THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

July 28, 2021

Why the Pegasus Snooping is a Hacking of India's Democracy

By: Seema Chishti

The widespread use of the Pegasus spyware in India suggests a disrespect for the institutions of democracy at the highest levels of government. What could be worse for the future of India's democracy?

If the Covid-19 pandemic has revealed in full the many societal and economic ills in India, the 10-day-long and continuing reportage on the hacking of phones of opposition leaders, union government ministers, officials in high places, army and police officers, corporate leaders, civil society activists and journalists has revealed the extent of subversion of democracy and its institutions in the country.

Pegasus, a military-grade spyware, developed and exported by NSO, an Israeli firm, is reported to have been used to hack into cell phones of a global cast of characters at the behest of various and as-yet-unknown government agencies. At least 300 of the global list of 50,000 potential targets have been confirmed to be in India. Forensic examination suggests that at least 10 phones in India were indeed infected by the spyware.

The implications are chilling for the individuals who have been hacked. But look closer and it feels like an Arctic winter.

The Pegasus intrusions reveal that it is a level playing field, a must for a healthy democracy to operate in, that has been fully hacked. Fundamental rights are now being violated in India with banal impunity even without them being formally suppressed with a declaration of an Emergency.

The importance of privacy

As Gabriel Garcia Marquez told his biographer Gerald Martin: "Everyone has three lives: a public life, a private life, and a secret life." The "secret life" often might not have any public interest, but is of deep value to the person and has tremendous potential to be weaponized. If phones are hacked, this life is available for extraction by a snooping state, messages and locations can be tracked, and phones can be used as microphones and cameras. The wide range of personal and secret lives that the Pegasus snooping would have unveiled could have become tools for bullying and blackmail. Any sliver of fact can become a hook on which any big charge or trial can be made to hang.

Consider the case of Moroccan historian Maati Monjib, who was targeted using Pegasus. Gathering enough evidence about his private life over a year, armed intelligence agents raided his home at 9 am one morning, "finding him and a female friend in his bedroom together. They stripped him naked and arrested him for 'adultery,' which is a crime in Morocco. He spent 10 months in a Casablanca prison". Or the life of the Azerbaijani journalist Khadija Ismayilova. For nearly three years, her phone was regularly infected with Pegasus, intimate pictures were procured via surveillance and made public to destroy her reputation, and damage her ability to think freely.

> *The wide range of personal and secret lives that the Pegasus snooping would have unveiled could have become tools for bullying and blackmail.*

Preserving privacy is directly about preserving democracy. The Oxford-based scholar Carissa Veliz, author of *Privacy is Power*, speaks of the danger of citizens losing power as data is vacuumed out;

```
The power that comes about as a result of knowing personal details about someone is a very particular kind of power, although it also allows those who hold it the possibility of transforming it into economic, political, and other kinds of power.
```

When governments, ruling parties, political executives, or corporations start holding and using that data in unlawful ways, they hold power disproportionate to that held by citizens and thus distort democracy.

The Indian subversion

The hacking in India by spyware inverts the lawfully laid out system of surveillance that may be mandated by demands of national security. In India, hacking phones, even if 'authorised' by secretaries to the Government of India in the Ministry of Home Affairs, has no legal sanction. It is not to be mistaken for surveillance. The new minister for information technology has tried to sit on the fence by neither denying nor accepting responsibility, but as the digital rights group Internet Freedom Foundation puts it:

> It is important to note that no such power to hack the phones of Indian citizens exists under Indian law, and the pre-existing surveillance powers available under the Telegraph Act, 1885 and the Information Technology Act, 2000 do not permit the installation of spyware or hacking mobile devices. Hacking of computer resources, including mobile phones and apps, is in fact a criminal offence under S[ection] 66 of the Information Technology Act, 2000.

Let us look at more specific instances of how Pegasus-led invasive actions on certain citizens of India reveals-and widens-the democratic deficit.

Let us begin with the story of an election commissioner, who, at the time, was on course to be the next chief of the Election Commission of India, being on the snoop list. He was the only one of the three in the commission who found certain statements by Prime Minister Narendra Modi during the 2019 general election campaign as violative of the model code of conduct. The journalist who reported on the commissioner's objections and a member of the prominent election watchdog, who is known to not take things lying down, were also on the snoop list.

The one thing India could claim even as its rank dipped in global indices of democracy, was conducting 'free and fair' elections. But how free and fair could elections be if an election commissioner, a journalist reporting on the Election Commission of India, and an independent watchdog are under such invasive surveillance?

Equally damning is news that a range of opposition figures might have been the victim of state-sponsored hacking. This includes the principal political opponent of the BJP, former Congress party president Rahul Gandhi. At least two of Gandhi's phones and those of five others in his social circle, who are not in public life, were on the snoop list. In Karnataka, phones used by senior members of the Janata Dal(S)-Congress government and their aides were likely hacked ahead of the BJP's toppling of the government there. In Assam, two important political figures opposed to the controversial Citizenship (Amendment) Act 2019 had their numbers on the list for possible use by the Israeli spyware just before the act was passed in December 2019.

> *[H]ow free and fair could elections be if an election commissioner, a journalist reporting on the Election Commission of India, and an independent watchdog are under such invasive surveillance?*

Democracies are based on a supposition of a level playing field, ensuring all political players have a similar handicap. If invasive software is deployed by the state on the institution mandated to conduct elections and on significant opposition players, the field is skewed and far from level.

But it gets worse.

In democracies, the system of checks and balances is sought to be maintained by an independent judiciary. In the case of a former chief justice, who had a case of sexual harassment filed against him by a junior staffer, it was bad enough that the chief justice himself headed a three-judge bench that rubbished the charges. A controversial and opaque 'in-house inquiry' ordered by the Supreme Court also said later that there was nothing in the charges against the chief justice. The snoop list has now revealed that the staffer, along with her relatives, were on the list of potential Pegasus targets.

> *[T]he jury is out on how independent the judiciary was when this particular chief justice decided several crucial cases after the sexual harassment case was buried.*

In months after being declared innocent, the chief justice went onto preside over crucial benches that decided among other things, Ayodhya, the fate of election laws relating to electoral bonds, the Rafale fighter jet deal, and Kashmir's habeas corpus cases. In each of these decisions, the executive happened to emerge on the winning side. Four months after his retirement, the same chief justice was nominated by the same executive as an MP to the Rajya Sabha.

With the Pegasus list including 11 cell phone numbers of the family of the complainant staffer, not only does it raise questions about that case, but the jury is out on how independent the judiciary was when this particular chief justice decided several crucial cases after the sexual harassment case was buried.

Similarly, in an ugly fight between the then head of the Central Bureau of Investigation (CBI)-a senior police officer, an appointee of the Modi government-and his deputy, who had worked closely with PM Modi when he was chief minister in Gujarat, it transpires that phones of both the officials were on the Pegasus list, as were those of the CBI chief's wife, daughter, and son-in-law. So how pressure-free could goings-on have been within this supposedly 'independent' investigative agency?

> *No democracy can survive a surveillance regime mounted upon those who do the heavy-lifting of keeping a democracy alert…*

That several journalists, civil society activists, and even the India head of the Bill and Melinda Gates Foundation - one of the world's largest philanthropic organisations - are on the Pegasus list of numbers must ring alarm bells loudly on this government's ability to let civil society function. Casting an illegal net to fish out all manner of information amounts to attempting to control and subvert the functioning of these actors who are expected to be independent. No democracy can survive a surveillance regime mounted upon those who do the heavy-lifting of keeping a democracy alert by maintaining a system of feedback between the grassroots and those at the top.

Subversion of law by planting evidence

While other countries in the Pegasus project list have seen journalists and civil society activists being surveilled, India has seen a significant criminal variant of concern of the problem. The *Washington Post* has revealed that eight of the 16 undertrials in the Bhima Koregaon case were targeted by Pegasus before being imprisoned. There is evidence of digital files being planted remotely on the computers of two of those surveilled, according to Arsenal Consulting, a US-based digital forensic firm. These files are precisely what were deemed as critical evidence for keeping them behind bars. In the meantime, an 84-year old undertrial has died in custody. The two undertrials who have formally complained of the planted evidence and have moved court.

Looking at how the Indian government has handled the controversy so far points to a breakdown in systems. NSO says it sells only to "vetted governments" or their agencies. So if it is not the Indian state but a rogue agency within the government or even 'a foreign hand' that is using Pegasus, should the government not be concerned about the bombing of military-grade spyware onto phones of Indian citizens?

The Indian system is revealing more rot as days go by. Citizens of other countries are getting a systemic response with enquiries being lodged. France has instituted three enquiries, Mexico's anti-corruption investigator has made statements, Israel has set up a commission and even the King of Morocco has sued *Forbidden Stories* in France. Indian citizens appear to have no recourse other than seeking the intervention of the judiciary, as a few have done, when it is the executive of the Union Government that should investigate this hacking. It has been left to a state government to formally institute a judicial commission of enquiry to investigate the Pegasus episode. Far from making the government of the day look strong, all this makes Indian democracy appear very vulnerable.

> *Data on the government and the rulers will be black-boxed, but citizens' data must be sucked up, both legally and illegally.*

There is a larger message to be gleaned from the Union Government being blasé over serious charges of infringement and invasion of the data of its citizens. India has been witnessing a sharp slide in executive transparency. The current government has been anxious for all aspects of a citizen's life to be made available to it, even as the Personal Data Protection Bill has been delayed indefinitely, the Right to Information law has been run into the ground, and election funding has grown opaque to the benefit of the ruling party.

Pre-legislative consultations on policy are almost absent. Last year, a campaign against changes in the Environment Impact Assessment rules resulted in police cases being slapped on the organisers and the arrest of one of them, a 22-year old student.

A contrasting image has emerged of this government's approach to its citizens' data versus its own, which points to a textbook authoritarian approach. Data on the government and the rulers will be black-boxed, but citizens' data must be sucked up, both legally and illegally. The centre has walked back so much on transparency norms that it does not even find it necessary to disclose something

as innocuous as the details of the prime minister's college degree. Compare this with the spurious 'what-have-you-got-to-hide?' obfuscation when it comes to citizens' lives. If the government has nothing to hide, why does it not order a Joint Parliamentary Committee enquiry into the current snooping case?

Summing up

WhatsApp confirmed that it had informed the government of India in 2019 that at least 121 Indian numbers-belonging to academics, lawyers, Dalit activists, and journalists-had been hacked by Pegasus, exploiting a chink in the chat app's armour. The government got away by deflecting attention to issues with the Facebook-owned chat app, which was really not the point. Now, as bigger and more fish have been revealed as being on the hack list, if the state were yet not held answerable, there would be a heavy price that India's democracy would have to pay.

> *Pegasus has revealed the dark cloud over the Election Commission, judiciary, media, and the autonomy of the political opposition. What could be worse for India?*

As the government tries to put a lid on serious charges of political espionage, it is clear that fundamental tenets of democracy are at a tipping point. Democracies, rely on institutions that provide checks and balances to the executive. Else they degenerate into sultanism or despotism, with only an outer shell of democracy. The reportage on Pegasus has revealed the dark cloud over the Election Commission, judiciary, media, and the autonomy of the political opposition. What could be worse for India?

If the Pegasus hacking is not thoroughly investigated and if those who approved the use of the spyware are not held accountable, "The India Story"-eloquently termed so in Debashish Roy Chaudhury and John Keane's *To Kill a Democracy, India's Passage to Despotism*-will have an ending that is far from cheerful. Future historians would find it hard to believe that democracy in India was allowed to be strangulated in broad daylight. It doesn't seem to always "die in the darkness."

(*The first version of this article had stated that charge sheets had not been filed in the Bhima Koregaon case. This is not correct; some charge sheets have been filed.*)