BLIND FOLD LEGAL JOURNAL

VOLUME-1 ISSUE-2

E-Mail:- blindfoldjournal@gmail.com

Website: - www.blindfoldjournal.com

Pegasus Spyware: Privacy of People at Peril

By: Riya Sharma

Introduction

The right to privacy is innate and inherent to everyone. It is a fundamental human right to be left alone, free of intrusion or disruption. "A state in which one is not watched or disturbed by other people," according to the Oxford English Dictionary, or "the state of being free from public attention." Article 21 of the Indian Constitution protects the right to privacy, which is an extension of the right to life and personal liberty.[1]However, as technology progresses, the operation of these rights has grown increasingly difficult with the introduction of complex data storage and administration programmes.

Spyware is an example of a potentially dangerous technology that might intrude on one's privacy. Spyware is malicious software that infiltrates a person's computer, mobile device, or other devices in order to collect information about them and send it to a third party without their permission. This type of dangerous software is designed to make money of stolen information. Spying is a violation of a person's privacy, dignity, and freedom to exercise civic and political rights by exerting near-complete control over his or her life. Spyware first appeared in the early 1990s and has since grown into a booming industry with tens of thousands of users. Pegasus is currently the most widely used and functional spyware in the world. The NSO Group (NSO stands for Niv, Shalev, and Omri, the company's founders' names) produced Pegasus, a proprietary surveillance software developed in Israel. Because it provides its developer or owner influence over the user devices, proprietary software does not respect the freedom of its users.

BLIND FOLD LEGAL JOURNAL

How is the use of Pegasus Spyware against the Tenets of Privacy?

When spyware is put on a device, it immediately begins taking images, videos, and other digital data to send to the criminal. It can even record calls and track a target's location while running the phone's microphone and camera on its own and invisibly. The attacker can exploit this feature to listen in on private and sensitive chats and relay them back to the user. Even a missed WhatsApp

[1] India Const. art. 21.

call could start a chain of events that leads to the smartphone being hacked. This demonstrates that claims of end-to-end encryption and security are false and speculative.

NSO Group insists on only licencing its spyware to approved government clients under the pretence of combating international crime and terrorism. To do this, the company entered into its first partnership with Mexico in 2011, while former President Felipe Calderon was still in power, and gave the government its flagship product Pegasus, which is used to follow drug gangs. Pegasus assisted in the arrest of Joaqun Guzmán alias El Chapo, a famous Sinaloa Cartel drug boss, in 2016 by gaining access to his phone and tracking his travels. It's a good thing that this malware is being used to catch criminals and terrorists. According to allegations from 17 news organisations, the NSO-made Pegasus spyware was allegedly used to try to hack into the phones of political leaders in India, the United Arab Emirates, Saudi Arabia, Mexico, Morocco, and Hungary, including heads of state, lawyers, activists, and journalists. There has been evidence of Pegasus's mistreatment in the past. It was related to the suspected hacking of Jeff Bezos' and journalist Jamal Khashoggi's phones by Saudi Arabia's crown prince in 2018.

According to the Pegasus Project, Pegasus has been linked to the monitoring of roughly 300 Indian phone lines, including those belonging to opposition leaders like Rahul Gandhi and leading journalists.[2] 22 of these phones were forensically examined by Amnesty International, which was then peer-reviewed by the Citizen Lab at the University of Toronto.[3] Ten of them were positively recognised as Pegasus targets, while the other eight were unconfirmed. According to The Wire, the database includes over 40 journalists, three prominent opposition leaders, one constitutional authority, two sitting ministers in the Narendra Modi administration, current and former security chiefs and personnel, and hundreds of business people.

BLIND FOLD LEGAL JOURNAL

Existing Privacy and Surveillance Related Laws in India

[2] Joanna Slater & Niha Masih**,** *The spyware is sold to governments to fight terrorism. In India, it was used to hack journalists and others,* THE WASHINGTON POST, , <https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/>.

[3] Bill Marczak et al., *Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware*, THE CITIZEN LAB,(31 October, 2019, 8:58 PM), <https://www.thehindu.com/sci-tech/technology/pegasus-the-spyware-that-came-in-via-whatsapp-how-safe-are-you/article29845259.ece>.

In India, there is no separate personal data protection law that protects personal data and information submitted or acquired. The majority of the safeguards are dispersed throughout a slew of laws, standards, and recommendations. The most essential clauses are found in the Information Technology Act of 2000 (IT Act, 2000). The IT Act of 2000 is the primary law in India that governs electronic trade and cybercrime**.** Section 72 of the IT Act is the only explicit clause dealing with privacy and confidentiality breaches. Anyone who reveals the contents of any electronic record, register, book, or other object without the approval of the person involved faces a two-year prison sentence, a fine of one lakh rupees, or both under Section 72 of the IT Act, 2000.[4]

Awful things can happen when sensitive information slips into the wrong hands. A security breach at a government entity, for example, could provide unauthorised access to critical information. When it comes to data privacy, it appears that users have every option available to them except the one they want, which is data control. Understanding who collects data, where it is stored, how it is used, and what can be done if the data is misused are all part of the Data Protection bill. There have been far too many instances of personally identifiable information being misused, whether anonymised or not. According to Canalys research, the data of nearly three-quarters of the adult population of the country has been in threat since 2017. The majority of these intrusions took place while India pushed its IT reforms, digitising various papers, and the risk of future incursions is certain to increase.

Data Protection Bill

With the increase of user-generated data and the ever-increasing industrial value of data, governments must defend individual data rights more than ever. Personal data is safeguarded by data protection regulations, which control the collection, use, transfer, and disclosure of such information. They also give individuals access to their data and hold businesses that collect personal data accountable, as well as providing remedies for unauthorised or harmful processing. This bill, however, has several flaws. The PDP Bill creates a monopoly in which the state and its agencies will have exclusive access to all personal and non-personal data. While it gives Indians main rights over their personal data, it also gives the federal government exemptions that go against the norms of data processing. This bill safeguards people's fundamental rights, including as their

[4] Information Technology Act, 2000, § 72, No. 21, Act of Parliament, 2000 (India).

right to privacy and data protection, but it also allows the government to process sensitive personal data as needed without the data owners' express approval.

Conclusion

In August 2017, the Supreme Court unanimously confirmed the right to privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution in the landmark case of K. S. Puttaswamy and Anr. v. Union of India and Others.[5] The Supreme Court declared in this landmark decision that privacy is a cornerstone and important component of future judicial battles over the government's surveillance powers. India is a democratic nation with its people at its heart. When instances like Pegasus espionage occur, citizens' fundamental rights are compromised. Surveillance in and of itself is a violation of personal rights, and so breaches both Article 14 and Article 19 of the Constitution. Such an intervention chills the populous, prompting people to practise self-censorship in the event that someone is listening. As a result, it is vital to ensure that every individual has the right to regulate his or her personal data and the ability to govern his or her own life, including the right to control one's own life and online presence.

.

BLIND FOLD LEGAL JOURNAL

[5] *K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Others,* (2019) 1 SCC 1.