The Dialogue™
INFORM ENGAGE IDEATE

Technical Brief March, 2022

ANALYSING THE TECHNICAL WORKAROUNDS TO END-TO-END ENCRYPTION

About the Technical Brief

This technical brief is prepared basis the workshop 'Decrypting Encryption' hosted by The DialogueTM on 16th December 2021, with the objective of analysing the technical and policy aspects of encryption technology. The workshop was led by Dr. Sandeep Shukla, Professor, Computer Science and Engineering, IIT- Kanpur and Mr. Anand Venkatnarayanan, Strategic Advisor, DeepStrat. The technical brief has been edited by Mr. Pranav Bhaskar Tiwari, Programme Manager, The Dialogue™.

Abstract

With the increase in the perpetration of cybercrimes like fake news proliferation, child sexual abuse material, and online drug trade, behind the veneer of encryption-enabled anonymity, the demand to find those using encrypted services for nefarious purposes has also risen. This technical brief aims to explain the core features of end-to-end encryption (E2EE) technology and then assesses the feasibility to deploy two methods proposed in India to catch bad actors using E2EE platforms.

Firstly, the brief initiates with an explanation of how E2EE functions.
Secondly, after a discussion on the core features of E2EE technology, the brief explains the proposal submitted by Professor V Kamakoti before the Madras High Court to trace bad actors on E2EE platforms. It also identifies the key challenges associated with the proposals of Professor V Kamakoti, including privacy, deniability, feasibility, and false implications.
Thirdly, the working of the more recent 'originator traceability' proposal envisaged in the IT Rules 2021 is analysed. It also identifies the key challenges associated with the originator traceability proposal including privacy, feasibility, mass surveillance, global repercussions, and false implications.
Fourthly, it concludes that neither of the proposals can be deployed and identifies privacy respecting alternatives. Lastly, it recommends legislating a surveillance law with procedures for seamless sharing of data between platform and the law enforcement, building meta data analysis capabilities of law enforcement agencies, and not enforcing originator traceability.

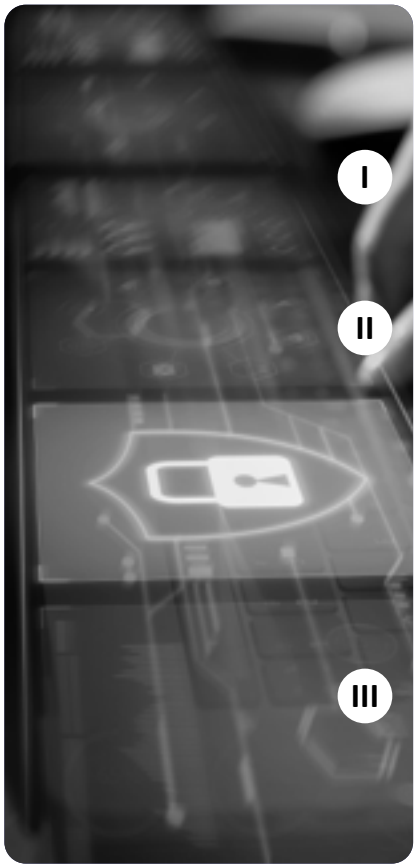

Table of Content

How End-to-End Encryption Works

End-to-end encryption (E2EE) is one the most popular approaches to protect users' digital communications. It prevents service providers as well as third parties from accessing and reading message content. In recent years we have seen a range of communication platforms move towards this technology, with the promise of increased user privacy.

1. Functional Aspects

E2EE, as the name suggests, focuses on encryption at endpoints of communication. Instead of a message being transported to a server and then being encrypted, E2EE encrypts the message within the sender's device, converting plain text into cipher text. Only users who possess a decryption key can decipher, or decrypt, the message into plaintext.

E2EE, as seen on communication platforms, predominantly makes use of both, a*symmetric key cryptography*, where different keys (a public key, and a private key) are used to encrypt and decrypt messages, and *symmetric key cryptography*, which makes use of the same key. In the former, each message sent generates a pair of keys (a public key and a private key), which in tandem with the application, takes care of encryption and decryption within the communicating device itself. With its two keys, this mode keeps intermediaries from accessing the key and decrypting the message. In *symmetric key cryptography*, the same key is used to encrypt and decrypt contents. However, in this scenario, the key itself must be transported securely and may be vulnerable to interception. The Signal protocol used by Signal Foundation and WhatsApp is much more advanced, uses a combination of symmetric and asymmetric key cryptography, and the double ratchet mechanism, which continuously discards encryption keys after a set period.

2. Core Features

Having briefly explored the working of an E2EE enabled communication, it is necessary to explore the factors due to which it has currently become the gold standard for privacy.

- **Dynamic Keys:** The constant creation and discarding of keys, makes sure that communication remains private in every session. It also ensures that if a key is compromised, it does not impact past or future communication which is governed by a separate key.
- **Integrity:** Messages cannot be modified in transit.
- **Confidentiality:** Only the sender and recipient are fully aware of the contents of the message.

- **Cryptographic Deniability:** In communications, offline deniability refers to the ability to "a-posteriori deny having participated in a particular communication session." In the context of E2EE, as the key is known to only the sender and the recipient, a third-party entity can never fully point out which one of the two had sent it. Moreover, in the Signal protocol used by Signal Foundation and WhatsApp, the one-time dynamic keys are unsigned. Therefore, anyone can easily forge an entire conversation that never really occurred. Accordingly, it is cryptographically impossible to attribute who sent a message to whom.

Analysing Professor Kamakoti's Proposals

In 2019, a Public Interest Litigation was filed before the Madras High Court that sought the linking of social media accounts with government authorised identity proofs. The court rejected this possibility on account of its inconsistency with the earlier rulings of the Apex court. However, during the course of the discussion, the State of Tamil Nadu contended the need for 'identifying' the problem makers on encrypted platforms which led to the court seeking expert inputs on the technological feasibility of introducing traceability on encrypted platforms like WhatsApp. In response, Professor V. Kamakoti submitted two proposals.

1. Professor Kamakoti's Proposals

- **The First Proposal:** This proposal stipulates that *WhatsApp may embed sender information in an open format*, where originator information is an innate part of each encrypted message. This would mean that each recipient of a WhatsApp message or forward would get to know the identity of the person who originally sent the message. As part of this proposal, the encryption of originator information happens on the sender's device, and the corresponding decryption happens at the receiver's device.

- **The Second Proposal:** This proposal stipulates that *WhatsApp may encrypt the sender information*, where the originator information continues to travel with each message, but the recipient is not able to view it. However, this encrypted information could be revealed by WhatsApp, whenever demanded per the procedure established by law. As part of this proposal, each such encryption involves asymmetric cryptography. The originator information is encrypted using a public key, while the corresponding private key for decrypting the information is escrowed by WhatsApp.

2. Challenges associated with Professor Kamakoti's Proposals

While Professor Kamakoti's proposals seek to address a growing conflict between privacy and security, there are several challenges associated with them, having serious repercussions. The proposals are also inconsistent with the technological reality of E2EE, apart from concerns of privacy, deniability, feasibility, and false implications. A concise exploration of these challenges now follows.

i. Erodes user privacy

The incorporation of any kind of digital signatures on messages related to sender/originator information would defeat the privacy guarantee currently offered by E2EE enabled communication platforms. The idea of E2EE is based on the premise that only the sender and the recipient are fully aware of the authenticity of messages, and the platforms have zero access to message contents. However, once the originator information includes decryptable information (either with platforms or recipients), it creates a considerable risk of exposure. Such an incremental change risks the privacy of all users on the platform. Another privacy concern arises from forwarding unencrypted originator details on forwards, exposing unsuspecting senders to a lot more recipients.

All Indian users are entitled to the reasonable expectation of informational privacy. Even those sending a message to a single user without the intention of making the message viral would bear the risk of their name being associated with the message at the will of the receiver. Under the proposed system, to catch a very small percentage of potential law breakers, the privacy of all is trampled upon. This could also have a chilling effect on the free speech of journalists and dissenters.

ii. Overlooks technological design of E2EE

The previous section explained how one of the advantages of modern E2EE was the dynamic interplay of symmetric, and public key cryptography, alongside constant creation and discarding of keys. However, Professor Kamakoti's proposals rely heavily on the assumption that platforms use only public key cryptography, which is not the case for platforms using the Signal Protocol.

Cryptographic deniability allows the sender and the receiver to enjoy deniability from having participated in a communication session. But the above proposals, by way of including originator information in messages, weaken this privilege. Thus, while the contents of the message may be private, the possibility of exposure and implication stays. Similarly, the Telecom Regulatory Authority of India in its recommendations to the Department of Telecommunications notes that the security architecture of E2EE platforms should not be tinkered with, as it may render the entire user base susceptible to vulnerabilities.

iii. Cannot track the absolute originator & also falsely implicate

The proposals do not account for the possibility of someone being wrongly identified as an originator. While this method could enjoy a relatively higher success rate in direct forwards, it doesn't account for a message being copy-pasted (or being screenshot) from another platform and then sent. In this case, the sender is not the same as the absolute originator but an originator relative to the platform. This may lead to him/her being falsely implicated, in the context of maliciously worded messages, even if the same was shared to create awareness, or for journalistic or academic purposes.

iv. Can be circumvented

While the proposal may be effective to catch a low hanging fruit, it can be easily circumvented. Some mechanisms of possibly achieving the same are listed below:

- **Creation of or shifting to new E2EE platforms:** The Signal Protocol is publicly available on GitHub and it is easy to create another encrypted messenger. Bad Actors would easily switch to such alternatives, when traceability is deployed on commercial communication applications.

- **Modified Apps:** It is possible to reverse-engineer an app to create a modified version wherein the metadata about originator information would be missing.

- **Creating Alias:** WhatsApp account authentication is based on OTPs sent to registered phone numbers. Modified versions of WhatsApp, coupled with cheap, disposable phones, would ultimately render the identification exercise ineffective. The ease of acquiring phone numbers anonymously, in addition to the growth of various Voice over Internet Protocol (VoIP) enabled communication platforms, further complicates the identification of originators.Internet Protocol (VoIP) enabled communication platforms, further complicates the identification of originators.

v. Investigative value but no evidentiary value

Cryptographic deniability is a core feature of E2EE. This, in simple terms, entails that if Abhay receives a message from Binoy, then Abhay can be absolutely sure that it was sent by Binoy and not forged by a third party, yet Abhay cannot prove to anyone that Binoy had sent this message. This happens because the sender and receiver(s) (Abhay and Binoy) utilise a shared secret known only to them. This shared secret is used to create an encryption key that encrypts the message. Now given that the encryption key is only known to Abhay and Binoy, they themselves can be sure who sent a message to whom but cannot prove the same to someone else as both of them have the capability to create that conversation.

Further, the Signal Protocol now uses unsigned one-time keys. This entails that anyone can now access Abhay's public key (A) and make up an ephemeral keypair for the same (a) thereafter combine it with their own identity key B and ephemeral key (b) and produce a fake conversation that never happened. To explain simply, the signal protocol allows Binoy to whisper in Abhay's ears cryptographically such that Abhay can hear everything and know Binoy told him that yet not prove that it was indeed Binoy.

Moreover, there is no way to establish if a person is an originator relative to a platform (as the person may have copied the content from social media and then shared it on an E2EE messaging platform) or an absolute originator (who created the content himself). Accordingly, any evidence collected via this method may be useful for investigative purposes, yet it does not hold evidentiary value before the Court.

Analysing the Originator Traceability Mandate per the IT Rules 2021

1. How Originator Traceability Functions

Per the recent Originator Traceability mandate under the IT Rules 2021, an encrypted messaging service provider is expected to store the hash value of every message on their platform by Indian citizens. Hashing can be understood as a fingerprint of a message. Consider this example:

Herein the hashing algorithm is applied to content data a unique alpha-numeric hash value is generated. The probability of some other piece of content to create this alpha-numeric hash value is highly unlikely. It is important to note that hashing is a one-way process, i.e., we cannot use '**1207DHF52BN**' to deduce the actual message on which the hashing algorithm was applied.

Per the proposed method, the law enforcement agency will approach the encrypted messaging service provider with a viral text message and ask them to convert them by running the hashing algorithm to get a hash value. Thereafter they search their database with the hash values of the messages sent by every Indian user for a match and give details of the person who first sent the message with the hash value presented to them.

2. Challenges Associated with deploying the Originator Traceability Mandate

i. Overlooks technological design of E2EE

Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 requires that any significant social media intermediary that provides messaging "shall enable the identification of the first originator of the information on its computer resource", in response to a judicial order. However, this concept of enabling identification is antithetical to modern-day encryption systems used to protect privacy-E2EE used by messaging and other communication platforms. In an E2EE architecture like WhatsApp, message contents and calls are only shared with the intended recipient and platforms do not have access to it. However, traceability forces messaging platforms to keep track of billions of messages, and their contents, sent every day. Traceability requires messaging services to store information that can be used to ascertain the content of people's messages, in the process breaking the technological guarantee that E2EE provides.

What complicates matters is that tracing even one message would involve tracing every message on the platform. This will render all the users of the platform vulnerable and will be contrary to the fundamental service provided by the platform which is providing secure private messaging through E2EE.

ii. Traceability reverses technological developments on Privacy

Recent developments in technology have focused on key aspects of privacy such as data minimization, and purpose limitation. However, with the current mandate, there is a risk of going backwards on the progress made on the above fronts. It would force communication platforms to enable a mechanism for easily retrieving message information, in the process also forcing it to store extra information about the data. Moreover, knowing that a fingerprint of every message shared on the platform is maintained casts a chilling effect on the free speech of the citizenry. Further, with no certainty about investigations, platforms have no clear purpose to keep a hold of the above data. There would be a substantial erosion of the element of voluntariness, as E2EE technologies are not designed to offer conditional privacy.

iii. Traceability may be a domestic mandate with global repercussions

What the traceability mandate overlooks is that E2EE is a system-level design and one that is the same for all users of an application. Forcing communication platforms to enable tracing of the first originator cannot be a country-specific change due to multiple reasons. First, the likes of Signal and WhatsApp have a common application interface and design, and these are not country-specific. Secondly, these platforms enable cross border communication between users. Such a law in India would put into danger the privacy of all users on these platforms, irrespective of the country. It would also lead to the fragmentation of the internet, with demands for country-specific versions of technologies. Such a scenario would ultimately result in a great deal of disharmony and incompatibility of regulations.

iv. Fosters Dystopian Surveillance

The idea behind E2EE was that the users need not trust anyone, not even the platform. Nobody should have access to their content data. The traceability mandate forces E2EE messaging platforms to store a fingerprint of all messages sent on the platform. There is a lot that can be done from such a humongous amount of dataset.

- **Corporate Surveillance:** An E2EE messaging platform never had access to hash values of content data. Such a platform may run its hashing algorithm on commonly used phrases and search it for matches and map trends based on geography, time, frequency, among other metrics and utilise it for commercial purposes.

- **State Surveillance:** The State may utilise this unchecked power to conduct mass surveillance without surveillance legislation to institute checks and balances.

- **Espionage & Hacking:** The entire dataset is essentially a honeypot, which if attacked by bad actors would compromise the security of all users as the bad actors would be able to map trends and track users too.

v. Cannot track the absolute originator

Like challenges in Professor Kamakoti's proposal, the traceability mandate per the IT Rules, 2021 cannot always ascertain who the absolute originator is, and the process does not meet the evidentiary burden of proof as required by law.

vi. The slippery slope to perceptual hashing

As explained before, post running a hashing algorithm on a message an alphanumeric hash value is generated. Even a minute change in the message content would lead to an astronomical change in the hash value. Accordingly, some experts may rely on perceptual hashing, wherein the platform does not look for an exact match but a similar one. This leads to severe implications at two levels.

- If a bad actor gets to know which hashing algorithm is used by WhatsApp, then it may use it to manually match the hash value of a seemingly innocuous picture, or meme, with that of a known child sexual imagery to falsely implicate an innocent person

- Moreover, we would be unnecessarily giving the platforms the power to run perceptual hash matches and surveil the citizenry. It would be even more concerning if those companies were headquartered in another country. The platforms never enjoyed this power as they never had the hash value of each message sent on their platform.

Conclusion

1. Worsening the symptom and more

While technical solutions offered may help curb the virality of fake news to some extent, it is a fact that many share fake news on unencrypted platforms. In the guise of preventing the spread of fake news, a solution that does not prevent it but only worsens privacy trade-offs for the citizenry, is not a desirable approach.

2. Privacy respecting alternatives exist

For instance, in response to a request under the Freedom of Information Act, on what information do messaging platforms can reveal to law enforcement , the FBI shared the datasets available with the messaging platforms tabulated below:

App	Legal process & additional details
Apple iMessage	• **Message content:** limited. • **Subpoena:** can render basic subscriber information. • **18 USC §2703(d):** can render 25 days of iMessage lookups to and from a target number. • **Pen Register:** no capability. • **Search Warrant:** can render backups of a target device; if target uses iCloud backup, theencryption keys should also be provided with content return can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud'
Line	• **Message content: limited.** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc. • Information on usage. • Maximum of seven days worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed).
Signal	• **No message content.** • Date and time a user registered. • Last date of a user's connectivity to the service.
Telegram	• **No message content.** • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities.
Threema	• **No message content.** • Hash of phone number and email address, if provided by user. • Push Token, if push service is used. • Public Key. • Date (no time) of Threema ID creation. • Date (no time) of last login.
Viber	• **No message content.** • Provides account (i.e. phone number)) registration data and IP address at time of creation. • Message History: time, date, source number, and destination number.
WeChat	• **No message content.** • Accepts account preservation letters and subpoenas, but cannot provide records for accounts created in China. • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active.
WhatsApp	• **Message content limited.** • **Subpoena:** can render basic subscriber records. • **Court order:** Subpoena return as well as information like blocked users. • **Search warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts. • **Pen register:** Sent every 15 minutes, provides source and destination for each message. If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content.
Wickr	• **No message content.** • Date and time account created. • Type of device(s) app installed on. • Date of last use. • Total Number of messages. • Number of external IDs (email addresses and phone numbers) connected to the account, but not to plaintext external IDs themselves. • Avatar image. • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information). • Wickr Version number.

Subsriber Data | Message Sender Receiver Data | Deivice Backup | IP Address | Encryption Keys | Data/Time Information | Registration Time data | User's Contact

Moreover, the success of Project Trojan Shield, wherein the FBI, along with other law enforcement agencies, targeted only bad actors by planting a compromised encrypted App AN0M and arrested over 800 criminals, explains what traditional surveillance manoeuvres coupled with law enforcement's ingenuity can achieve.

On similar lines, out of the 208 law enforcement agency officials interviewed in the SIRIUS EU Digital Evidence Situation Report (2021), only 20% selected 'content data' amongst the top three data sets required for investigation. For the remaining 80%, the following metadata like phone number, registration details, IP address etc. was sufficient.

Given the meta data shared by various encrypted messaging platforms with law enforcement, and the SURIUS EU Digital Evidence Report establishing that it is indeed meta data that they need the most complimented with success of project trojan shield, it is evident that security interests can be met without weakening encryption.

Recommendation

1. Do not enforce traceability.

Enforcing traceability in the way proposed by Professor Kamakoti or as envisaged in the IT Rules, 2021 has deleterious consequences for the citizenry's privacy at large as it will break end-to-end encryption and guarantees provided by the technology.

2. Legislate a surveillance law with procedures for seamless sharing of data between platform and the law enforcement.

State surveillance practices need to be regulated by clear, purposive, proportionate, and comprehensive legislation. Such a law must allow for a seamless sharing mechanism between platforms and LEAs and ensure legislative or judicial oversight. These laws should not compel decryption and attach liabilities for failing to do the same, where such decryption is not technically possible without fundamentally altering the architecture of the platform.

3. Capacity building of law enforcement agencies to enhance their meta data analysis capabilities.

Our current capacity for metadata analysis needs to be enhanced through a concerted effort by the government. As explicated in the foregoing parts, metadata is enough for actionable leads, we must move towards building police capacity to actualize this potential.

The Dialogue™
INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Recommended citation: The Dialogue. (2022, March). Analysing the technical workarounds to end-to-end encryption. New Delhi.

https://thedialogue.co
https://www.linkedin.com/company/the-dialogue-india/
@_DialogueIndia
https://www.facebook.com/TheDialogueIndia
@thedialogue_official