Opinion

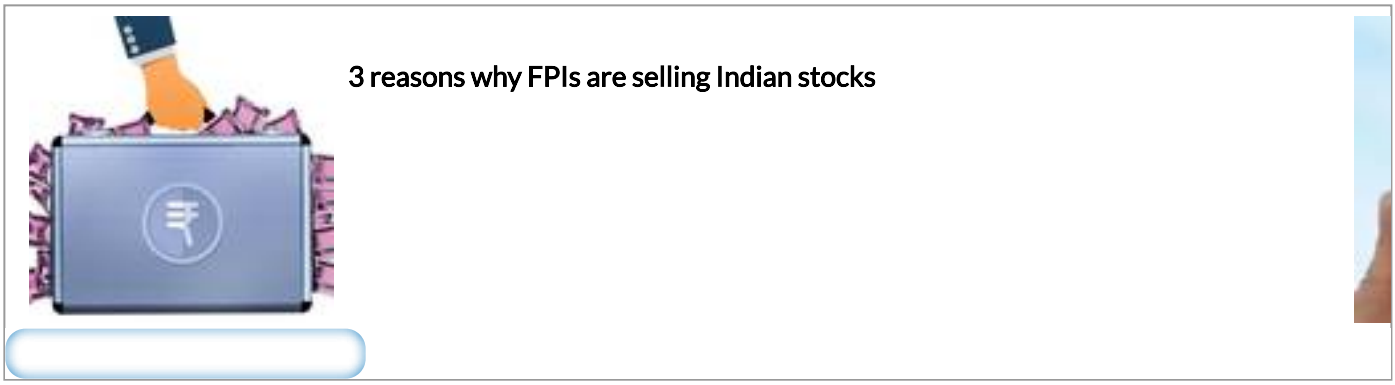
E2E encryption: Key to data-led growth

TV Ramachandran | Updated on December 20, 2021

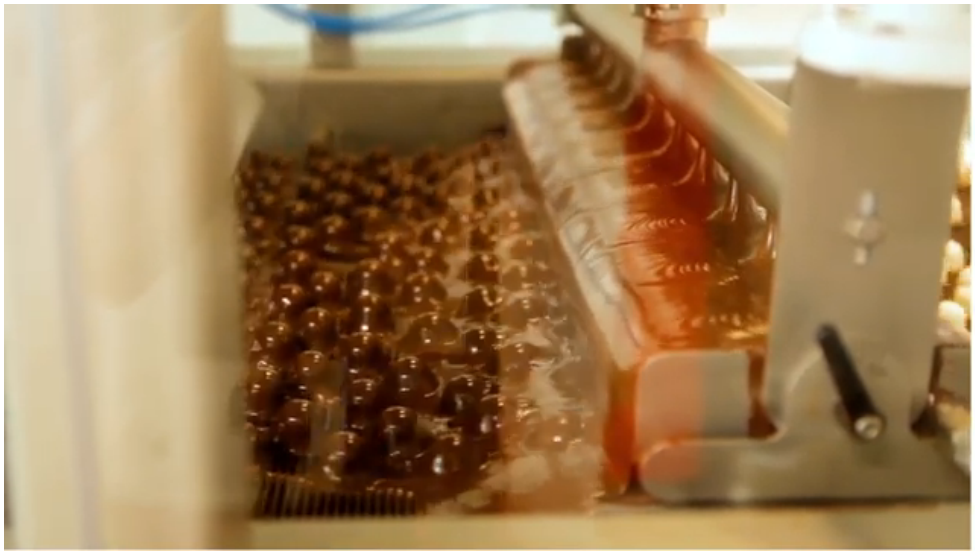
The PDP Bill should help safeguard privacy and socio-economic benefits of end-to-end encryption

We all have reasonable expectations of our police, government, and laws to protect us from criminal activity. However, would you feel comfortable sharing a copy of your front-door key with your local police station and municipal corporation office for safekeeping? Or, would you be okay with storing copies of your bank locker key at a local warehouse, just in case someone breaks in?

Each time we make copies of our keys and share them with others, we further compromise our security. Similarly, in the digital world, when we chip away at airtight end-to-end encryption (e2e), we create massive dents in our ability to protect our information.



So, while it is highly commendable that the Centre wishes to regulate and protect our personal data from the dark forces of the interwebs, the traceability requirement of the Personal Data Protection Bill (PDP, 2019) could well compromise that very endeavour. The Bill requires that technology platforms decode and share information about the originator of a message whenever a government agency wants it. This act introduces data vulnerabilities for cybercriminals to exploit. This, in turn, negatively impacts our data and India's socio-economic capital.



Encryption is the bedrock of cybersecurity. Doubling a nation's score on the Global Cybersecurity Index (GCI) is associated with a $2,700 increase in GDP/capita (Aapti Institute report, November 2021). Many industries like finance, health, communications, and IT data processing rely on e2e to offer domestic and international customers superior data security.

Traceability tangle

So, if India's laws protect the integrity of e2e transactions and communications, the more attractive we become to foreign investment and economy-boosting industries making their base here. Airtight e2e encryption ensures that no one, except the sender and the recipient,

can access the contents of a piece of communication – not even the technology platform or app on which the message is sent. However, the traceability requirement means that e2e is completely compromised.

India is the data processing capital of the world. Our IT and digital services industries are dependent on global companies trusting that their citizens' data can be processed safely and securely on our shores. Traceability negates that privacy, which may make international businesses hesitant to use India-based companies to handle their data.

Of course, the question arises: how to tackle national security issues, child pornography, or cybercriminal activity? This is indeed an extremely significant point that needs to be addressed for the safety of our citizens.

However, the traceability requirement is not the answer. It actually introduces more vulnerabilities that compromise national security and child safety and allow criminals a backdoor entry to protected information. It is not even a case of closing the proverbial stable door after the horse has fled. We are actively untethering the horse, opening the stable door, and walking away.

To understand why, let's look at how traceability can be applied. Companies will have to store every piece of data on large databases, just in case they may be required to provide information. This is an expensive undertaking. Also, encryption is automatically weakened once information is stored on servers, and data is vulnerable to attacks. Another way to find the originator of a message is to encode information about the originator of the message to every single message.

Apart from becoming a more inelegant form of communication, this introduces massive weaknesses in the system. For example, if you use an e2e service now, you can securely send your child's picture to their grandparents and trust that no one else can see it. However, suppose it is stored on a database. In that case, it offers easier access to cybercriminals and the vast number of global employees of the technology platform that hosts this data.

Right to privacy

The issue of traceability also compromises our social capital – the fundamental right to privacy granted by the Supreme Court to all Indians. In 2020, TRAI also recommended that encryption services must not be compromised to protect an individual's right to privacy.

Online communication is quickly becoming the norm in today's age – whether text messaging, as QWEE email, video, or more. Even government communication heavily relies on e2e encryption. It is in the interest of national security to ensure that this encrypted data is not exposed to foreign or domestic agents of terror.

Additionally, breaking encryption on one platform has not helped protect child safety online as lawbreakers shift to newer platforms. As the Centre now wishes to digitise our health information onto one health card, isn't it more reassuring if that information is heavily encrypted?

As a nation, we are dedicated to sustaining a bustling economy, one in which we make in India for the world. However, this success is reliant on trust. We need domestic and global partners and our citizens to trust our laws to protect us.

As the PDP Bill of 2019 is being debated, we must not lose sight of the Bill's original mission – to protect our personal data. End-to-end encryption is the best way to secure our messaging, communications, and more, and ensure data privacy is upheld. Compromising encryption in any form, as traceability will, opens Pandora's box of new privacy concerns that will hurt our socio-economic stability.

The writer is Honorary Fellow, IET (London), and President – Broadband India Forum. Views expressed are personal. Research inputs by Chandana Bala

Published on December 20, 2021