March 15, 2019

To:
Mr Ravi Shankar Prasad
Hon'ble Union Minister for Law and Justice, and Electronics and Information Technology
Government of India

CC:

- IT Secretary Ajay Prakash Sawhney, Ministry of Electronics and IT
- Group Coordinator - Cyberlaw and eSecurity Group, Ministry of Electronics and IT
- Joint Secretary S. Gopalakrishnan, Ministry of Electronics and IT
- Prime Minister's Office, Government of India

Subject: International coalition of organizations and experts call on the Ministry of Electronics and Information Technology to withdraw the draft amendments proposed to the Information Technology (Intermediary Guidelines) Rules

Sir,

The undersigned organizations and experts urge you to protect a free, open, and secure internet in India. We are an international coalition of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online; and security researchers with expertise in encryption and computer science; all of whom share a commitment to strong privacy, freedom of expression, encryption, and cybersecurity standards. We respectfully call on you to withdraw the draft amendments proposed to the Information Technology (Intermediary Guidelines) Rules, as proposed by the Union Ministry of Electronics and Information Technology (MeitY) of the Government of India in December. As published, the draft amendments would erode digital security and undermine the exercise of human rights globally.

Based on what has been made public by statements from Ministry officials, the stated intent behind this proposal to amend the intermediary guidelines is to tackle incidents of alleged misuse of social media platforms and the spreading of targeted disinformation in India. However, the proposed amendments would harm fundamental rights and the space for a free internet, without necessarily addressing the problems that the ministry aims to resolve. The Government of India has repeatedly stated that it seeks to protect fundamental rights and internet freedom, and these amendments are inconsistent with those important goals.[1]

As many of the signatories to this letter have observed previously, strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, or repressive governments trying to stifle dissent. Encryption thereby protects us from innumerable criminal and national security threats. Additionally, encryption is essential to the rights of privacy and free expression. David Kaye, the

[1] Govt working to ensure free, safe internet access to all: Ravi Shankar Prasad, Mint, November 25, 2017 (Accessible at https://www.livemint.com/Politics/klLCxKVG4wQfMMEiiJAc1J/Govt-working-to-ensure-free-safe-internet-access-to-all-Ra.html)

United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, recommended in his 2015 report that states promote encryption and anonymity, noting that they "facilitate and often enable the rights to freedom of opinion and expression."[2]

We urge the Union Government to build on the strong position in favour of protecting fundamental rights online that was laid down by the Indian Supreme Court in its landmark *Shreya Singhal*[3] and *Puttaswamy*[4] judgements in 2015 and 2017. As the world's largest democracy and the second largest base of internet users in the world, India plays a crucial role in determining the present and future of the global internet, and should therefore champion robust protection for freedom of expression and privacy online.

In addition to the detailed feedback and input already provided by several organisations in the earlier consultation,[5] we wish to emphasise the following concerns:

1. **The proposed amendments would undermine secure communications and create an overbroad surveillance regime for intermediaries by empowering a wide variety of government organisations to request "information and assistance" from intermediaries**.

   This would include requesting intermediaries to ensure "traceability" of messages, by providing information related to the originator and receivers of a message, which has been shared on, for example, a peer-to-peer encrypted messaging platform like WhatsApp. It is not clear what actions could be covered by the requirement to "enable tracing out of such originator of information," but in order for WhatsApp, which is used by over 220 million people in India, to comply with such a request, the platform may be required to weaken encryption, or include encryption backdoors in its product. The government might also try to rely on a "tracing out" provision to require intermediaries to collect and store additional metadata, which would create further threats to privacy rights. In addition, there is a risk that the "tracing out" requirement could be read to permit government demands that intermediaries undermine authentication systems (which underpin the trust that communications are indeed between the sender and their intended recipients), install software that may introduce new vulnerabilities, or otherwise weaken the security features of their products.

   Undermining security features in order to ensure traceability would affect all users of that platform, not just those that are the subjects of the information request. Protections for privacy, data security, and free expression that are derived from the availability of strong encryption would be weakened or eliminated through the use of this amendment.

---

[2] David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report on the use of Encryption and Anonymity in Digital Communications (May 22, 2015), paragraphs 59-60, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement.

[3] Supreme Court of India, Writ Petition (Criminal) No.167 Of 2012 (Accessible at https://meity.gov.in/writereaddata/files/Honorable-Supreme-Court-order-dated-24th-March%202015.pdf)

[4] Supreme Court Of India, Writ Petition (Civil) No 494 Of 2012 (Accessible at https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf)

[5] Submissions available at https://meity.gov.in/comments-invited-draft-intermediary-rules

Compelling changes in technologies that undermine digital security and encryption is beyond what is acceptable in Indian law and international human rights standards.[6] Providing such wide and ambiguous powers to a number of government actors beyond those currently specified by legal provisions on interception of communications would directly harm the fundamental right to privacy of Indians and facilitate unchecked surveillance. To that extent, we respectfully disagree with statements from MeitY officials that requiring "traceability" would not undermine encryption or involve surveillance. Any proposal that relies on the hashing of transmitted content would be impossible to achieve for any provider that enables end-to-end encryption, because the service would have no access to the content being transmitted. To implement this proposal, the government would have to require providers to make changes to their client software that would hash the unencrypted content and upload the result. Such changes, however, would pose unprecedented privacy harms and the risk of security vulnerabilities. Technical proposals such as scanning and storing hashes of content transmitted on encrypted messaging services would undermine a secure internet and mandate data retention, harming privacy.

This amendment would also degrade the confidence of everyday, lawful users in their online communications platforms. Any proposal that undermines user trust penalizes the overwhelming majority of technology users while merely incentivizing those few bad actors to shift to readily available products beyond the law's reach. It is a reality that encryption products are available all over the world and cannot be easily constrained by territorial borders.[7] Thus, while the few nefarious actors targeted by the law will avail themselves of other services, average users will disproportionately suffer consequences of degraded security and trust.

India has already seen widespread opposition to undermining encryption, which led to the withdrawal of the earlier draft national encryption policy made available for public review in September 2015. We instead encourage the Government of India to extend the headway made in the *Puttaswamy* judgment of the Supreme Court of India and ensure that any governmental access to data or surveillance actions build on the necessary and proportionate standards and include effective institutional checks and balances - particularly with respect to judicial approval and oversight of user data requests.

Additionally, the draft intermediary guidelines propose an overbroad mandate to retain data that is antithetical to privacy. The guidelines require intermediaries to preserve content requested by law enforcement agencies for 180 days or longer as deemed necessary by government agencies or a court. By leaving the duration for storage of such data open-ended, the provision runs contrary to the principle of 'Storage Limitation' recommended by the Srikrishna Committee.[8] Provisions regarding storage limitation and data retention must not be included within the fold of the Intermediary Guidelines, and should be subject to parliamentary lawmaking.

[6] Please refer to securetheinternet.org
[7] Bruce Schneier, Kathleen Seidel & Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Feb. 11, 2016, https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf
[8] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians," p.60 available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

2. **The draft amendments would require intermediaries to take down and remove content in a way that would undermine free expression**.

   In particular, the proposed regulatory mandate for proactive monitoring, selection, and deletion of "unlawful content" by intermediaries via automated means would directly conflict with the legal standard laid down by the Supreme Court of India in the *Shreya Singhal* judgment,[9] which holds that intermediaries should only be legally compelled to take down content on the basis of court orders or legally empowered government agencies. Furthermore, India is a state party to the International Covenant on Civil and Political Rights (ICCPR), which restricts permissible limitations on freedom of expression to only those that are "necessary" and specified in Art. 19(3). The UN Human Rights Committee in its General Comment 34 requires that: "Any restriction on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of Article 19 of the ICCPR]". These limitations, moreover, "must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected."[10]

   We believe that the proposed amendments, by threatening intermediaries with adverse consequences for failing to censor, do not pass this standard. The provision stating that intermediaries should deploy automated tools to identify and remove "unlawful" content, would likely cause intermediaries to err in favor of takedowns, resulting in unnecessary censorship of free expression. In addition, the amendments would legally force private actors to increasingly use their discretion to mediate human rights, which will likely result in inconsistent, unnecessary, and disproportionate restrictions wholly controlled by intermediaries.

To protect human rights online and a secure internet in India, we call on you to please withdraw the proposed amendments. We urge the Government of India to re-consider these proposed amendments in their totality. Any policy or regulatory action should involve a greater discussion of the concerns facing government along with data from stakeholders on the issues under consideration and the different tools available to policymakers. A rushed notification of these amendments to the Intermediary Liability (Due Diligence) Guidelines under the Information Technology Act would not only violate Indian constitutional standards regarding fundamental rights and international human rights law, but also chill free expression and access to information as India's General Elections commence.

Further, with the upcoming General Elections in India and the imposition of the Model Code of Conduct on new policy decisions in place, we urge the government to not push through these amended regulations given their impact on fundamental rights and secure communications.

[9] Supreme Court of India, Writ Petition (Criminal) No.167 Of 2012 (Accessible at https://meity.gov.in/writereaddata/files/Honorable-Supreme-Court-order-dated-24th-March%202015.pdf)
[10] HRC General Comment 27 and General Comment 34.

We believe that India, as the world's largest democracy, has the opportunity to enact a rights-based regulatory framework for the internet that could act as a template not just for other emerging economies but for governments worldover.

Thanking you,

Civil Society Organizations

1. Access Now
2. Advocacy for Principled Action in Government
3. Asociación para una Ciudadanía Participativa, ACI Participa (Honduras)
4. Blueprint for Free Speech
5. Center for Democracy & Technology
6. Centre for Internet and Society
7. Defending Rights & Dissent
8. Derechos Digitales (Latin America)
9. Digital Empowerment Foundation
10. Electronic Frontier Foundation
11. Engine
12. Fundación Acceso (Centroamérica)
13. Government Accountability Project
14. Human Rights Watch
15. Internet Democracy Project
16. Internet Freedom Foundation
17. Internet Society (Panamá)
18. IPANDETEC - Centroamérica
19. Manushya Foundation
20. New America's Open Technology Institute
21. Observatorio de Información y Datos de Latinoamérica
22. SFLC.in
23. The Bachchao Project
24. The Dialogue
25. X-Lab

Security and Policy Experts*

1. Adam Shostack, author, Threat Modeling: Designing for Security
2. Jon Callas, Senior Technology Fellow, ACLU
3. Liz McIntyre, Author and Consumer Privacy Expert
4. Riana Pfefferkorn, Stanford Center for Internet and Society
5. Sarvjeet Singh, Centre for Communication Governance, National Law University Delhi
6. Susan Landau, Bridge Professor, Fletcher School of Law & Diplomacy and School of Engineering, Department of Computer Science, Tufts University

*Affiliations provided only for identification purposes.