Countering the Surveillance State

What is the issue?

\n\n

\n
- Over the past few years, the government has taken several steps to enhance its capacity to monitor citizens through various structures.
\n
- This has led to apprehensions of India becoming a surveillance state due to the government’s growing powers to spy on citizens.
\n

\n\n

What are the significant government moves to establish surveillance?

\n\n

\n
- **Home Ministry -** The ministry recently stated its intention to create a centralised nationwide database of fingerprints of criminals.
\n
- This is part of the proposed “Crime and Criminal Tracking Network System” (CCTNS), which also plans to include face recognition capability.
\n
- There are also reports of the ministry seeking access to the Unique Identification Authority of India (UIDAI) biometric database.
\n
- **SEBI -** Securities and Exchange Board of India (SEBI) had set up a panel to review the regulatory powers of it and recommend improvements.
\n
- The panel recently recommended that SEBI be given powers to wiretap and record phone calls in order to enhance its ability to monitor insider trading.
\n
- **Cyber Space -** The Netra (Network Traffic Analysis) system for internet monitoring has been operational for several years.
\n
- But its exact capabilities are unknown since it is shielded from the Right to Information Act owing to security implications.
\n

- Further, the government had also mooted creating a social media monitoring hub in order to enable “360-degree monitoring” of the social media activity.
\n
- This was put on hold only after the Supreme Court (SC) observed that it would be akin to “creating a surveillance state”.
\n

\n\n

What are the implications?

\n\n

\n
- The above cases effectively mean that the SC judgment recognising the right to privacy as a fundamental right is being undermined in practice.
\n
- Until there are specific laws limiting the surveillance powers of governments, the surveillance activities of the state will likely proliferate.
\n
- But the recent data protection legislation as suggested by the Srikrishna Committee provides too much leeway for the government for surveillance.
\n
- More significantly, even already existing rules limiting the state’s powers to infringe on a citizen’s privacy are not followed in letter and spirit.
\n
- For instance, although wiretaps are supposed to be authorised only by senior officials for specific purposes, they are done on a truly massive scale.
\n

\n\n

What is the way ahead?

\n\n

\n
- As the years roll by since technological advances are likely to make surveillance systems even more invasive and efficient.
\n
- But technical solutions are also being evolved to better rationalise our ability to share data online like the MIT’s “Social Linked Data (Solid)” project.
\n
- However, the mere existence of technology will not prevent the government from coercively collecting data, and laws are needed for curbing them.
\n
- While the state needs to create such capabilities for legitimate reasons, each case of surveillance must be justified by high profile requests.

\n
- Moreover, the right to forget regulations need to be strengthened so that citizens can ask for data to be deleted from government databases.
\n

\n\n

\n\n

Source: Business Standard

\n