Source : www.livemint.com Date : 2021-07-20

A SPYWARE SCANDAL THAT CAN’T BE BRUSHED ASIDE

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

If Pegasus was snooping on our public figures, we must find out who exactly was using this invasive tool. So grave a matter calls for an independent probe. We also need a privacy law

In a world of nation-states on perpetual high alert over national security, our right to privacy was compromised even before leaps of technology gave espionage agencies a window to our private lives through smartphones. Technically, it would seem that nobody who ventures online can escape the prying eyes of the state. Pegasus, the spyware developed by Israel’s NSO Group that’s in the eye of our ‘snoopgate’ scandal, is said to enable the complete hijack of a target handset. Beyond relaying voice calls, mirroring its screen elsewhere and extracting data once a phone is bugged, this software is reputedly also capable of using its microphone and camera at the will of a remote spymaster. As befits such an intrusive tool, its maker has claimed it is only available to governments. Allegations of India’s government being among its users had surfaced back in 2019, too, but a flaring list of Indian targets—backed by forensic reports of some break-ins—has only just emerged. It has evoked consternation. And for good reason.

The news-grabber on that list of 300 public figures is the name of Congress leader Rahul Gandhi, though it features a motley bunch of journalists, politicians, businessmen and social activists, few of whose public utterances would indicate a friendly disposition towards the ruling dispensation led by the Bharatiya Janata Party (BJP). If that’s not scandalous enough, it includes Ashok Lavasa, who had a constitutional role as an election commissioner till last August, and family members of a woman who’d accused Rajya Sabha member Ranjan Gogoi of sexual misconduct when he was our chief justice. Prashant Kishor, a poll strategist, finds mention too. This list was drawn from a leak of about 50,000 mobile numbers obtained by Amnesty International and France-based Forbidden Stories before it was analysed by 17 media outlets, including the UK’s Guardian, America’s Washington Post and an Indian news website, The Wire. Among politicians, it is not just opposition leaders whose devices were allegedly bugged (or sought to be), but a couple of serving ministers in the BJP government, too, a charge that has raised the episode’s intrigue quotient. On its part, the Centre has denied any “unauthorized surveillance" of citizens and averred its adherence to protocols on espionage, by which our spooks can intercept private communication only in the national interest, and that too, only after due clearances. Yet, since it is very likely that interceptions of some sort did occur, it is incumbent upon the Centre to issue a clear statement on this specific case. Did it or did it not use Pegasus to spy on these citizens? If NSO’s access policy is not foolproof and a rogue unit or freelance operator is suspected to be behind these violations, we still need to know. Either way, an independent investigation must be instituted right away. This could take the form of a judicial enquiry or a joint parliamentary panel probe.

Even without high-profile individuals under watch, it is unnerving that our phones can be taken over by spyware. Thus, we urgently need to assure everyone of privacy as a fundamental right, as held by the Supreme Court of India, by enacting an appropriate law to safeguard us. The proposed Personal Data Protection Bill of 2019, described as “Orwellian" by some legal experts, would give a central data authority inordinate power over fiduciaries to access our digital trails. Without judicial oversight, this should not be allowed. Further, we should be granted explicit ownership of our personal data. As a proud democracy, we can’t afford to slip the way of a surveillance state.

END