# Pegasus: Privacy and Surveillance in India

July 24, 2021

In response to the finding by a global collaborative investigative project that Israeli spyware Pegasus was used to target at least 300 individuals in India, the government has claimed that all interception in India takes place lawfully. In this scenario, let us know more on the issues involved with surveillance and privacy in India.

**In news:** Laws for surveillance in India, and the concerns over privacy
**Placing it in syllabus:** Security
**Dimensions**

- What is Pegasus?
- Laws for Surveillance in India
- Brief on the provisions of Indian Telegraphic act
- Provisions of IT Act
- Supreme Court observations on Surveillance
- Way forward

## Content:

### What is Pegasus?

- **Pegasus aka Q Suite**, marketed by the NSO Group aka Q Cyber Technologies as "a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract" data "from virtually any mobile devices".
- It was developed by veterans of Israeli intelligence agencies.
- Project Pegasus is revealed to have been used to target hundreds of phones in India, and has grown less reliant

on clicks.

- Pegasus can infect a device without the target's engagement or knowledge.
- Until early 2018, NSO Group clients primarily relied on SMS and WhatsApp messages to trick targets into opening a malicious link, which would lead to infection of their mobile devices.
- A Pegasus brochure described this as **Enhanced Social Engineering Message (ESEM).** When a malicious link packaged as ESEM is clicked, the phone is directed to a server that checks the operating system and delivers the suitable remote exploit.
- In its October 2019 report, Amnesty International first documented use of 'network injections' which enabled attackers to install the spyware "without requiring any interaction by the target".

## How does it work?

- Pegasus can achieve such zero-click installations in various ways.
- One over-the-air (OTA) option is to send a push message covertly that makes the target device load the spyware, with the target unaware of the installation over which she anyway has no control.
- Usually, an attacker needs to feed the Pegasus system just the target phone number for a network injection. "The rest is done automatically by the system," says a Pegasus brochure, and the spyware is installed in most cases.
- Once infected, a phone becomes a digital spy under the attacker's complete control.
- Upon installation, Pegasus contacts the attacker's command and control (C&C) servers to receive and execute instructions and send back the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls (even those via end-

to-end-encrypted messaging apps).
- The attacker can control the phone's camera and microphone, and use the GPS function to track a target.

**What kind of devices are vulnerable?**

- All smart devices, practically.
- iPhones have been widely targeted with Pegasus through Apple's default iMessage app and the Push Notification Service (APNs) protocol upon which it is based.
- The spyware can impersonate an application downloaded to an iPhone and transmit itself as push notifications via Apple's servers.
- In April 2017, security firm Lookout and Google released details on an Android version of Pegasus.
- In October 2019, WhatsApp blamed the NSO Group for exploiting a vulnerability in its video-calling feature.

## Laws for Surveillance in India:

Communication surveillance in India takes place primarily under:

- ***The Telegraph Act, 1885:*** It deals with interception of calls.
- ***The Information Technology Act, 2000 (IT Act) :*** It was enacted to deal with surveillance of all electronic communication, following the Supreme Court's intervention in 1996.
- ***The Indian Post Office Act, 1898***: It allows the Centre and state to intercept postal articles in public emergencies or in the interest of public safety or tranquility.

However, a comprehensive data protection law to address the gaps in existing frameworks for surveillance is yet to be enacted.

## Brief on the provisions of Indian Telegraphic act:

- According to **Section 5(2)** of the Telegraph Act the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may intercept messages transmitted by telegraph lines under certain conditions.
- The government can intercept calls only in certain situations – the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order, or for preventing incitement to the commission of an offence.
- These are the **same restrictions imposed on free speech under Article 19(2)** of the Constitution.
- Even these restrictions **can be imposed only when there is a condition precedent** – the occurrence of any **public emergency, or in the interest of public safety**.
- **Reasons for ordering interception have to be recorded in writing** by the officials concerned.
- A provision in **Section 5(2) states that even this lawful interception cannot take place against journalists.** "Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

## Provisions of IT Act:

- **Section 69 of the Information Technology Act** and the Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were enacted to further the **legal framework for electronic surveillance**.
- Under the IT Act, **all electronic transmission of data can be intercepted**.
- Section 69 the IT Act adds another aspect that makes it broader.

- It allows for interception, monitoring and decryption of digital information “for the investigation of an offence”.
- Significantly, IT Act omits the condition precedent set under the Telegraph Act that requires “the occurrence of public emergency of the interest of public safety”.
- This omission widens the ambit of powers under the IT Act.
- So, for a Pegasus-like spyware to be used lawfully, the government would have to invoke both the IT Act and the Telegraph Act.

## Supreme Court Observations on Surveillance:

### *Public Union for Civil Liberties v Union of India (1996):*

- In **PUCL v Union of India (1996)**, the Supreme Court pointed out lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions.
- A public interest litigation was filed in the wake of the report on “Tapping of politicians phones” by the CBI.
- The court noted that authorities engaging in interception were not even maintaining adequate records and logs on interception.
- The court observed that tapping is a serious invasion of an individual’s privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one’s home or office without interference, is increasingly susceptible to abuse.
- And hence citizen’s right to privacy has to be protected from being abused by the authorities of the day, the court said.
- Among the guidelines issued by the court were **setting up a review committee that can look into authorisations** made under Section 5(2) of the Telegraph Act.

- The Supreme Court's guidelines formed the basis of introducing **Rule 419A** in the **Telegraph Rules in 2007** and later in the rules prescribed under the IT Act in 2009.

***R Rajgopal alias RR Gopal and another Vs State of Tamil Nadu (1994)***:

- the Supreme Court held that the **right to privacy is implicit in the right to life and liberty** guaranteed to the citizens of this country by **Article 21.**

***Puttaswamy vs Union of India (2017)*** :

- The judicial debate on the status of the right to privacy was, however, settled in August 2017 when a nine-judge bench **held that the right to privacy is a fundamental right**.
- The court added that **telephone tapping and internet hacking by the State**, of personal data, is another area that **falls within the realm of privacy.**

**Rule 419A** states that a Secretary to the Government of India in the Ministry of Home Affairs can pass orders of interception in the case of Centre, and a secretary-level officer who is in-charge of the Home Department can issue such directives in the case of a state government.

In unavoidable circumstances, such orders may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary or the state Home Secretary.

## Way forward:

- ***Independent Public Inquiry:*** Institute an independent public inquiry to credibly investigate these allegations, and therefore repair public trust.
- ***Judicial oversight on Surveillance***: To achieve the ideal of due process of law, oversight from another branch of

the government should be established. Considering the gravity, only the judiciary can be competent to decide on such matters. Oversight should involve deciding whether specific instances of surveillance are proportionate, whether alternatives are available, and to balance the necessity of the government's objectives with the rights of the impacted individuals.

- ***Enacting strong data protection laws:*** There is a need for a strong data protection law that protects the individual right to privacy, including protection from surveillance and unauthorized data collection by government agencies.
- ***Ban on the use of private spyware***: A collective decision banning the use of private spyware will be a step forward.

**Impact of surveillance**

***On 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.
- 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.

***Obstructs free exchange of information:***

- It prevents people from reading and exchanging unorthodox, controversial, or provocative ideas.

***Breeds distrust:***

- Surveillance threatens the safety of journalists, especially those whose work criticizes the government, and the personal safety of their sources is compromised. It creates an atmosphere of distrust.

**Mould your thought:** In the wake of surveillance spyware, the only solution is immediate and far-reaching surveillance reform. Critically evaluate.***Approach to the answer:***

- Introduction
- Discuss the issue of Pegasus in brief
- Discuss the impacts of such surveillance
- Mention briefly about the laws on surveillance in India
- Discuss Supreme Court’s view on the matter
- Suggest some solutions
- Conclusion