Surveillance reform is the need of the hour

The proposed legislation related to the personal data protection of citizens fails to consider surveillance

ANUSHKA JAIN & TANMAY SINGH

AFP

It is worth asking why the government would need to hack phones and install spyware when existing laws already offer impunity for surveillance. This unsettling query arises on the basis of reports emerging from a collaborative investigation by journalists from around the world, including from India's *The Wire*, titled the 'Pegasus Project'. Reports say that over "300 verified Indian mobile telephone numbers, including those used by ministers, opposition leaders, journalists, the legal community, businessmen, government officials, scientists, rights activists and others", were targeted using spyware made by the Israeli firm, NSO Group.

Threat to press freedom

Subsequent reporting showed that the Pegasus spyware had been used to target 37 phones, of which 10 belonged to Indians. Amnesty International's Security Lab was then able to confirm that Pegasus was used to compromise the phones of former journalist of *The Indian Express* Sushant Singh, former editor of the *Economic and Political Weekly* Paranjoy Guha Thakurta, former *Outlook* journalist S.N.M. Abdi, and *The Wire*'s two founding editors Siddharth Varadarajan and M.K. Venu.

These revelations highlight a disturbing trend with regard to the use of hacking software against dissidents and adversaries. In 2019, similar allegations were made about the use of Pegasus against journalists and human rights activists. Most of them were situated in Maharashtra and Chhattisgarh as the hack targeted lawyers related to the Bhima Koregaon case and Dalit activists, respectively. However, despite repeated calls for investigations, the relevant State governments failed to do so.

A significant number of Indians reportedly affected by Pegasus this time are again journalists. This is not surprising since the World Press Freedom Index produced by Reporters Without Borders has ranked India 142 out of 180 countries in 2021. What is shocking, however, is that the press requires (and in democracies is afforded) greater protections on speech and privacy. Privacy and free speech are what enable good reporting. They protect journalists against threats of private and governmental reprisals against legitimate reporting. This has been recognised in Supreme Court decisions. In the absence of privacy, the safety of journalists, especially those whose work criticises the government, and the personal safety of their sources is jeopardised. Such a lack of privacy, therefore, creates an aura of distrust around these journalists and effectively buries their credibility.

Problematic provisions

The government, in its purported undated and unsigned response, relied on existing provisions of law under the Indian Telegraph Act of 1885 and the Information Technology (IT) Act of 2000. Even without the use of Pegasus or any other hacking software and surveillance, these provisions are problematic and offer the government total opacity in respect of its interception and monitoring activities. While the provisions of the Telegraph Act relate to telephone conversations, the IT Act relates to all communications undertaken using a computer resource. Section 69 of the IT Act and the Interception Rules of 2009 are even more opaque than the Telegraph Act, and offer even weaker protections to the surveilled. No provision, however, allows the government to hack the phones of any individual since hacking of computer resources, including mobile phones and apps, is a criminal offence under the IT Act. Nonetheless, surveillance itself, whether under a provision of law or without it, is a gross violation of the fundamental rights of citizens.

The very existence of a surveillance system impacts the right to privacy and the exercise of freedom of speech and personal liberty under Articles 19 and 21 of the Constitution, respectively. It prevents people from reading and exchanging unorthodox, controversial or provocative ideas. Regardless of whether a citizen knows that their email is being read by the government, the perceived danger, founded on reasonable suspicion that this may happen, itself impacts their ability to express, receive and discuss such ideas.

There is also no scope for an individual subjected to surveillance to approach a court of law prior to or during or subsequent to acts of surveillance since the system itself is covert. In the absence of parliamentary or judicial oversight, electronic surveillance gives the executive the power to influence both the subject of surveillance and all classes of individuals, resulting in a chilling effect on free speech. Constitutional functionaries such as a sitting judge of the Supreme Court have reportedly been surveilled under Pegasus without any checks outside the executive wing of government. Vesting such disproportionate power with one wing of the government threatens the separation of powers of the government. In response to a Right to Information (RTI) request in 2013, the Central government had revealed that 7,500 to 9,000 orders for interception of telephones are issued by it every month. However, RTI requests for such information are now denied citing threats to national security and to the physical safety of persons.

The government, in its purported response, stated that any surveillance which takes place happens through a "due process of law". However, the existing provisions are insufficient to protect against the spread of authoritarianism since they allow the executive to exercise a disproportionate amount of power. Such surveillance, when carried out entirely by the executive, curtails Articles 32 and 226 of the Constitution (empowering the Supreme Court and High Courts, respectively, to issue certain writs) as it happens in secret. Thus, the affected person is unable to show a breach of their rights. This violates not only the ideals of due process and the separation of powers but also goes against the requirement of procedural safeguards as mandated in *K.S. Puttaswamy (Retd) v. Union of India* (2017).

Role of judiciary

Thus, in order to satisfy the ideal of "due process of law", to maintain an effective separation of powers and to fulfill the requirements of procedural safeguards and natural justice, there needs to be oversight from another branch of the government. Only the judiciary can be competent to decide whether specific instances of surveillance are proportionate, whether less onerous alternatives are available, and to balance the necessity of the government's objectives with the rights of the impacted individuals. The need for judicial oversight over surveillance systems in general, and judicial investigation into the Pegasus hacking in particular, is also essential because the leaked database of targeted numbers contained the phone number of a sitting Supreme Court judge, which further calls into question the independence of the judiciary in India.

Surveillance reform is the need of the hour in India. Not only are existing protections weak but the proposed legislation related to the personal data protection of Indian citizens fails to consider surveillance while also providing wide exemptions to government authorities. When spyware is expensive and interception is inefficient, the individuals surveilled will be shortlisted by priority and perceived threat level to the existing regime. But as spyware becomes more affordable and interception becomes more efficient, there will no longer be a need to shortlist individuals. Everyone will be potentially subject to state-sponsored mass surveillance. The only solution is immediate and far-reaching surveillance reform.

Anushka Jain is the Associate Counsel (Surveillance and Transparency) and Tanmay Singh is the Litigation Counsel at Internet Freedom Foundation