Source : www.indianexpress.com Date : 2019-10-11

PRIVACY RIGHTS & WRONGS

Relevant for: Security Related Matters | Topic: Role of Media and Social Networking Sites in internal security challenges

A year ago, the Telecom Regulatory Authority of India (TRAI) had commenced a process of consultations to bring over the top (OTT) services like WhatsApp and Telegram under “lawful interception”. Now, it is reported to be ready to submit recommendations to the Department of Telecommunications. The objective of the exercise is public security, since criminals and terrorists are known to use the end-to-end encryption offered by such services to fly under the radar. Parity has always been an issue, too, since telecom providers complain that they are regulated and must respond to requests for information from governments and agencies, while the OTT sector is untrammelled. However, the most significant question remains unanswered: Is interception technologically feasible, at all?

Technology companies have always argued that end-to-end encryption is completely private between the correspondents in the conversation, since it is encrypted by a pair of security keys which their devices exchange, and which are available to no one else, not even the OTT provider. Providers are, therefore, unable to provide governments with any communications content, except metadata like the frequency of contact. The US Attorney General’s request to Facebook, which owns WhatsApp, suggests that this is correct. Along with his counterparts in Australia and the UK, he has requested Mark Zuckerberg not to deploy systems which “preclude any form of access to content, even for preventing or investigating the most serious crimes.” TRAI has said that it is looking at practices worldwide, but it is probably rediscovering this blank wall for itself.

Concerns about crime, terrorism and lethal mischief-making using encrypted communications are legitimate and, worldwide, pressure is developing on providers and platforms to make content available for inspection. However, privacy concerns are equally legitimate, because compromising security would degrade privacy across platforms. Blackberry, the pathbreaker in the secure communications sector, had kept a copy of encrypted communications and provided it to the governments of India, Saudi Arabia and the United Arab Emirates. As a consequence, the former smartphone giant is now an inconsequential player. Governments are asking OTT providers to go the Blackberry way, but it is insupportable. The cost to privacy, now recognised as a right, would be immense. It would open the door to situations like the NSA mass surveillance scandal. Governments should be careful what they wish for.

END