Source : www.thehindu.com Date : 2022-07-22

IN PEGASUS BATTLE, THE FIGHT FOR SURVEILLANCE REFORM

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

‘The surveillance industry is becoming increasingly accessible, and the nature of surveillance, exponentially intrusive’ | Photo Credit: Getty Images/iStockphoto

A year has passed since the disclosures about the Pegasus Project revealed the threat to India’s democracy. A leading digital news platform reported that the cellphones of at least 300 Indians had been hacked with Pegasus, the spyware from the Israel-based NSO Group; 10 of the cases were confirmed by Amnesty International’s Security Lab using forensic analysis. The victims, important members of India’s constitutional order, included cabinet Ministers, Opposition leaders, journalists, judges and human rights defenders.

India has been aware of the existence of Pegasus since October 30, 2019 when WhatsApp confirmed that the spyware has been used to exploit a vulnerability in its platform to target activists, academics, journalists and lawyers in India. Since then, NSO has been able to advance its technology, and Pegasus can now infect devices without any action on the user’s part. Considering the severity of the threat posed by these disclosures, and the credibility of the evidence which backs them, it is important to examine how each branch of the Indian state has responded, or failed to respond, in protecting the privacy of citizens.

The expectation is that the executive will provide the first response and that government agencies will respond with action given the serious nature of the disclosures. But on July 19, 2021, the Minister of Electronics and Information Technology, Ashwini Vaishnaw, referring to “press reports of 18th July 2021”, refused to directly address the claims made by the Pegasus Project; he stated that the existing legal framework prevents unauthorised surveillance.

On November 28, 2019, the former Minister of Electronics and Information Technology, Ravi Shankar Prasad, had responded similarly to allegations over the use of Pegasus. A report by *The New York Times* of January 31, 2022 contradicted both their statements and stated that ‘India has bought Pegasus in 2017 as part of a $2-billion’ defence package. The apathy shown by cabinet Ministers has been mirrored by specialised agencies.

In response to disclosures by the Pegasus Project, CERT-IN, the nodal agency, the Indian Computer Emergency Response Team, that deals with cybersecurity threats, has remained silent. However, WhatsApp’s statement in 2019 did compel CERT-In to issue notices to NSO and WhatsApp on November 26, 2019. But the agency has not provided any updates on what has transpired.

Under India’s constitutional scheme, the legislature is responsible for holding the executive accountable. However, practice has failed to match principles. When on July 28, 2021, the IT Committee sought to question officials from the IT Ministry and the Home Ministry on Pegasus, members (primarily from the ruling party), according to news reports, abstained as a bloc and prevented a quorum. Previously, on November 19, 2019, those who had been targeted by Pegasus using a vulnerability in WhatsApp, wrote to the IT Committee which even discussed the issue. However, it has not provided any updates on its findings. Separately, in every parliamentary session since the revelations, the Opposition has sought a discussion and a probe. Both demands have been ignored.

When it became evident that no answers were forthcoming from the executive and the legislative branches, the victims turned towards the judiciary to seek redress. Thus, on August 5, 2021, the victims approached the Supreme Court of India where they demonstrated that forensic analysis had found their phones to have been infected.

On October 27, 2021, the Court constituted a technical committee to examine whether the spyware had been used on Indian citizens. Eight months have passed but the committee has yet to arrive at any findings. In this period, the committee has been examining the phones of the victims and seeking comments from the public on surveillance reform. On May 20, 2022, it placed an 'interim report' before the Court asking for time to place the final report; this was granted. The case is now listed for the end of July 2022. While the top court is waiting for the technical committee to submit its report, on December 16, 2021 it restrained a Commission of Inquiry (constituted by the Government of West Bengal) from investigating whether the spyware had been used on residents of West Bengal.

Perhaps commentators jumped the gun when they made the remark that Pegasus was India's 'Watergate Moment'. In the aftermath of Watergate, the institutional response in the United States held President Richard Nixon and others involved accountable, in which all branches of the state acted to check the abuse of power. But in India, the story continues to persist as one of official stonewalling with no accountability in sight.

Unlike the polity in India, other countries have responded to the Pegasus disclosures. Israel, for example, set up a senior inter-ministerial team to begin an investigation while the Foreign Minister, Yair Lapid, said that the government would work to ensure that Pegasus did not fall into the wrong hands. France ordered a series of investigations within a day of the revelations; on September 25, 2021, its cybersecurity agency confirmed that the spyware had been used to target French citizens. On November 3, 2021, the United States added NSO to its 'Entity List for Malicious Cyber Activities', which restricted the ability of U.S. companies to export goods or services to NSO. In the United Kingdom, the spyware company implemented a change to ensure that Pegasus could no longer target U.K. numbers after revelations, in 2021, that Dubai's ruler, Sheikh Mohammed bin Rashid Al Maktoum, had used the spyware to hack the phones of his wife, Princess Haya, and her divorce lawyers, Baroness Fiona Shackleton and Nick Manners, amid an ongoing custody battle.

The lack of accountability has spurred further violations. While the Pegasus victims in India wait for answers, there are documented instances of the advanced spyware being used in India against human rights defenders. Reports by a digital forensics consulting company, Arsenal Consulting (dated February 8, March 27, and June 21, 2021) revealed that two of the 16 accused in the Bhima Koregaon case, Rona Wilson and Surendra Gadling, had been targeted by a commercially available spyware, 'NetWire', for almost two years. The spyware was used to surveil and plant incriminating documents on their devices — documents which now form the basis of the National Investigation Agency's case against them.

The Indian 'surveillance for hire' industry is growing. These firms offer their services to anyone who can pay, following which they proceed to spy on indicated targets by hacking their devices. A Reuters report from June 30, 2022 termed these firms as "Indian cyber mercenaries" who were being used by litigants around the world to sway litigation battles. One such Indian company, BellTroX, was engaged in surveillance-for-hire activities and was one of the several entities Facebook investigated, identified, and removed from its platforms in December 2021. Much like what happened with the Pegasus Project, there has been no official response to both these reports.

An overhaul of surveillance laws is necessary to prevent the indiscriminate monitoring of people

and entities by the state and private actors. The Information Technology Act, 2000 and the Indian Telegraph Act 1885 which empower the Government to surveil, concentrate surveillance powers in the hands of the executive, and do not contain any independent oversight provisions, judicial or parliamentary. These legislations are from an era before spyware such as Pegasus were developed, and, thus, do not respond to the modern-day surveillance industry.

Unfortunately, legislative proposals by the Union Government for surveillance reform do not exist. The proposed data protection law does not address these concerns despite proposals from members of the Joint Parliamentary Committee. Instead, the proposed law provides wide exemptions to the Government relating to select agencies from the application of the law; one which might be used to exempt intelligence and other law enforcement agencies. This gap in the surveillance framework has led to severe harm being caused to India's democratic ideals.

The past year has showcased why the need for comprehensive surveillance reform is so urgent. The Freedom House 'Freedom in the World' report — it tracks global trends in political rights and civil liberties — changed India's status from 'free' to 'partly free' in 2021. It has cited the alleged use of Pegasus on Indian citizens as one of the reasons for the downgrade. From targeting activists and journalists for civil and political purposes, to the targeting of litigants for commercial benefits, the surveillance industry is becoming increasingly accessible, and the nature of surveillance, exponentially intrusive. In the absence of immediate and far-reaching surveillance reform, and urgent redress to those who approach authorities against unlawful surveillance, the right to privacy may soon become obsolete.

Anushka Jain is the Associate Policy Counsel (Surveillance and Transparency) and Krishnesh Bapat is the Associate Litigation Counsel at the Internet Freedom Foundation. Mr. Bapat is representing victims of Pegasus in proceedings before the Supreme Court of India