Spy in hand

The Govt. must come clean on the issues raised by revelations of phone surveillance.

Highlights:

1. At least 1,000 Indian phone numbers are in a list of potential targets of surveillance using the Pegasus spyware sold by Israeli company the NSO Group to "vetted governments" with the approval of the Israeli government.
2. Of these, 300 numbers have been verified; 22 phones were subjected to forensic analysis by Amnesty International and peer-reviewed by the University of Toronto's Citizen Lab. Of these, 10 were clearly established as being targeted by Pegasus; eight of the other 12 yielded inconclusive results.
3. The evidence is strong, and the credibility of these revelations is extremely high. Indian citizens were indeed targets of a vicious, abominable and uncivil surveillance campaign by a government entity, Indian or foreign. The buck stops with the Government of India.
4. Instead of coming clean and explaining what it intends to do to protect citizens, the GoI has fallen back on a disingenuous claim that no illegal surveillance is possible in India.
5. There are legal provisions for intercepting communication and accessing digitally stored information in the interests of national security and public safety.
6. The capture of a handheld machine by Pegasus turns that into a real-time spy on the target who can be watched over and followed every step. This surveillance is total, into their private and intimate lives, which have no bearing on any public interest.

Widespread Surveillance:

1. The cohort of people who were potential targets — journalists, politicians, probably a Supreme Court judge and a former Election Commissioner — does not indicate that the surveillance was necessitated by national security or public safety concerns.
2. It is safe to assume that no information regarding terrorism or Chinese intrusion can be obtained by spying on a woman who complained of sexual harassment by a former CJI.

3. On the contrary, the composition suggests that private craving, turpitude and even voyeurism motivated the perpetrators. This violation is about privacy and much more.
4. Information obtained illegally may have been used to compromise institutions, to steal elections, sabotage Opposition campaigns, and even dislodge an Opposition government.
5. That the accused in the Bhima Koregaon case had their computers breached by unknown entities to plant evidence that the prosecution is now using against them is notable in this context.
6. That state agencies can trample upon the lives of citizens in such a manner while elected representatives plead ignorance is unsettling for a democracy. This is antithetical to the basic creed of democracy.

The truth about these revelations must be unearthed through an investigation by a JPC or by the Supreme Court or any other credible mechanism. A starting point for the Government must be in clearing the air on the foremost question it is skirting around — has any Indian agency bought Pegasus?

Pegasus is India's Watergate moment

Intelligence gathering needs to be professionalised, parliamentary oversight introduced, and liberties and laws protected.

Go easy on the salt

1. 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.
2. 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.
3. 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.

4. Indeed there are numerous examples of surveillance powers being misused for personal and political gain, and to harass opponents.

Earlier examples

1. 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.
2. 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.
3. 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.

The laws

1. 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.
2. 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.
3. 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 an interception under the Indian Telegraph Act.
4. 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.

5. 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).

Way Forward:

1. 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.
2. 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.
3. That same year, parliamentarian Manish Tewari introduced a private member's Bill to bring intelligence agencies under a legislative framework. That Bill soon lapsed.
4. 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".
5. 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.

We need 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.