July 4, 2022

To,
Shri Rajeev Chandrasekhar
Hon'ble Minister of State
Ministry of Electronics and Information Technology
Government of India

CC
Shri Alkesh Kumar Sharma
Secretary, Electronics & Information Technology
Ministry of Electronics and Information Technology
Government of India

Subject: International group of organizations and individuals call on MeitY to withdraw the requirement for end-to-end encrypted messaging services to enable the identification of the first originator of information

Sir,

The undersigned organizations and individuals share a commitment to strong encryption, security, and privacy. **We are writing to urge you to withdraw the requirement for end-to-end encrypted messaging services to enable the identification of the 'first originator' of information on their platforms** as contained in the IT Rules 2021. The traceability requirements in the IT Rules 2021 would threaten India's national security, as well as the security of its citizens and businesses.

The following are the main concerns we perceive with regard to the implementation of this requirement:

1) **Implementing this requirement will require messaging services to link each message with its originator, endangering national security and security of citizens and businesses:**
End-to-end encrypted (e2ee) messaging services do not have the capability to read messages shared on their platform or identify the first originator of messages. The proposal being considered by the Government of India currently may not overtly require messaging services to *disclose* a message, but that does not mean the service will not need to *access* the contents of the message. In most cases when the government is seeking originator information, it may be on the basis of already knowing the contents of a particular message. However, to comply with this requirement, **messaging services will need to link each message with its originator**. They could only do so by accessing each message exchanged on their platform - and crores of messages are exchanged on messaging platforms every day - thus breaking end-to-end encryption.

E2ee ensures that data and communication is confidential between the sender and receiver. No third party can read e2ee data. E2ee helps prevent spies, terrorist organizations and hostile governments from accessing confidential communication of government officials, law enforcement officers, military personnel, and emergency responders. Critical infrastructure runs on services and platforms available to consumers and is protected by the same encryption. Crores of people access national critical infrastructure services - the power grid, transportation systems, the financial system - using their personal devices. Employees at these infrastructure entities often connect to internal sites and networks to manage operations or exchange sensitive information that enables the smooth operation of such services. The encryption present on our smartphones protecting these interactions is vital to the nation's security.

Mandating traceability on e2ee messaging services will also result in associated costs for storing all the data needed for tracing every message ever exchanged on such a platform, impacting affordability and preventing new startups from easily and affordably offering e2ee messaging services in the country.

2) **Mandating traceability on end-to-end encrypted messaging platforms is not technically feasible:** There are two proposals currently being considered to help with the implementation of traceability, and proponents of both claim that they do not undermine e2ee. Our concerns with both proposals are as follows:

> (a) **The identity of the originator will be tagged and included in an encrypted form with each message.** Originally formulated by Professor V. Kamakoti of the Indian Institute of Technology, Madras, this proposal will require an intermediary to hold in escrow the key to decrypt the originator's information, which may be used to reveal the same for a particular message in response to an order from an authorized body. Further, the proposal suggests that users mark a message 'forwardable' or 'non-forwardable' in order to indicate assumption of responsibility as an originator. If a user originates a message and marks it as 'forwardable', their information gets linked with the message. However, if a sender marks a message 'non-forwardable' and the recipient forwards it nonetheless, the recipient becomes the originator and their information is linked with the message.
>
> The premise of a traceability mandate is that forwarding a message is the only way in which the same content circulates on a platform. However, that is not true. For instance, if a user downloads a viral message or image and instead of forwarding it, and then copies and pastes the message to send it to several others (or sends the image from their gallery), this starts a new messaging chain altogether of which they become the originator. Thus, the same message is not necessarily sent in a linear fashion that can be traced back to a single originator.
>
> As a result, the very concept of the "first originator" of a message is inherently ambiguous. For instance, suppose User A sends an image to User B. A few days later, User C obtains the same image from a social media handle and shares the link with Users D, E and F. The second chain then goes viral. It is unclear who would be treated as the first originator in such cases – User A or User C? There can be thousands of such chains of simultaneous communications. The bottom line is that in practice it would be onerous, if not impossible, to discern the "first originator" of a specific message, especially without accessing the content of e2ee messages to determine which chains are carrying the same content.

This proposal has been critiqued by a number of eminent experts, most notably by Professor Manoj Prabhakaran of the Indian Institute of Technology, Bombay. Prof. Prabhakaran in his critique, speaks to the limited effectiveness of the proposal and its impacts on users' privacy.

(b) **A library of alpha-numeric hashes for every message will be maintained, against which the hash of a message subject to a government order can be compared to enable traceability.** Hashing is the practice of using an algorithm to map data to a fixed length. An e2ee messaging service would therefore have to maintain a library of numerous hashes to assist the government trace the originator of a message in case of an authorized order. However, the proposal rests on the faulty assumption that the hash value of a message remains the same if the content of the message remains the same. In fact, when e2ee platforms like Signal and WhatsApp generate a hash value, the unique identity of the sender and the recipient is also taken into account.

Therefore, if User A sends "hey there!" to User B, and User B forwards that message to User C, each of those exchanges will carry a different hash value. When the message from User B to User C is taken to the intermediary for comparison against its repository of hashes, it will not reveal User A's message to User B at all. That is because the protocol underlying services such as WhatsApp and Signal use 'forward secrecy', a privacy-enhancing feature that essentially changes the key between two users for every message. Thus, to comply with the government's demands, e2ee messaging services would have to effectively give up this feature and undermine the privacy and security of their services.

The government's proposal would also be likely to prove ineffective because the hash value changes with even the most insignificant change in the content of a message. For example, the hash of "hey there!" and "Hey There!!" would not be the same. Also, thanks to 'forward secrecy', if the identical message is sent by User B to User C twice, each of those messages will have a different hash value. Therefore, there is no practically feasible method of tracing any message back to its originator using alpha-numeric hashes.

3) **Traceability will result in an impairment of security, privacy, free speech and access to information for everyone:** No matter how traceability is implemented, it will either severely undermine or break e2ee, resulting in a loss of security, privacy, free speech and access to information for all. The Indian Supreme Court laid down a necessity and proportionality test when it recognized that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution." The four essential limbs of the test are: "(i) the action must be sanctioned by law; (ii) the proposed action must be necessary in a democratic society for a legitimate aim; (iii) the extent of such interference must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of such interference."

The traceability requirement may well not be able to meet every part of this test: (i) nothing in the parent statute, the Information Technology Act, contains any traceability or comparable requirement and thus it does not appear to be sanctioned by law; (ii) the requirement is not necessary for a legitimate aim since it will not actually achieve its professed aim; (iii) the interference is disproportionate because it imperils the privacy and free expression rights of crores of users, and the country's information security; and (iv) there are no material safeguards against interference for users of e2ee platforms, as the government can order the disclosure of identity information without any form of prior judicial review.

E2ee is a vital tool that enables users to communicate safely. It creates a secure space within which users can share intimate thoughts, personal information, medical and financial information, business transactions and ideas, and access critical infrastructure services, all without any fear. Traceability would undermine that in exchange for little or no public benefit.

As India heads towards rapid digitization, especially aimed at crucial public service delivery and national ambitions such as education, employment and public health, it is critical that strong, end-to-end encryption is upheld.

In order to protect national security as well as security of citizens and businesses, privacy and freedom of expression, and uphold an open, globally connected, secure and trustworthy Internet, it is imperative that the traceability requirement contained within the Indian IT Rules 2021 be withdrawn.

Thanking you,

Africa Media and Information Technology Initiative (AfriMITI)
ARTICLE 19
Center for Democracy & Technology
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Electronic Frontier Foundation
Encrypt Uganda
Global Partners Digital
Human Rights Journalists Network
Internet Freedom Foundation
Internet Governance Project, Georgia Institute of Technology, USA
Internet Society
LAYLO
Matthew T Roberts, President, Internet Society Liberia Chapter
Privacy & Access Council of Canada
Ranking Digital Rights
Simply Secure
Sivasubramanian M.
Tech for Good Asia
UBUNTEAM
University of Bosaso