Surveillance reform is the need of the hour

(Mains GS 3 : Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security)

Context:

- Recently, a report emerged from a collaborative investigation by journalists from around the world 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 many phones, of which few belonged to Indians.
- Amnesty International's Security Lab was then able to confirm that Pegasus was used to compromise the phones of many journalists.
- 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.

Press requires greater protection:

- The World Press Freedom Index produced by Reporters Without Borders has ranked India 142 out of 180 countries in 2021.

- Thus, the press requires greater protections on speech and privacy as privacy and free speech enable good reporting.
- They protect journalists against threats of private and governmental reprisals against legitimate reporting.
- 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 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.
- However, no provision 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.

Surveillance systems impact fundamental rights:

- 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.

Absence of parliamentary or judicial oversight:

- There is very little 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.
- 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 were 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.
- 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:

- 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.
- 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 is also essential because the leaked database of targeted numbers contained the phone number of a sitting Supreme Court judge.
- This further calls into question the independence of the judiciary in India.

Conclusion:

- The existing protections as well as proposed legislation related to the personal data protection of Indian citizens fails to consider surveillance while also providing wide exemptions to government authorities.
- As spyware becomes more affordable and interception becomes more efficient, mass surveillance becomes a real threat.
- Thus, the solution lies in immediate and far-reaching surveillance reform which ensure privacy and freedom of speech.