November 9, 2022

Shri. Naveen Kumar
Joint Secretary - Telecom
Department of Telecommunications
Ministry of Communications
New Delhi 110001

Comment on the Indian Telecommunication Bill 2022

Thank you for the opportunity to comment on the draft Indian Telecommunication Bill (the "Bill") 2022. We are computer security, privacy, and technology policy researchers. Our work on communication systems has examined security and privacy risks posed by content moderation, censorship, and surveillance. In this comment, we briefly describe our concerns relating to Chapters 2, 3, 6 and Schedule 3 of the Bill, with specific focus on network security and privacy.

Chapters 2 and 3: Licensing

The definition of a "telecommunication service" in Section 2(21) is overbroad, encompassing all online services, including virtual private networks (VPNs), end-to-end encrypted (E2EE) communication services, and private social networks. Under Chapter 3, a licence is required to run a "telecommunication service".

- Licensing places an onerous burden on individuals and organisations who host such services for personal, family or community use. It would destroy the "self-hosting" movement in open-source software. Examples of popular self-hosted software include home-office VPNs (e.g., Tailscale), private social networks (e.g., Mastodon), and private chat (e.g., Matrix).
- Licensing greatly reduces competition in the marketplace by steeply increasing the barrier to entry. It favours entrenched well-resourced incumbents over new disruptive entrants.
- We strongly disagree with the false equivalence of "Same Service, Same Rules" propounded by the Cellular Operators' Association of India (COAI). E2EE

services offer much stronger privacy and security protections than cellular service operators in India. Even if operators—that currently monetize user communication data—were to deploy IP-based Rich Communications Services (RCS), they would have no business incentive to offer strong privacy protection. Treating E2EE services and cellular services alike will dilute privacy and security of Internet users.

We recommend that the definition of "telecommunication service", for the purposes of the Bill, be narrowed down to traditional telephony and messaging, and exclude any online services.

Chapter 3: Sender Identification

Section 4(8) prescribes that "the identity of a person sending a message using telecommunication services shall be available to the user receiving such message." This is an important security measure in case of cellular networks where caller ID spoofing is a widespread issue. However, this provision could also apply to E2EE communication services that already provide strong sender authentication mechanisms. Such an obligation would end up undermining privacy guarantees offered to senders (e.g., Signal, SecureDrop). Whistleblowers, journalists, and disempowered groups depend on these privacy protections for their physical safety. Recent research indicates that sender anonymity is compatible with abuse detection in E2EE.[1] We recommend that the Bill exclude Internet services from the obligation to reveal the sender's identity to recipients.

Chapter 6: Operating Standards

Section 23 gives the Central Government the power to prescribe standards pertaining to telecommunications infrastructure and service reliability. This is necessary to ensure affordable access to reliable telecommunications services across India. However, the present draft does not address network security or user privacy. We note that a similar provision in the Information Technology (IT) Act has been previously used to advance

[1] Issa, R., Alhaddad, N., & Varia, M. (2022). Hecate: abuse reporting in secure messengers with sealed sender. In: *31st USENIX Security Symposium* (pp. 2335-2352).

policy that seriously undermines privacy protections offered by E2EE services.[2] We recommend that the Bill explicitly state that any Government-prescribed standard must not have a negative impact on network security or user privacy. This could be ensured by prescribing strong encryption for communication data: both at rest and in transit.

Chapter 6: Surveillance of E2EE Communication

Section 24(2)(a) empowers the Government to order interception of communication data upon a written request. The draft provision could also apply to E2EE services (e.g., WhatsApp, Signal) that cannot access messages carried by them. It is technically infeasible[3] to intercept end-to-end encrypted communications, as decryption keys are only known to the participants, and not to the service provider. We recommend that—akin to the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009—the obligation on online services to assist with interception be limited "to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key."[4]

Chapter 6: Surveillance Accountability

The surveillance powers created in Section 24 should be in tandem with strong accountability mechanisms.

- The draft Bill grants unilateral power to authorised government personnel to order interception of communications. In contrast, principles of international human rights law require that surveillance requests be sanctioned by an impartial and independent authority, such as the judiciary.[5] Domestic legislation

[2] Ministry of Electronics and Information Technology (MeitY), Draft National Encryption Policy, 2015. *MeitY*. 2015. <https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf>.; *Also see* Mohanty, B. "The Encryption Debate in India." *Carnegie Endowment for International Peace*. 2019. <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213>

[3] Kulshrestha, A., & Mayer, J. (2021). Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation. In: *30th USENIX Security Symposium* (pp. 893-910). Knodel, M. et al. Definition of End-to-end Encryption. *Internet-Draft, work in progress*. 2022. <https://datatracker.ietf.org/doc/html/draft-knodel-e2ee-definition>

[4] Rule 13(3) and Rule 2(g)(i), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[5] "Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance." *Electronic Frontier Foundation and ors*. 2014. <https://necessaryandproportionate.org/principles/>

enabling communications surveillance (including the Telegraph Act and the Information Technology Act) are similar to the draft Bill in that they do not require judicial review,[6] and Indian courts have not struck them down yet.[7] However, legal scholars have argued that after *Puttaswamy v. Union of India* cases (which affirmed the constitutional right to privacy to all Indians, and adjudged the legality of the Aadhaar program), judicial review of surveillance is a "constitutional imperative."[8] To align the Bill with international human rights and constitutional jurisprudence, we strongly recommend that the Bill require judicial review of all surveillance/interception requests.

- The draft Bill—through omission—disregards the rights of the targets of the surveillance. Targets should be informed of governmental interception of the communications as soon as possible, and as long as it does not defeat the purpose of the surveillance.[9] This will enable them to challenge unlawful and/or unconstitutional surveillance, and exercise their constitutional right to legal remedy.[10]
- The draft Bill also omits public accountability measures. Central and State Governments should release transparency statistics regarding their surveillance activities, at least annually. For example, the U.S. Intelligence Community has published a transparency report every year since 2014. Cryptographic techniques may be used to protect user privacy and guarantee trust in the generated statistics.[11]

Schedule 3: Unauthorised Access

Under Schedule 3(2), "gaining or attempting to gain unauthorised access to a telecommunications service" and "intercepting a message unlawfully" are criminal offences. This is necessary to deter malicious actors. However, without reasonable

[6] Section 5(2), Indian Telegraph Act, 1885. Section 69, Information Technology Act, 2000.
[7] *People's Union Of Civil Liberties v. Union of India* (1997) 1 SCC 301.
[8] Bhandari, V., & Lahiri, K. (2020). The surveillance state, privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world. *Vol. 3(2) U. Oxford Hum. Rts. Hub J.*, 55.
[9] *Electronic Frontier Foundation and ors* (n 5).
[10] Articles 32 and 226, Constitution Of India, 1949.
[11] Kulshrestha, A., & Mayer, J. (2022). Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum. In: *31st USENIX Security Symposium* (pp. 1705-1722).

exceptions, this provision could have a negative impact on network security.

- The provision could criminalise almost all vulnerability testing and will have a chilling effect on responsible disclosure of exploitable bugs. It could render our telecommunication infrastructure insecure. Security researchers like us face serious legal risks from such ambiguous laws and enforcement.[12] We recommend that the Bill carve an exception for good faith computer security research that is responsibly disclosed. In May 2022, the U.S. Department of Justice created a similar exemption under the Computer Fraud and Abuse Act (CFAA).[13]
- The technical meaning of "access" varies by online service. If the same standard is applied across all services, it could criminalise certain legal usage of authorised access like web scraping.[14] Within this framework, the Bill should clarify the meaning of "access", at least for Internet services.

We hope the Ministry finds our suggestions valuable.

Sincerely,

Anunay Kulshrestha
Doctoral Candidate, Center for Information Technology Policy, Princeton University[15]

Gurshabad Grover
Information Controls Fellow, Open Tech Fund[15]

[12] Saini, K., Prakash, P., & Hickok, E. (2019). Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India. *Centre for Internet and Society*. <https://cis-india.org/internet-governance/blog/improving-the-processes-for-disclosing-security-vulnerabilities-to-government-entities-in-india>
[13] Computer Fraud and Abuse Act (Title 18, United States Code, Section 1030). <https://www.justice.gov/opa/press-release/file/1507126/download>
[14] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019).
[15] All expressed views are personal. We are grateful to Jonathan Mayer, Aayush Rathi, and Divyank Katira for their valuable feedback.