Ending encryption

Traceability

1. Barely a day before the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 came into force, WhatsApp moved the Delhi High Court against the rules — specifically the one that mandates that a "significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order".
2. Given the specification that a "significant social media intermediary" is one with more than 50 lakh registered users, WhatsApp's messenger service would clearly be affected.
3. WhatsApp's contention is that for compliance and traceability, it would have to break its end-to-end encryption service that allows messages to be read-only by the sender and the receiver.
4. Its argument is that the encryption feature allows for privacy protections and breaking it would mean a violation of privacy. The question to be asked is whether the traceability guidelines (by breaking encryption) are vital to law enforcement in cases of harmful content.
5. A release by the Ministry of Electronics and IT has said that the traceability measure will be used by law enforcement as the "last resort" and will come by only in specific situations, such as "for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India... or child sexual abuse material, punishable with imprisonment...."
6. The assertion suggests that this requirement is in line with the Puttaswamy judgment that clarified that any restriction to the right of privacy must be necessary, proportionate and include safeguards against abuse.

Existing Provisions:

1. But the Government, as the law stands now, can already seek access to encrypted data under Section 69(3) of the IT Act, and Rules 17 and 13 of the 2009 Surveillance Rules that require intermediaries to assist with decryption

when they have the technical ability to do so and when law enforcement has no other alternative.

2. Besides, it can still seek unencrypted data, metadata and digital trails from intermediaries such as WhatsApp.
3. The trouble with enforcing traceability is that without safeguards such as having an independent or judicial oversight, government agencies could seek any user's identity on vague grounds and this could compromise the anonymity of whistle-blowers and journalistic sources, who can claim to be acting in the public interest.
4. WhatsApp's contention that "requiring messaging apps to 'trace' chats is the equivalent of asking us to keep a fingerprint of every single message sent... and fundamentally undermines the right to privacy" is, therefore, not hyperbole.
5. If anything, the Government needs to revisit its position on traceability commitments of intermediaries and instead revise the IT Act, 2000 in line with existing global best practices besides legislating the long-pending Data Protection Bill.

Power play to bring the digital ecosystem to heel

New Rules:

1. Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposes an obligation on significant social media intermediaries providing a messaging function, to ensure traceability of the originator of information on their platforms.
2. A failure to implement this obligation can lead to intermediaries being held responsible for illicit content on their platforms.

Proportionality test:

1. The Government primarily relies on the argument that: privacy is not an absolute right, and that the traceability obligation is proportionate, and sufficiently restricted.
2. Notably, the new Rules mandate traceability only in the case of significant social media intermediaries that provide messaging services (i.e. those that

meet a user threshold of 50 lakh users, which WhatsApp does), subject to an order being passed by a court or government agency and only in the absence of any alternatives.

3. While it is indeed true that privacy is not an absolute right, the Supreme Court of India in the two K.S. Puttaswamy decisions (of 2017 and 2018) has clarified that any restriction on this right must be necessary, proportionate and include safeguards against abuse.

On traceability as a feature

1. However, as we argue in a recent paper, a general obligation to enable traceability as a systemic feature across certain types of digital services is neither suitable nor proportionate.
2. Additionally, the Rules lack effective safeguards in that they fail to provide any system of independent oversight over tracing requests made by the executive.
3. This allows government agencies the ability to seek any messaging user's identity, virtually at will. However, anonymity from the government can be important, particularly in contexts of journalistic source protection and for whistle-blowers. Therefore, deciding whether to remove anonymity requires the application of an independent judicial mind.
4. In applying the Puttaswamy tests to the Rules, one must examine not just whether the weakening of encryption systems will lead to some law enforcement gains, but whether these are worth the costs involved.
5. Thus, one must consider the impacts of such a measure on the general digital ecosystem in terms of the overall cybersecurity and privacy problems such an obligation could create.
6. There is a near-universal consensus that mandating the presence of backdoors or weakening encryption generally — which a traceability mandate would do — would compromise the privacy and security of all individuals at all times, despite no illegal activity on their part, and would create a presumption of criminality.

Other means exist

1. In any event, the Government already has numerous alternative means of securing relevant information to investigate online offences including by accessing unencrypted data such as metadata, and other digital trails from intermediaries.
2. Therefore, the present Rules attempt to shorten the investigative process, even though, as we argue in our paper, law enforcement is not supposed to be an entirely frictionless process. Frictionless processes lacking sufficient checks will merely incentivise fishing expeditions by government agencies.
3. Further, the surveillance powers of the Government are in any case vast and overreaching, recognised even by Justice B.N. Srikrishna Committee report of 2018.
4. Importantly, the Government already has the ability to access encrypted data under the IT Act. Notably, Section 69(3) of the Information Technology Act and Rules 17 and 13 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 require intermediaries to assist with decryption where they have the technical ability to do so, and where law enforcement has no alternatives.
5. The newly notified Rules go well beyond current provisions in the law by seeking to punish relevant intermediaries for failing to adequately weaken encryption systems.

Recognising caste-based violence against women

Highlights:

1. On the heels of the Hathras crime came a new judgment of the Supreme Court (Patan Jamal Vali v. State of Andhra Pradesh) addressing the intersectionality of caste, gender and disability.
2. In this case, the victim of sexual assault was a blind 22-year-old Dalit woman. The trial court and the High Court had convicted the accused for rape under Section 376 of the Indian Penal Code (IPC), and under Section 3(2)(v) of the PoA Act, and sentenced him to life imprisonment.

3. The Supreme Court confirmed the conviction and the punishment for rape under the IPC but set aside the conviction under the PoA Act.
4. On the one hand, this judgment is a huge step forward as the court used the opportunity to bring recognition to intersectional discrimination faced by women on the grounds of sex, caste and disability. However, by setting aside the conviction under the PoA Act, it is like many other previous judgments of the Supreme Court.

The intersectional approach

1. Let us focus on the positive aspects first. The Supreme Court, in a first, elaborated on the need for an intersectional approach, to take into account the multiple marginalities that the victim faced.
2. The court recognised that when the identity of a woman intersects with her caste, class, religion, disability and sexual orientation, she may face violence and discrimination due to two or more grounds.
3. It said we need to understand how multiple sources of oppression operated cumulatively to produce a specific experience of subordination for the blind Dalit woman.
4. Placing special emphasis on making the criminal justice system more responsive to women with disabilities facing sexual assault, the court also laid down directions to train judges, the police and prosecutors to be sensitised in such cases.

The PoA Act

1. But despite using an intersectional lens, the court set aside the conviction under the PoA Act.
2. The PoA Act was enacted to address atrocities against persons from SC and ST communities and was amended in 2015 to specifically recognise more atrocities against Dalit and Adivasi women including sexual assault, sexual harassment and Devadasi dedication.
3. Section 3(2)(v) states that if any person not being an SC/ST member commits an offence under the IPC punishable with imprisonment of 10 years or more against a person **knowing** that such a person is from an SC/ST community, he shall be punishable with imprisonment for life and with fine.

4. In cases of sexual violence against Dalit and Adivasi women, courts have almost consistently set aside convictions under the PoA Act. In 2006 in Ramdas and Others v. the State of Maharashtra, where a Dalit minor girl was raped, the Supreme Court set aside the conviction under the PoA Act stating that the mere fact that the victim happened to be a woman who was a member of an SC community would not attract the PoA Act.
5. There are several precedents insisting on an unrealistic burden of proof. This issue needs to be referred to a larger bench to take a different view.

Undermining The PoA Act

1. It matters because the repeated setting aside of convictions under the PoA Act bolsters the allegations that the law is misused and amounts to the erasure of caste-based violence faced by women.
2. Further, as stated in the recent Parliamentary Standing Committee Report on Atrocities and Crimes against Women and Children, the "high acquittal rate motivates and boosts the confidence of dominant and powerful communities for continued perpetration".
3. This judgment was a missed opportunity for the court to use intersectionality to uphold the conviction under the PoA Act or refer the matter to a larger bench if needed.
4. We need to stop hiding behind smokescreens of hyper-technicality of evidence and recognise caste-based violence against women when it stares us in the face.
5. Else, our caste discrimination laws will be rendered toothless. If intersectionality theory mattered in this case, it should have influenced an interpretation of the PoA Act that reflects the lived experiences of women facing sexual violence.

Burden of proof

1. In all these judgments, the court held that there was no evidence to show that the accused committed sexual assault on the ground that the victim was a member of an SC/ST community.
2. The only evidence that can be led is that the victim was from an SC/ST community and that the accused was aware of that.

3. When a woman is from a marginalised caste and is disabled, she faces discrimination due to her sex, caste/tribe and disability, all of which render her vulnerable to sexual violence. This is what intersectionality theory requires us to recognise.