E-PAPER
MAIL TODAY

MAIL TODAY ePaper

Snooping can lead to data abuse

by Sunil Abraham

Enlarge Image

THE NATGRID, aiming to link databases of 21 departments and ministries for better counter-terror measures, adopts blunt policy approach, subjecting every citizen to the same level of blanket surveillance, instead of a targeted approach that intelligently focuses on geographic or demographic areas that are currently important.

All you manage to do with the current approach help software, hardware and biometric equipment vendors achieve their sales targets.

It is quite unlikely that security agencies will learn anything insightful by putting everybody under the same degree of surveillance.

There is no scientific evidence to show that we will be a safer nation if the government eavesdropped into all aspects of a citizens life.

Targeted surveillance, on the other hand, is like good old- fashioned detective work. Put a particular section — of potential troublemakers — under surveillance and leave the others alone.

With round- the- clock, 100- per cent, 360- degree surveillance, all the data is scrutinised all the time.

The more effective approach is to sample and collect data while maintaining data trails. If anything suspicious is noticed, the rest of the trail can be dug up.

Blanket surveillance only leads to leaks and abuse and tremendous distraction. The surveillance infrastructure will be overburdened as 99 per cent of the records and files scanned will be of no interest terms of fighting terrorism, etc.

The 21 databases need to be opened only when there is anything suspicious in any of the extracted and scrutinised samples or subsets. If there is a suspicious pattern, it should lead to opening of subsets in all the databases. Obviously, there should be ways in which the databases can talk to each other — demand for a particular subset, and not for all the records to be available to agencies all the time.

The NATGRID has to be able to let investigators selectively go in and out of the necessary subsets data. No one should be able to have a 360 degree view of all activities of all Indians.

AS OF now, the NATGRID design does not appear to have a safeguard for data abuse. And no matter what you see Hollywood movies, this configuration does not exist in Europe or the US. Two important forms of protections that should be available in democracies with robust privacy laws are missing in India. The first is breach notification.

If intelligence agencies and the police have looked up your files, you have a right to be informed. Secondly, you can request for a copy of the information that is maintained on you and request modifications if the data is inaccurate, so as to prevent harassment.

Such checks and balances are necessary an intelligent and appropriate surveillance regime.

Merging all 21 databases for 1.2 billion people into a single system only provides a juicy target for any internal or external enemy. From the perspective national security, it is a foolish thing to do. Terrorist groups will be able to target a single failure point destroy over a billion lives.

Since the current configuration of the NATGRID only undermines national security, one is forced conclude that national security is a false pretext.

This explains the deep scepticism among many the intelligence agencies involved.

The real purpose of the project is to scare citizens in the age of Arab springs. The NATGRID is a disciplinary measure aimed at social engineering of citizens behaviour. Unfortunately, our media has been misled by the corporate cheerleaders of this humongous waste of money.

The writer is executive director at the Centre for Internet and Society in Bangalore.

(As told to Max Martin)

COMMENTARY

by Sunil Abraham

⊞ Enlarge Image