Source : www.thehindu.com Date : 2021-06-01

POWER PLAY TO BRING THE DIGITAL ECOSYSTEM TO HEEL

Relevant for: Science & Technology | Topic: IT, Internet and Communications

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. A failure to implement this obligation can lead to intermediaries being held responsible for illicit content on their platforms. These rules have recently come into effect. Consequently, WhatsApp has filed a petition in the Delhi High Court alleging that the mandate for traceability violates the privacy rights of Indian citizens, by rendering WhatsApp unable to provide encrypted services.

In response, the Government has, through a press release, sought to question the substance and timing of WhatsApp's petition. On scrutiny, however, it appears that the response is misconceived.

The Government primarily relies on the argument that: privacy is not an absolute right, and that the traceability obligation is proportionate, and sufficiently restricted. 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.

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.

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. Additionally, the Rules lack effective safeguards in that they fail to provide any system of independent oversight over tracing requests made by the executive. 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 application of an independent judicial mind.

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. 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. There is 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.

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. 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.

Further, the surveillance powers of the Government are in any case vast and overreaching, recognised even by the Justice B.N. Srikrishna Committee report of 2018. 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. 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.

The Government's press release appears to be well aware that this is in effect what would happen if the traceability mandate were to be imposed. However, it notes that it is the responsibility of intermediaries to find an alternative method to protect user privacy, with or without the use of encryption.

The press release also claims that the new Rules were introduced pursuant to consultation. However, this does not reveal the entire story. The traceability related provision in the draft version of the Rules released in 2018 faced significant opposition from numerous stakeholders, ranging from service providers, academia, and civil society organisations. The new traceability provisions are substantially similar, and carrying out a consultation merely to reject all the views that go against state interests is far from best practice. Ideally, and given the substantive changes made to the 2018 draft (including the addition of several entirely new parts such as those pertaining to regulation of digital news), the new Rules should also have been put through a period of consultation before being notified. . Ideally, the rules should also be accompanied by an explanatory memorandum explaining the rationale for regulation.

Of course, this entire discussion is notwithstanding the fact that the intermediary rules are not the manner or place to go about putting in place new substantive regulation to solve the myriad problems caused by the digital ecosystem. Indeed, the ability of the government to issue progressively more onerous obligations under the guise of "due diligence" requirements under Section 79 of the IT Act (which in essence, deals with the issue of take-down of illegal content) must be subject to judicial scrutiny.

Overall, however, it is clear that the move by the Government is part of a broader power play against foreign-based technology companies, and to generally bring the digital ecosystem to heel. While, undoubtedly, there are numerous problems in the digital ecosystem that are often exacerbated or indeed created by the way intermediaries function, ill-considered regulation of the sort represented by the new intermediary rules — which appear to have little basis in evidence or care for consequences —– is not the way forward. Indeed, the only truly democratic and relatively long-term solution would be for legislative change along multiple avenues, including in the form of revising and reforming the now antiquated IT Act, 2000.

Rishab Bailey is a technology policy researcher at the National Institute of Public Finance and Policy, New Delhi. Vrinda Bhandari, a lawyer practising in Delhi, was involved in challenging the Intermediary Guideline Rules 2021 before the Kerala High Court

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

END