Source : www.thehindu.com Date : 2021-06-04

INFORMATION TECHNOLOGY RULES: A CASE OF OVERREACH?

Relevant for: Indian Polity | Topic: Judiciary in India: its Structure, Organization & Functioning, Judges of SC & High Courts, Judgments and related Issues

Last week, WhatsApp decided to legally challenge one of India's new Information Technology rules which requires messaging platforms to help investigative agencies in identifying the originator of problematic messages. WhatsApp reckons this would break end-to-end encryption and undermine people's right to privacy. The government responded saying it is committed to ensuring the right of privacy for all its citizens, and that it also has to ensure national security. Have these new rules been framed to adequately address the privacy versus security balance, especially in the context of social media intermediaries such as WhatsApp? ***Rishab Bailey*** *and* ***Parminder Jeet Singh*** *discuss this question in a conversation moderated by* ***Sriram Srinivasan****. Edited excerpts:*

Rishab Bailey: The short answer is that every provision of the new IT rules is ultra vires the Constitution and the parent IT Act of 2000. The rules only make superficial attempts at balancing privacy and security interests. But it's very clear that security interests are being given primacy over both civil liberty interests as well as economic interests.

IT Rules: a case of overreach? | The Hindu Parley podcast

Keep in mind that the government already has huge powers of surveillance. This was recognised even in the Justice Srikrishna Committee report that accompanied the draft data protection law in 2018. So, rather than seeking to revise these powers, the government is giving itself greater ability to snoop on and interfere with the private lives of citizens. In particular, the traceability obligation in the new rules is problematic because the technical literature on this is nearly universal, in agreeing that this would mean breaking the use of end-to-end encryption for all users on platforms such as WhatsApp.

Also, end-to-end encryption is really needed in the digital economy because data theft and hacking are only increasing in India. There's also an issue of platforms themselves misusing user data. So, ideally, we should be looking to encourage more user-controlled encryption and not limiting this possibility.

Parminder Jeet Singh: I'll start with the points of agreement with Rishab, and that is the context of the way the state has been using its powers in a manner which is becoming very dangerous.

WhatsApp is indulging in anti-user practices: Government

Having said that, we also need to see things in the sense of the fact that our societies are changing from pre-digital to digital societies, and many fundamental structural changes have to take place. Among those are also the levers of law enforcement, required in the new context. Second, as Justice Srikrishna said, a new law should be brought out, which discusses the rationale, gives good institutional checks and balances, and then places this significant and new legal possibility for the law enforcement in that context. Third, the biggest problem with WhatsApp is that it is a private communication channel, and after certain virality, becomes public. So, what happens is that with the originator or traceability mandate, anybody who's writing a personal message to his or her friend is afraid that though they are giving an analysis which, in a private sense, is not criminal, but it could be criminal in a public sense. So, how do

you balance the private and the public part of it is a concern.

Rishab Bailey: It's unclear why you need to have a specific mandate for traceability. Yes, metadata as well as other forms of unencrypted data can be accessed by law enforcement. Keep in mind also that the current law in India also allows the government to request decryption of data where it's held by an intermediary or where the intermediary holds the private encryption key.

Explained | Why is WhatsApp opposed to traceability?

Rishab Bailey: That is actually the fundamental issue here, which is that the government wants you to move away from encryption controlled by the users to encryption done by the intermediary itself. If the intermediary is controlling the encryption keys, the government can just go to them and ask for this information.

Parminder Jeet Singh: I don't believe traceability of encrypted messages requires breaking encryption. The metadata, which carries many layers of information already, including a counter that tells you that the message has crossed a certain limit of virality, can be a good enough place to lock the originator of every message when it is created. Now, you can always say it doesn't go with my method of encryption. But the law does not follow private models of business; private models of business follow the law.

Comment | WhatsApp and its dubious claims

I have been a law enforcement officer, and I can see many situations where there is really almost no other way — I mean you can spend decades of investigation and always find the originator. So, there are examples like somebody sending out a message which is derogatory to, say, Dalits and this goes viral. This is illegal under Indian law. So, what should the law do? A second example relates to systematic election-related manipulation, which has happened in the West on Twitter; in India it happens on WhatsApp. Foreign countries can do it, Indian political cells can be doing in a manner which is illegal. And all these can really be traced when you are able to find an originator. Another example is of obscene pictures, non consensual, intimate pictures (that are shared). And finally, a lot of the wrong kind of content is today leaked on WhatsApp by the police itself, who get access to a lot of digital media when they do investigation. All these require the originator to be found out and these cases are going to keep on multiplying. And just to say I think it could be found out otherwise is not sufficient.

Rishab Bailey: The rule as it's currently drafted is vague, disproportionate, and probably unnecessary. The reasons for which this traceability power can be used are quite broad and therefore capable of misuse. The provision uses the phrase 'security of the state', which unfortunately has virtually come to mean criticising the government in any way. Similarly, to say that this power can be used to detect or prevent an offence basically gives executive authorities free rein to identify people even before an offence has been committed.

Parminder Jeet Singh: This should have been a new law with systemic explanation of intent, purpose, and institutional safeguards. Like now, the court has said that sedition has to be redefined. There are two problematic terms here: 'security of the state' and 'public order'. People are shouting in my street; is it a public order issue? And we need our Supreme Court to define these terms and lay out the law on that.

New IT rules don't apply to us, Google tells Delhi High Court

I am also strongly of the belief that for these kind of cases, executive authority should not be

able to give an order. Only a judicial order, which should insist on the purpose, how you are going to do it, whether the intermediary has been given an opportunity of being able to do it through less intrusive means, which are all the part of the new rules, should allow access to the originator of a message. So, these institutional systems should be in a new law, and the Supreme Court should clarify terms like ‘public order’ and ‘security of the state’.

It will always be an ongoing battle. The powers that a police constable was given during the colonial regime... it is the same power the Indian policeman has in New Delhi and the Toronto policemen have: of arresting people, going into people’s houses. It is the institutional safeguard around those which keep their power in check. The same would apply in the digital arena.

Parminder Jeet Singh: Probably much of it is not of the delegated rule-making level. These kinds of things should go to Parliament and a full-fledged law should be written.

Twitter has to comply with new IT rules for digital media, says Delhi High Court

Rishab Bailey: What has progressively happened over the last few years is that the Section 79 of the IT Act route, and the fact that you can make rules under this, is being used to introduce progressively more onerous obligations, including on many issues where you might actually need regulation. The argument is that all the rules under Section 79 can do is give effect to the main provision. They can’t introduce new offences, they can’t go beyond what the original provision or, in fact, the parent Act itself contemplates.

Rishab Bailey: Actually, every jurisdiction is struggling with the issue of how to deal with the fact that sometimes messages may not be accessible, or data may not be accessible to law enforcement agency. But I don’t think there is a single liberal democracy that actually implements laws mandating traceability in the same way that the new IT rules actually do. This issue of access to encrypted data has come up over the last 25 years in many different countries. Even in the U.S., for instance, it’s been discussed since the mid-1990s. It particularly comes up every five or six years when there’s a terrorist attack or something like that and technology companies say we can’t provide you this data because it’s encrypted. But there have been no laws actually implemented that specifically deal with this issue, largely due to opposition from the technical community as well as civil society and academia.

Editorial | Rules and rulers: On social media curbs

In Australia, fairly wide-ranging powers have been given to the government under a law known as the Telecommunications and Other Legislation Amendment Act. This allows law enforcement to request information and assistance from intermediaries. But even here, they can’t mandate the creation of systemic weaknesses or vulnerabilities.

It’s also important to keep in mind that often, platforms don’t always want to get on the bad side of governments. This might not necessarily apply in the Indian context, because clearly there’s an adversarial position that’s been adopted here. But platforms can also be arm-twisted into building in what’s called weakness by design into their product. For instance, Apple is said to have dropped plans to encrypt its iCloud data because the FBI pressured it. These are bigger questions that need to be discussed, but I don’t think that you will actually find too many countries which have similar provisions in the law.

Parminder Jeet Singh is Executive Director, IT for Change; Rishab Bailey is Technology Policy researcher at the National Institute of Public Finance and Policy

Our code of editorial values

Please enter a valid email address.

To reassure Indian Muslims, the PM needs to state that the govt. will not conduct an exercise like NRC

END