KHAITAN &CO
Advocates since 1911

UPDATE

ERGO
Analysing developments impacting business

SUPREME COURT ORDERS AN INDEPENDENT INVESTIGATION INTO THE PEGASUS SPYWARE ATTACK

31 October 2021

INTRODUCTION

On 27 October 2021, the Supreme Court of India (Supreme Court) ordered the constitution of a technical committee headed by a retired judge of the Supreme Court to probe into the alleged use of a spyware called Pegasus for surveillance of several citizens of India. The judgment is of particular importance as it addresses the larger impact of the use of surveillance technologies on the fundamental right to privacy, protection of data and freedom of the press, and the need to balance these rights against the security interests of the State.

BRIEF FACTUAL BACKGROUND

The Supreme Court has passed this order in a batch of writ petitions filed before it, under which allegations had been made regarding misuse of Pegasus, to spy on citizens of the country. The petitioners were also seeking an independent investigation into the matter.

Though in May 2019, reports of WhatsApp being compromised by Pegasus first surfaced, in July 2021, a consortium of nearly 17 journalistic organizations from around the world, including one Indian organization, released the results of a long investigative effort indicating the alleged use of the Pegasus software on several private individuals. This investigative effort was based on a list of some 50,000 leaked numbers which were allegedly under surveillance by clients of the NSO Group through the Pegasus software. Initially, it was discovered that nearly 300 of these numbers belonged to Indians, many of whom are senior journalists, doctors, political persons, and even some court staff. At the time of filing of the writ petitions, devices of nearly 10 Indians were allegedly forensically analysed to confirm the presence of the Pegasus software.

The Union of India (UoI) was asked to file an affidavit to clarify its stand regarding the allegations raised, and to provide information to the Supreme Court regarding the various actions taken by it over the past two years, since the alleged Pegasus spyware attack was first disclosed. The UoI had filed a limited affidavit stating that they will constitute a committee of experts to address the issues raised. However, the UoI did not file a detailed counter affidavit citing security concerns.

KEY OBSERVATIONS AND FINDINGS OF THE SUPREME COURT

1. RIGHT TO PRIVACY OF AN INDIVIDUAL TO BE BALANCED AGAINST THE SECURITY INTERESTS OF THE STATE

- In matters pertaining to national security, the scope of judicial review is limited. However, mere invocation of national security by the State is not sufficient to grant it blanket immunity against judicial review. If the State is declining to provide information when constitutional considerations exist such as security of state or immunity under a specific statute, it is incumbent on the State to not only plead but also prove and justify the same to the Supreme Court on affidavit.

- The right to privacy is directly infringed when there is surveillance or spying done on an individual, either by the State or by any external agency. However, if done by the State, the same must be justified on constitutional grounds.

- The legal position laid down by the Supreme Court in the seminal decision of *K.S. Puttaswamy (Privacy-9J.) v. Union of India*, (2017) 10 SCC 1 was reiterated that an invasion of life or personal liberty must meet the threefold requirement of legality, which postulates the existence of law; need, defined in terms of a legitimate State aim; and proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

- The Supreme Court observed that it is cognizant of the fact that information gathered by intelligence agencies through surveillance is essential to fight against violence and terror. To access this information, a need may arise to interfere with the right to privacy of an individual, provided it is carried out only when it is absolutely necessary for protecting national security/interest and is proportional. The considerations for usage of such alleged technology, ought to be evidence based. Further, in a democratic country governed by the rule of law, indiscriminate spying on individuals cannot be allowed except with sufficient statutory safeguards, by following the procedure established by law under the Constitution of India.

2. FREEDOM OF THE PRESS

- Surveillance of the press could result in self censorship by the press itself, directly impinging upon the freedom of the press and consequently on the freedom of speech. This may undermine the ability of the press to provide accurate and reliable information.

- An important corollary of such a right is to ensure the protection of sources of information. Protection of journalistic sources is one of the basic conditions for the freedom of the press.

3. RECOMMENDATIONS SOLICITED FROM TECHNICAL COMMITTEE

The Supreme Court, being satisfied that a *prima facie* case was made out by the petitioners to examine the allegations in the writ petitions, ordered an independent investigation by a Technical Committee comprising of three members, including those who are experts in cyber security, digital forensics, networks and hardware, to be overseen by Justice R.V. Raveendran, former Judge of the Supreme Court. In addition to entrusting the task of investigating

specific questions in relation to the use of Pegasus, the Supreme Court has also solicited recommendations regarding the following from the Technical Committee:

- Enactment or amendment to existing law and procedures surrounding surveillance and for securing improved right to privacy.
- Enhancing and improving the cyber security of the nation and its assets.
- Ensuring prevention of invasion of citizens' right to privacy, otherwise than in accordance with law, by State and/or non-State entities through such spywares.
- Establishment of a mechanism for citizens to raise grievances on suspicion of illegal surveillance of their devices.
- Setting up of a well-equipped independent premier agency to investigate cyber security vulnerabilities, for threat assessment relating to cyberattacks and to investigate instances of cyberattacks in the country.
- Any *adhoc* arrangement that may be made by the Supreme Court as an interim measure for the protection of citizen's rights, pending filling up of lacunae by the Parliament of India.

CONCLUSION

The Supreme Court, in this judgment, has attempted to balance the right to privacy of an individual against the national security interests of the State. The Supreme Court has been cognizant of the evolution of technology in recent times, its growing potential for misuse, and consequent impact on the rights of individuals. It will be of particular relevance to see if the recommendations of the Technical Committee are taken into account during the passage of the Personal Data Protection Bill 2019 in the Parliament of India.

- Anushka Sharda (Partner), Supratim Chakraborty (Partner), Sumantra Bose (Principal Associate), Smriti Ramesh Nair (Associate) and Ankit Chhaparia (Associate)

For any queries please contact: editors@khaitanco.com