ASIA 04.06.2020 | Kim Arora

India's growing surveillance state

The country's intelligence agencies have little to no independent oversight. The Covid-19 crisis has exacerbated the problem

India's homegrown Covid-19 contact-tracing app Aarogya Setu recently saw a series of pushbacks and resistance over privacy issues, in particular when the app was made mandatory for certain activities. Since then, an order from the Ministry of Home Affairs (MHA) has since diluted the obligation somewhat.

However, apart from the important perspectives of security, privacy and data protection, we need to look at such mass data collection in the light of India's broader surveillance architecture. Crucially, the country's intelligence agencies lack independent and external oversight, which is a standard feature in most democracies today.

Late in December 2018, the central government issued an order allowing 10 federal agencies to intercept, monitor and decrypt any information 'generated, transmitted, received or stored in any computer resource'. This order from two years ago takes on a greater significance in the light of the fact that the Aarogya Setu app crossed 100 million downloads within 40 days of its launch. The app is seeded with sensitive personal details such as name, age, gender etc, along with GPS location and other health data of Indians.

India's surveillance architecture

There are many issues with accountability in India's surveillance architecture. To begin with, it was executive orders and not statutes that created the country's most vital intelligence agencies at the central level. These include the foreign intelligence agency Research and Analysis Wing (RAW), the domestic intelligence agency Intelligence Bureau (IB) and the Central Bureau of Investigation (CBI). The formation of the IB, in fact, has been traced to a pre-Independence era telegram from a British colonial official. These federal investigation and intelligence agencies report directly either to federal ministries or federal government

departments.

Among the legal provisions that empower the state and federal governments to issue orders for interception mandate that they go through a review committee. However, this committee does not meet the standards of independence and externality, as it is composed of civil servants attached to government ministries and/or departments. Moreover, as pointed out elsewhere, it reviews interception orders, not how the agencies implement them.

The lacuna of an independent and impartial accountability framework in India's surveillance apparatus has been repeatedly addressed and formally identified but never decisively acted upon.

The laws allow surveillance on the grounds of national security, maintenance of public order, and maintenance of friendly relations with other foreign nations, among others. Similar grounds are also used to deny information under the Right to Information (RTI) Act, 2005 – an important tool for accountability and transparency, which in principle, is similar to Freedom of Information provisions in the EU framework. Digital rights advocacy organisation Software Freedom Law Center (SFLC) filed several RTI requests to get more information on the functioning of India's communication surveillance. Their queries were only partially answered, while others were denied because of 'security concerns.' RTI applications are therefore rendered futile when checking state surveillance overreach.

The fight for accountability

Efforts to bring in other kinds of accountability have also borne little fruit, fears of compromising security being the oft-repeated reason. In 2018, the Supreme Court rejected a plea asking for India's chief intelligence agencies to be brought under financial audit, saying that a 'judicial order to audit these agencies will create a dent in their functioning and security. This would lead to a dangerous situation.'

The lacuna of an independent and impartial accountability framework in India's surveillance apparatus has been repeatedly addressed and formally identified but never decisively acted upon.

After the 21-month state of emergency in India was over in 1977, the newly elected federal government at the time set out to review police action and surveillance excesses during the period. Government

committees recommended various intelligence reforms, including drawing up a charter of duties for the IB and the CBI. Celebrated former RAW officer B. Raman, for one, strongly criticised the fact that successive governments failed to act upon or even consider such reforms.

'It is possible to introduce some of these checks and balances in the functioning of our intelligence community without damaging their operational secrecy. There is reluctance from the political class because it sees the agencies as instruments for partisan exploitation and not for defending national interests,' Raman wrote in 2010. Another government committee formed in the aftermath of the Kargil War in 1999 pointed to the lack of oversight, monitoring and performance reviews in India's intelligence agencies. 'These are all standard features elsewhere in the world. In the absence of such procedures, the Government and the nation do not know whether they are getting value for money,' the committee said in its report.

The Covid-19 state of exception

Congress politician and Member of Parliament Manish Tewari tried the legislative route in 2011. He floated a private member's Bill called 'The Intelligence Services (Powers and Regulation) Bill, 2011' which proposed the institution of a National Intelligence and Security Oversight Committee, which would include Leaders of Opposition. The Bill could not come up for discussion and lapsed the following year.

Elsewhere in the world, questionable mass surveillance practices have impacted international business. When Austrian privacy activist Maximillian Schrems first sued Facebook in 2013, the point of contention was the use of Facebook's user data by US surveillance agencies as revealed by NSA whistleblower Edward Snowden. Schrems argued it violated his right to privacy as an EU citizen. As a result, the EU-US transatlantic commercial data transfer arrangement, International Safe Harbor Privacy Principles (Safe Harbour) came into question. Two years later, in 2015, the European Court of Justice declared it invalid. The EU and the US were forced to adopt another set of principles to govern transatlantic data flows. Called the Privacy Shield, it came into force in 2016. Just like its predecessor, it is also under the legal scanner for possible privacy violations.

Coupled with that is the fact that the Indian political climate of the last few years has seen student

The instances of exploitative, extensive and illegal mass surveillance as exposed by Snowden in the summer of 2013 involved not just India, but also developed democracies of the Global North. What is remarkable here is that the

bodies, activists and media alike facing the force of the state.

latter already had varying sorts of oversight mechanisms in place. But even these could not prevent the violation of fundamental rights. One can then only imagine the impudence and brazenness of such operations where these mechanisms do not exist. In the US, the Snowden revelations sparked a debate on the oppressive confidentiality requirements of the Foreign Intelligence Surveillance Court (FISC) and led to a drop in the use of the US Patriot Act. In Germany, it prompted a review of intelligence oversight. This was possible as there was room to demand accountability.

Today, without judicial or parliamentary oversight on surveillance agencies, India has already begun to widely deploy facial recognition technology. A citizen's registry, which sparked nationwide protests for being discriminatory towards minorities earlier this year, is in the works. Both international and domestic Internet and tech companies are creating more possibilities of making the people transparent and those in power opaque.

In her much celebrated book *The Age of Surveillance Capitalism*, Shoshana Zuboff points out how the 'declaration of a state of exception functions in politics as a cover for the suspension of the rule of law and the introduction of new executive powers justified by crisis.' The current Covid-19 crisis has without a doubt created the state of exception that Zuboff talks about. Coupled with that is the fact that the Indian political climate of the last few years has seen student bodies, activists and media alike facing the force of the state. This makes it more important than ever to institute accountability measures on surveillance agencies. It shouldn't take a global pandemic to do so.

The views expressed above are the author's own and do not reflect those of her employer.



Kim Arora
New Delhi

Kim Arora is a journalist and researcher from New Delhi, India. As a reporter, she has covered the burgeoning tech policy scene in India. As a German Chancellor Fellow, she analysed approaches to privacy and data protection in India and Germany.