Source : www.thehindu.com Date : 2021-07-21

PEGASUS IS INDIA'S WATERGATE MOMENT

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

"If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology." Those words of Sen. Frank Church, who led one of two committees on intelligence and surveillance reform established in the aftermath of the Watergate scandal, are just as relevant in India today given the revelations of extensive surveillance — it is unclear by whom, but signs point to the Indian government — by the use of spyware on people's phones. While there is much to be said about the international regulation of the unaccountable sale of spyware by shadowy entities such as the NSO Group, it is equally, if not more important to ensure that surveillance in India is made accountable.

My former colleague, Sunil Abraham, often likens surveillance to salt. A small amount of surveillance is necessary for the health of the body politic, just as salt is for the body; in excess, both are dangerous. While one cannot enjoy the liberties provided under the Constitution without national security, we must equally remember that national security is not meaningful if it comes at the cost of the very liberties such security is supposed to allow us to enjoy. Excessive and unaccountable surveillance imperils privacy, freedom of thought, of speech, and has a chilling effect on people's behaviour, while shattering the bedrock of the rule of law upon which a constitutional liberal democracy is built.

Also read: In 2019, IT House panel unsuccessfully tried to probe Pegasus breach

The government claims all its surveillance is authorised and justified. But then, the question arises: where are the prosecutions for terrorism, organised crime, espionage, etc., based on evidence from such surveillance? Who is ensuring that the surveillance is necessary and proportionate? Indeed, on the contrary, there are numerous examples of surveillance powers being misused for personal and political gain, and to harass opponents.

In 2012 in Himachal Pradesh, the new government raided police agencies and recovered over a lakh phone conversations of over a thousand people, mainly political members, and many senior police officials, including the Director General of Police (DGP), who is legally responsible for conducting phone taps in the State.

In 2013, India's current Home Minister was embroiled in a controversy dubbed "Snoopgate", with phone recordings alleged to be of him speaking to the head of an anti-terrorism unit to conduct covert surveillance on a young architect and her family members without any legal basis. The Gujarat government admitted the surveillance, including phone tapping, but claimed it was done on the basis of a request made to the Chief Minister by the woman's father. Yet, no order signed by the State's Home Secretary — a legal necessity for a phone tap — was ever produced, and the Gujarat High Court shut down an inquiry into "Snoopgate" upon the request of the architect and her father, on the shocking basis that it "did not involve public interest".

In 2009, the United Progressive Alliance government swore in an affidavit in the Supreme Court that the CBDT had placed Niira Radia, a well-connected PR professional, under surveillance due to fears of her being a foreign spy. Yet, while they kept her under surveillance for 300 days, they did not prosecute her for espionage.

Non-state actors such as the Essar group, have also been shown to engage in illegal surveillance. K.K. Paul, then the Governor of Meghalaya, noted complaints by telecom operators that private individuals were misusing police contacts to tap phone calls of “opponents in trade or estranged spouses”.

There are dozens of such examples of unlawful surveillance which seem to be for political and personal gain, and have nothing to do with national security or organised crime. Yet, there are few examples of people being held legally accountable for unlawful surveillance.

Currently, the laws authorising interception and monitoring of communications are Section 92 of the CrPC (for call records, etc), Rule 419A of the Telegraph Rules, and the rules under Sections 69 and 69B of the IT Act. Indeed, it is unclear when the Telegraph Act applies and when the IT Act applies. A limited number of agencies are provided powers to intercept and monitor.

In 2014, the Ministry of Home Affairs told Parliament that nine central agencies and the DGPs of all States and Delhi were empowered to conduct interception under the Indian Telegraph Act. In 2018, nine central agencies and one State agency were authorised to conduct intercepts under Section 69 of the IT Act. Yet, the Intelligence Organisations Act, which restricts the civil liberties of intelligence agency employees, only lists four agencies, while the RTI Act lists 22 agencies as “intelligence and security organisations established by the central government” that are exempt from the RTI Act. Thus, it is unclear which entities count as intelligence and security agencies.

Further, a surveillance alphabet soup exists, with programmes such as CMS, TCIS, NETRA, CCTNS, and so on, none of which has been authorised by any statute, and thus fall short of the 2017 K.S. Puttaswamy judgment, which made it clear that any invasion of privacy could only be justified if it satisfied three tests: first, the restriction must be by law; second, it must be necessary (only if other means are not available) and proportionate (only as much as needed); and third, it must promote a legitimate state interest (e.g., national security).

In 2010, then Vice-President Hamid Ansari called for a legislative basis for India’s agencies, and the creation of a standing committee of Parliament on intelligence to ensure that they remain accountable and respectful of civil liberties. In 2011, the Cabinet Secretary in a note on surveillance held that the Central Board of Direct Taxes having interception powers was a continuing violation of a 1975 Supreme Court judgment on the Telegraph Act. That same year, parliamentarian Manish Tewari introduced a private member’s Bill to bring intelligence agencies under a legislative framework. That Bill soon lapsed. In 2013, the Ministry of Defence-funded think-tank, the Institute for Defence and Strategic Analysis, published a report, “A Case for Intelligence Reforms in India”, a core recommendation of which was: “the intelligence agencies in India must be provided a legal framework for their existence and functioning; their functioning must be under Parliamentary oversight and scrutiny”.

In 2018, the Srikrishna Committee on data protection noted that post the K.S. Puttaswamy judgment, most of India’s intelligence agencies are “potentially unconstitutional”, since they are not constituted under a statute passed by Parliament — the National Intelligence Agency being an exception. In its 2019 election manifesto, the Indian National Congress — in what to my knowledge was a first for a national political party — called for parliamentary oversight of intelligence agencies.

The legacy of the Church Committee can be seen in the fact that the Snowden revelations in 2013 did not uncover any spying on Opposition politicians, journalists, judges, and human rights defenders for partisan political ends. What was shocking about the Snowden revelations was the extent of NSA’s surveillance, the overreach of the powers provided under the PATRIOT Act, as well as the lack of sufficient checks and balances provided by the Foreign Intelligence

Surveillance Court. The Snowden revelations led to meaningful reform of that court, and controversial domestic surveillance provisions of the PATRIOT Act expired in 2020.

We need such reforms in India, which are aimed at professionalising intelligence gathering, bringing intelligence agencies under parliamentary oversight, making them non-partisan, and ensuring that civil liberties and rule of law are protected. This is India's Watergate moment, and the Supreme Court and Parliament should seize it.

Pranesh Prakash was a co-founder of the Centre for Internet and Society, and is an affiliated fellow at Yale Law School's Information Society Project

Our code of editorial values

END