



The Case Against Surveillance

(This editorial is based on the article “The Case Against Surveillance” which appears in The Hindu on 26th December 2018.)

In context please refer: [Data Interception by Government](#)

Recently, the Ministry of Home Affairs issued an order authorizing 10 Central agencies to intercept, monitor, and decrypt “any information generated, transmitted, received or stored in any computer.”

The 10 agencies include Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Central Bureau of Investigation, National Investigation Agency, Cabinet Secretariat (RAW), Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only), and Commissioner of Police, Delhi.

The notification was described as a progressive step towards a surveillance state even though the government stated that the notification created no new powers of surveillance. While the order allows agencies to decrypt data of any computer only after seeking approval of a competent authority, it is true that the move triggers surveillance concerns. **The Opposition even called it Unconstitutional.**

But, it is being argued that the MHA notification lays bare the lopsided character of the surveillance framework in India, and highlights an urgent need for comprehensive reform of the same.

Why Surveillance is necessary?

- **The right to privacy is not absolute.** Surveillance is essential to ensure national security and pre-empt terrorist threats, and it is in the very nature of surveillance that it must take place outside the public eye. Consequently, the regime is justified as it strikes a pragmatic balance between the competing values of privacy and security.
- There is a need to strike a fine balance between privacy and ensuring that policing or national security is taken to a level where technology is a facilitator and not a hindrance.

Challenges

- **It is crucial to acknowledge that every act of surveillance, whether justified or not, involves a serious violation of individual privacy; and further, a system of government surveillance** can have a chilling effect upon the exercise of rights, across the board, in any society.
- **Consequently, given the seriousness of the issue, a surveillance regime cannot have the executive sitting in judgment over the executive:** there must be parliamentary oversight over the agencies that conduct surveillance. Surveillance by the State cannot simply be authorized

through executive notifications.

- **And equally important, all surveillance requests must necessarily go before a judicial authority**, which can apply an independent legal mind to the merits of the request, in light of the proportionality standards discussed above.
- **Judicial review will not achieve much if the grounds of surveillance remain as broad and vaguely worded as they presently are.** Therefore, every surveillance request must mandatorily specify a probable cause for suspicion, and also set out, in reasonably concrete terms, what it is that the proposed target of surveillance is suspected of doing.
- As a corollary, evidence obtained through unconstitutional surveillance must be statutorily stipulated to be inadmissible in court.
- **There must exist, a lawyer to present the case on behalf of the target of surveillance** — even though, of course, the target herself cannot know of the proceedings because if surveillance requests are unopposed — it will be very difficult for a judge to deny a request that is made behind closed doors, and with only one side presenting a case.

Criticism

- Even though the staunchest civil rights advocates will not deny that an individual reasonably suspected of planning a terrorist attack should be placed under surveillance, in this context, the evidence demonstrates clearly that a heavily bureaucratized and minimally accountable regime of surveillance does nothing to enhance security, but does have significant privacy costs.
- **For example, while examining the U.S. National Security Agency's programme of mass surveillance, an American court found that out of more than 50 instances where terrorist attacks had been prevented, not even a single successful pre-emption was based on material collected from the NSA's surveillance regime.**
- In India, the existing surveillance framework is complex and confusing. Simply put, two statutes control the field: telephone surveillance is sanctioned under the 1885 Telegraph Act (and its rules), while electronic surveillance is authorized under the 2000 Information Technology Act (and its rules).
- This framework is heavily bureaucratized. Decisions about surveillance are taken by the executive branch (including the review process), with no parliamentary or judicial supervision; indeed, the fact that an individual will almost never know that she is being surveilled means that finding out about surveillance, and then challenging it before a court, is a near-impossibility.
- **The surveillance regime is also vague and ambiguous.** Under Section 69 of the IT Act, the grounds of surveillance have been simply lifted from Article 19(2) of the Constitution, and pasted into the law. They include very wide phrases such as “friendly relations with foreign States” or “sovereignty and integrity of India”.

Article 19 in The Constitution Of India 1949

Protection of certain rights regarding freedom of speech etc.

(1) All citizens shall have the right

(a) to freedom of speech and expression;

(b) to assemble peaceably and without arms;

(c) to form associations or unions;

(d) to move freely throughout the territory of India;

(e) to reside and settle in any part of the territory of India; and

(f) omitted- subclause (f) was omitted by the Constitution (44th Amendment Act 1978)

(g) to practice any profession, or to carry on any occupation, trade or business

Article 19(2) Nothing in subclause (a) of clause (1) shall affect the operation of any existing law, or prevent

the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

- Lastly, the regime is opaque. There is almost no information available about the bases on which surveillance decisions are taken, and how the legal standards are applied. Indeed, the evidence seems to suggest that there are none: a 2014 RTI request revealed that, on an average, 250 surveillance requests are approved every day. It stands to reason that in a situation like this, approval resembles a rubber stamp more than an independent application of mind.

Way Forward

- **There needs to be greater transparency in the system as in the current system,** Government agencies are not accountable to anyone other than the government itself.
- A comprehensive reform of the surveillance framework in India is long overdue.
- **The current debate, therefore, is not about ‘whether surveillance at all’, but about ‘how, when, and what kind of surveillance’.**
- This is also the right time: across the world, there is an increasingly urgent debate about how to protect basic rights against encroachment by an aggressive and intrusive state, which wields the rhetoric of national security like a sword.
- **In India, the Supreme Court’s privacy judgment has taken a firm stand on the side of rights. Citizens’ initiatives, such as the Indian Privacy Code have also proposed legislative models for surveillance reform.**
- After the Supreme Court’s 2017 judgment in *K.S. Puttaswamy v. Union of India* (‘the Right to Privacy case’), the Constitutional contours within which the questions of ‘how, when, and what kind’ have to be answered have been made clear.
- Any impingement upon the right to privacy must also be proportionate.
- One of the factors of the proportionality standard is that the government’s action must be the least restrictive method by which a state goal is to be realized. In other words, if the same goal — i.e., protecting national security — can be achieved by a smaller infringement upon fundamental rights, then the government is Constitutionally bound to adopt the method that does, indeed, involve minimal infringement.
- **Reforms in the Indian surveillance regime, should, therefore, incorporate ethics of surveillance which considers the moral aspects of how surveillance is employed.**