# Are India's laws on surveillance a threat to privacy?

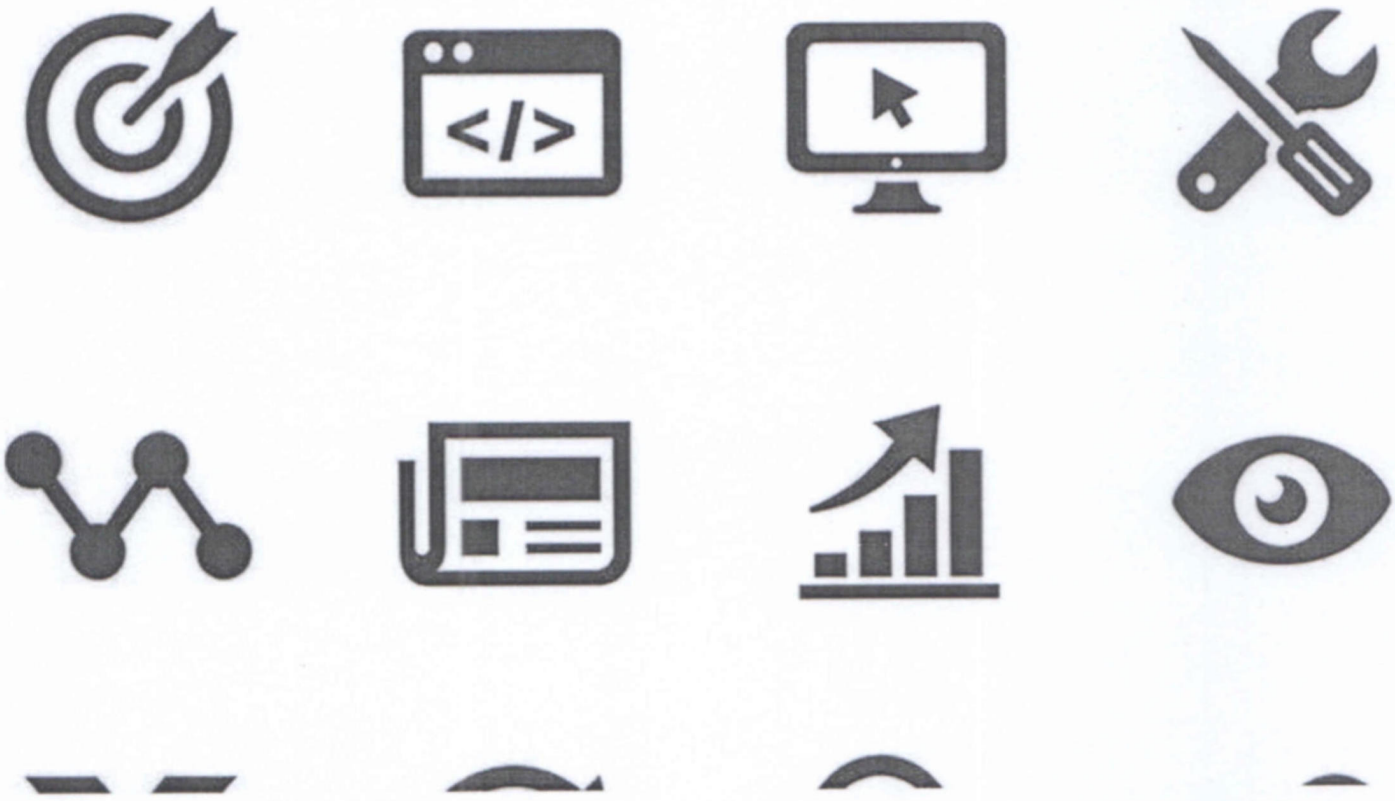
Tathagata Satpathy

Karnika Seth

Anita Gurumurthy

DECEMBER 28, 2018 00:22 IST
**UPDATED:** DECEMBER 28, 2018 00:22 IST





*In exceptional circumstances, the right to privacy can be superseded to protect national interest*

The Constitution of India guarantees every citizen the right to life and personal liberty under Article 21. The Supreme Court, in *Justice K.S. Puttaswamy v. Union of India* (2017), ruled that privacy is a fundamental right. But this right is not unbridled or absolute. The Central government, under Section 69 of the Information Technology (IT) Act, 2000, has the power to impose reasonable restrictions on this right and intercept, decrypt or monitor Internet traffic or electronic data whenever there is a threat to national security, national integrity, security of the state, and friendly relations with other countries, or in the interest of public order and decency, or to prevent incitement to

commission of an offence.

## Right to privacy is not absolute

Only in such exceptional circumstances, however, can an individual's right to privacy be superseded to protect national interest. The Central government passed the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, that allow the Secretary in the Home Ministry/Home Departments to authorise agencies to intercept, decrypt or monitor Internet traffic or electronic data. In emergency situations, such approval can be given by a person not below the Joint Secretary in the Indian government. In today's times, when fake news and illegal activities such as cyber terrorism on the dark web are on the rise, the importance of reserving such powers to conduct surveillance cannot be undermined.

There should be some reasonable basis or some tangible evidence to initiate or seek approval for interception by State authorities. This is the position in the U.S. Any action without such evidence or basis would be struck down by courts as arbitrary, or invasive of one's right to privacy. Therefore, the framework of the prescribed procedure needs to be adhered to, and its implementation needs conformance, both in letter and spirit. Any digression from the ethical and legal parameters set by law would be tantamount to a deliberate invasion of citizens' privacy and make India a surveillance state.

## Checks and balances

The government needs to increase accountability and responsibility, and infuse reasonable checks and balances in exercising these surveillance powers. The recent order passed by the Central government is within the ambit of its powers under Section 69 of the IT Act. However, present implementation of the Intermediary Rules of 2011 will have to be tested on the grounds of reasonableness, fairness, proportionality and judicious exercise of powers.

Another important aspect is that an individual may not even know if her electronic communications are being intercepted/monitored. If such surveillance comes within her knowledge, due to the obligation to maintain

confidentiality and provisions in the Official Secrets Act, she would not be able to know the reasons for such surveillance. This can make surveillance provisions prone to misuse.

Therefore, the role of the review committee is quite significant: The committee will aid in checking any arbitrariness in the exercise of these powers. Only 10 agencies have been declared as authorised agencies to confer certainty in this regard.

In *People's Union for Civil Liberties v. Union of India* (1996), the Supreme Court had set rules for the judicious exercise of surveillance and interception in phone tapping cases. The same fundamental principles should hold good in cyberspace too.

*Karnika Seth is a cyberlaw expert and advocate in the Supreme Court of India*

**IT'S COMPLICATED | ANITA GURUMURTHY**