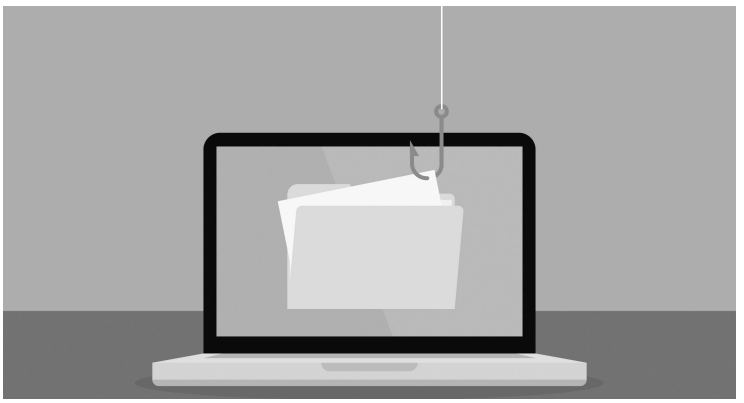
The hacking of Indian democracy

National security is important, but it can have an impact on human rights and civil liberties

DUSHYANT DAVE



ISTOCK PHOTO

The Pegasus revelations reflect an attack on Indian democracy and Indian citizens. Was the government directly responsible for the surveillance of a select group of Indian activists, politicians and journalists and others? Or was the surveillance at the instance of a private player? With the government in denial, a commission of inquiry by a sitting Supreme Court judge can alone unravel the mystery.

National security is important, but it can have an impact on human rights and civil liberties. The use of surveillance has serious implications for privacy. But the list of people targeted *prima facie* shows that national security is a pretext to suppress political and societal dissent in India.

Acting according to conscience

Pegasus is a technology sold to governments to fight terrorism. The Israeli Supreme Court, in September 1999, said in *Public Committee Against Torture in Israel v. Israel* that shaking, waiting in the 'Shabach' position, the frog crouch, excessively tight handcuffs and sleep deprivation were illegal. It held that they granted General Security Service investigators "the authority to apply physical force during interrogation of suspects suspected in involvement of... terrorist activities, thereby harming suspects' dignity and liberty". This, it said, "raises basic questions of law and society, of ethics and policy and of the rule of law and security."

Speaking for the Court, President A. Barak declared, "This decision opened with a description of difficult reality in which Israel finds herself... We are aware that this decision does make it easier to deal with that reality. This is the destiny of a democracy... A democracy must sometimes fight with one hand tied behind its back. Even so, a democracy has the upper hand. The rule of law and the liberty of an individual constitute important components in its understanding of security." He concluded, "We are aware of the harsh reality of terrorism in which we are, at times, immersed. The possibility that this decision will hamper the ability to... deal with terrorist and terrorism disturbs us. We are, however, judges... in deciding the law we must act according to our purest conscience."

NSO Group and the Indian government must be reminded of these words. In the name of fighting terrorism, democracy cannot be undermined. Indian democracy is founded with the cherished ideals enshrined in the Constitution. It belongs to the people and not to political parties. The surveillance of the target group raises doubts about the functioning of democracy in India. The chilling effect, if the government were to succeed, would be to turn democracy into a dictatorship. The government has a constitutional duty to protect the fundamental and human rights of its citizens, irrespective of who they are. Even if the government is not complicit in the surveillance, it has miserably failed in discharging this duty. There is clear evidence that the rule of law has been undermined. More evidently, this reflects extremely poor governance. The Intelligence Bureau, the Research and Analysis Wing, and the National Security Council Secretariat should have forewarned the government and citizens against such surveillance seriously violating privacy and fundamental rights. Their silence speaks volumes about either complicity or poor governance. This being the case, an inquiry at the highest level under the supervision of the judiciary is a constitutional necessity. If this does not take place, India will cease to call itself a democracy.

The Supreme Court, in *K.S. Puttaswamy v. Union of India* (2017), declared privacy a constitutionally protected value. The right to privacy is not absolute and its curtailment can take place only under a law which is just, reasonable and fair and subject to constitutional safeguards.

India is a signatory to the Universal Declaration of Human Rights. Article 12 provides that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The International Covenant on Civil and Political Rights, also signed by India, in Article 17 states, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." In *K.S. Puttaswamy*, the Supreme Court noted India's commitments under international law and held that by virtue of Article 51 of the Constitution, India has to endeavour to "foster respect for international law and treaty obligations..." The Protection of Human Rights Act, 1993 is a fallout of this commitment.

Recommendations of UNHCHR

The annual report of the United Nations High Commissioner for Human Rights (UNHCHR) in 2014 made fundamental observations and recommendations on "digital communications technologies". It said, "by amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights." But "communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection...."

Earlier, due to concerns of member states, the General Assembly adopted Resolution 68/167 affirming that rights held by people offline must also be protected online and called upon all states to respect and protect the right to privacy, including in digital communication.

The UNHCHR report also stated, "Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea..." It recommended an independent oversight body to keep checks and stated, "The International Covenant on Civil and Political Rights requires states parties to ensure that victims of violations of the Covenant have an effective remedy...." The report also dealt with the role of businesses and stated that when a state requires that an information and communications technology company provide user data, it can only supply it in respect of legitimate reasons.

Surprisingly, NSO, in its Transparency and Responsibility Report 2021, informed interested parties that it "strives to guarantee that our products are used... safely, effectively and ethically." If described options available if one of its customers "has acted in bad faith, or used one of our tools to target the electronic communications of someone who falls outside the prescribed target scope." It outlined the range of options available to it if this happened, including "completely ending a customer's access to our systems, as a situation may warrant." It stated, "We very much see today's release as a newly added necessity to the complex, ongoing international debate over electronic surveillance. We are opening our own processes to even deeper scrutiny..." Was this report prepared fearing the worst in the wake of the ongoing international debate?

Indians have a right to call upon NSO to terminate the agreement, if any, with the Indian government or any private player and to cooperate with citizens to unravel the truth.

Dushyant Dave is a Senior Advocate and former President of the Supreme Court Bar Association