human rights, including the right to privacy, clearly reaffirmed by India's Supreme Court in the landmark judgment of *Justice K.S. Puttaswamy* v. *Union of India*. We strongly advocate for incorporating essential safeguards such as judicial oversight, transparency in investigative procedures, proportionality, and protocols ensuring digital evidence integrity.

The ability to communicate safely and securely is a precondition to being able to communicate and express one's views. In India, where digital threats are growing, encryption helps prevent harassment, coercion, and violence. From a business standpoint, weakening encryption security could erode trust in India's digital economy. Companies handling sensitive financial and legal information may face increased risks of data breaches and cyberattacks, deterring investors and businesses.

The rise in financial fraud makes strong encryption even more critical. In FY 2024, high-value cyber fraud cases in India quadrupled, causing losses exceeding $20 million.[2]

---

[1] A. Gupta & M. Garg, IFF writes to the Select Committee to review the digital search and seizure powers under the Income Tax Bill, 2025, Internet Freedom Foundation available at https://s.42l.fr/ITBill2025.

[2] Reuters. *Cyber Fraud Cases in India Surged 4-Fold in FY24, Causing $20 Mn in Losses*. Business Standard, 11 Mar. 2025, https://www.business-standard.com/india-news/cyber-fraud-cases-in-india-surged-4-fold-in-fy24-causing-20-mn-in-losses-125031100484_1.html.

Weak encryption could further expose individuals and businesses to scams, financial fraud, and identity theft. Reduced security also increases risks of foreign espionage, threatening national security and economic interests. As cybersecurity remains a priority, weakening encryption could have lasting consequences for India's digital ambitions and global competitiveness.

The Global Encryption Coalition and all co-signatory organizations remain committed to providing our collective expertise and insights. We welcome constructive dialogue and are ready to engage collaboratively with Indian government stakeholders to ensure legislation protects privacy, security, and fundamental freedoms and human rights in digital spaces. Given the urgency of these issues, we sincerely hope for immediate and meaningful engagement by the government to address these critical concerns.

Signatories

Organizations

Internet Society
Internet Freedom Foundation
Center for Democracy & Technology
Global Partners Digital
Access Now
Electronic Frontier Foundation (EFF)
Internet Sans Frontières
Brave
CCAOI
Software Freedom Law Center, India (SFLC.in)
Digital Rights Nepal
Internet Governance Project, Georgia Institute of Technology
Paradigm Initiative
Index on Censorship
Tech for Good Asia
TEDIC
SecureCrypt
Africa Media and Information Technology Initiative (AfriMITI)
Encryption Advocates Council
Human Rights Journalists Network Nigeria
Janastu
Cybersecurity Advisors Network (CyAN)
Article 21 Trust
Internet Society Mali Chapter
Internet Society Ethiopia Chapter
Internet Society India Hyderabad Chapter
Internet Society India Bengaluru

Individual Experts*

Syeda Saadia Azim, Government of West Bengal
Nikhil Kulkarni, DSCI
Dhruv Dhody, Internet Architecture Board (IAB) Member
Siddhartha Das, IIIT Hyderabad

*Affiliations listed for identification purposes only