Online Content-Tracing Origins: RSTV – Big Picture

Anchor: Frank Rausan Pereira

Guests: Jiten Jain, Online Content Analyst; Karnika Seth, Advocate, Cyber Law; Prashant Mali, Cyber & Privacy Policy Expert; Munish Sharma, Consultant, IDSA.

Larger Background

- The government is finalizing new IT rules for social media companies that would mandate traceability of the originator of information on social media platforms and removal of malicious content within 24 hours of notice.
- The proposed new norms include the deployment of technology-based automated tools or appropriate mechanisms for proactively identifying and removing or disabling public access to unlawful information or content.
- Messaging giant WhatsApp has, in the past, drawn flak from the government on the issue of message traceability.
    - The government has been asking the Facebook-owned company to find ways to identify originators of rogue messages but the US-based firm has resisted the demand citing privacy concerns.

Tracking the origin of a message

- It is easier to track the source of a message on an open platform such as Facebook or Twitter than on a closed platform such as WhatsApp. This is due to the fact that most of the closed platforms make use of end to end encryption for their content.
    - End to end encryption indicates that the application doesn't store or monitor the content being shared. The information regarding the content would be exclusive to the individuals involved in the conversation.
- The government has suggested that a unique ID be created for photos and videos to allow traceability to the origin, instead of sharing information regarding the content, as most of the riots happening are initiated by a photo or a video hurting the sentiments of a particular set of people.
    - The metadata would reflect the size and origin IP address of the message. That is why the government wants access to the metadata of the message.
    - A content ID could be created for the photos and videos shared, so that it is trackable. The ID can be a unique ID or a hash value.
    - PhotoDNA of Microsoft (a technology that aids in finding and removing known images of child exploitation) can also be used for the purpose of tracking the origin of messages. The software utilizes hash values of the pictures and videos to identify similar images.

Availability of technology

- The availability of technology to trace the origin of a message has never been the issue. The issue lies in the compromise of the privacy of an individual and whether the closed platforms such as Whatsapp comply with the laws in the country.
- There are multiple ways that the origin of an encrypted message could be tracked.
    - Encryption is present in layers when a message is being forwarded. So there can be technical possibilities to isolate the origin of a message.
- Whatsapp admits to the availability of technologies that could help track the encrypted messages, however, they refuse to use such technologies stating that it would be a violation of their own privacy policies and business models.

- They feel that if they have to comply with the IT rules of one country, it will open a pandora's box to comply with many other jurisdictions.

Legal provisions for tracking the origin of messages

- When it is a question of national interest and security of the country, the open platforms will have to comply with the law of the land.
  - China and Russia banned Whatsapp, simply because the platform did not comply with their local laws.
- Open-ended platforms need to comply with the government in case a tangible and justifiable reason is provided for requesting access to the information.
  - For example, when interception of calls are required, a proper order should be given by the Home Ministry, as per section 5(2) of the Indian Telegraph Act of 1885.
- There are no pre-existing privacy laws in India apart from the right to privacy upheld by the Supreme Court.
  - The Supreme Court has ruled that there is a fundamental right to privacy under the Indian constitution, establishing that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty". Read more on the Right to Life at the linked article.
- There have to be changes made to the existing laws wherein metadata is admissible as direct evidence for a deduction, because metadata by itself can have a lot of discrepancies.
- The government has to focus on the modification of certain laws and the strict implementation of the existing laws for a solution, such as:
  - The **Information and Technology Act of 2000** has been there for so many years now, and yet has not been enforced in a stringent manner.
  - Section 65B of the Evidence Act defines how to produce electronic evidence which can be used to file a complaint, but the companies will have to comply.

Privacy concerns Vs State's interest

- There is a fine line between privacy concerns, fundamental rights, and the state's interests.
- If security requirements are prioritized, then privacy concerns take a back seat.
- Multiple events such as- the London Bridge attack, were stipulated to have been planned on WhatsApp and the authorities could not prevent it due to the inaccessibility of the encrypted messages.
- The lack of awareness about encryption in the country acts as an added advantage for such companies.
- Although granted by the Supreme Court, Right to Privacy is yet to be established by the law.
- The question is of privacy concerns and the sovereign control of the state over most of the communication.
  - **Draft Personal Data Protection Bill** if implemented will completely change the environment.
    - "The Bill regulates the processing of personal data of individuals (data principals) by government and private entities (data fiduciaries) incorporated in India and abroad. Processing is allowed if the individual gives consent, or in a medical emergency, or by the State for providing benefits."
- Since India doesn't have a deterrent action in place, foreign companies tend to exploit the Indian market at the expense of national security.

Challenges

- Implementation challenges: There are multiple challenges which could prove to be a hurdle in the implementation of laws for cybersecurity. A few examples are:

  - IT Act of 2000 has to be updated to the current scenario.
  - The cybersecurity infrastructure and cyber warfare need to be worked upon.
  - Stringent deterrent laws have to be put in place for the closed platform companies such as WhatsApp.
  - At the behest of National Security, an individual's privacy should not be breached. No country has been able to find a solution but to outrightly ban these platforms.
- Working out a model by fine-tuning the existing framework and strengthening it to ensure that the implementation is strong, is one of the challenges. Technical and legal solutions to the problems have to be found. One solution cannot be applicable to different types of problems.
- Awareness regarding encryption and its functionality has to be created in public.

Way Forward

- **Law needs to evolve:** The problem of privacy and state interests has to be looked at in a three-dimensional manner.
  - The first dimension is the law, the second dimension constitutes technology and the third dimension would be human privacy.
  - We have to modify certain laws and ensure the stringent enforcement of the other existing laws.
  - The existing laws have to be interpreted in different perspectives for the benefit of the national security of the country.
  - For example, the e-summons implementation took eight years and it was first implemented by the Delhi High Court. According to the law, if a read- receipt has been obtained for the e-summon it is treated as a delivered summon.
- **Lack of informed debate in society:** The government while talking about social media monitoring, does not refer to the personal chats in social media but to the monitoring of the open content available.
  - Awareness needs to be spread regarding encryption and the monitoring of the content in the country so that the citizens could be active participants in helping the government weed out fake messages or messages which could seemingly compromise the security of the country.
- **State before individual:** Privacy of a nation and the privacy of a society is of greater importance than the right to privacy of an individual.
  - In certain situations, to protect the privacy of the state, the privacy of an individual may have to be suspended. The privacy of an individual cannot be an absolute right when national security requires it to be breached.
- **Usage of technology:** There are enough technologies available to be used for the purpose of tracking the origins of a message which may threaten the security of the country.
  - The open platform companies will have to accept that there are technical possibilities of recovering the origins of an encrypted message under certain circumstances and take necessary actions to accommodate the same.
    - Encryption is one of the best methods to ensure the protection of the privacy of an individual, however, there has to be sufficient awareness created amongst the public regarding it.

Rules with respect to the traceability of the originator of information on social media platforms must help the law enforcement agencies and enable them to conduct investigation in a better manner. With privacy laws being strengthened, there would be several provisions that social media platforms would have to comply with. The whole idea is to trace the origin of the messages similar to call records being tracked. India's model is what the world is looking for.