International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

RIGHT TO PRIVACY - PEGASUS SPYWARE

PAVITHRAN K

PROV/LLB/9/23/006
SUBMITTED TO PROF.MAMATHA R

ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi
Alliance School of Law

TABLE OF CONTENTS :

ABSTRACT 1
INTRODUCTION 1
RIGHT TO PRIVACY IN INDIA 2
WHAT IS PEGASUS SPYWARE 2
IMPACT OF THIS SPYWARE ON THE RIGHT TO PRIVACY 2
HOW CAN WE HANDLE INVASION BY THIS TYPE OF SPYWARE 3
WHAT’S HAPPENING AROUND THE WORLD? 3
2019 WHATSAPP HACK IN INDIA 3
RECENT STEPS TAKEN IN INDIA 4
WHAT CAN I DO TO BE BETTER PROTECTED? 4
CONCLUSION 4

ABSTRACT :

Pegasus spyware was created by an Israeli company named NSO with the intention of helping governments all around the world with monitoring, mostly to remove wrongdoings. Pegasus spyware is not used to prevent such acts, despite its declared goals; on the contrary, its use has resulted in the infringement of private rights for a number of individuals. For example, it is reported that the Pegasus spyware was used to attack the cell phone of Congressman Rahul Gandhi in order to look at the strategies employed by other political parties. According to a research published by Amnesty International, nearly 1,000 of the 50,000 well-known people who might be the target of this malware are Indian citizens. The Pegasus spyware serves as a vehicle for undermining democracy's foundation. destroying the court's independence and suppressing those who try to reveal the misconduct of those in positions of power. In the case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court rendered a highly regarded decision that cleared the path for the right to be incorporated into the Indian Constitution. The Pegasus software has also violated a number of laws related to surveillance. Furthermore, there have been infractions of many laws related to monitoring as a result of the Pegasus infection. It is noteworthy, although, that the Union Government has stated that it is unable to accept any charge of this kind and has called the claims of such monitoring "baseless, fake, and concocted".

KEYWORDS: Right to privacy, Pegasus spyware, India

INTRODUCTION :

One fundamental human right that protects people from unjustified interference in their private lives is the right to privacy[1]. The idea of privacy has expanded in an era where technological innovations rule, particularly in light of new tools for surveillance and developing technologies. The Pegasus spyware is one notable and contentious example of this. [2]NSO Group, an Israeli cyber security company, developed Pegasus, a potent surveillance tool. Originally intended to fight crime and terrorism, Pegasus has become well-known for its purported abuse in violating people's privacy all over the world.

Spyware has the ability to infiltrate smartphones and grant unauthorized access to messages, calls, personal data, and even the camera and microphone of the device. Pegasus's effects on privacy rights have provoked heated discussions and legal challenges all around the world. Governments, proponents of human rights, and technologists are debating the moral and legal limits of monitoring technologies and the trade-off between personal privacy and

[1] Marlon Brando, Jr. was an American movie star and political activist

[2] https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/microsoft-exchange-email-hack-was-caused-china-us-says-2133991

national security. After it was discovered that Pegasus was being used against political, media, and activist figures, concerns were raised about possible abuse and the necessity of strong regulatory frameworks to shield citizens from unauthorized access.

With the world of digital privacy changing so quickly, the Pegasus spyware is a sobering reminder of the difficulties that come with using advanced monitoring technologies and the need to put protections in place to protect people's right to privacy. It is a delicate task to strike a balance between security requirements and individual rights, and the ongoing discussion surrounding Pegasus emphasizes how urgent it is to establish moral standards and legal frameworks to guarantee the preservation of our inalienable right to privacy.

RIGHT TO PRIVACY IN INDIA :

The right to privacy is becoming increasingly important in India as a result of the Pegasus spyware controversy, as it is being discussed in relation to the intrusion of digital surveillance technologies. The right to privacy was not expressly recognized by the Indian Constitution until the Indian Supreme Court issued a landmark decision in 2017 stating that privacy is an inherent and fundamental right. This acknowledgement creates a constitutional framework that requires the protection of an individual's personal space, autonomy, and control over their digital presence, which has significant ramifications for situations like the Pegasus controversy.[3]

Enshrined in Article 21 of the Indian Constitution, the right to privacy has emerged as a fundamental principle for assessing the conduct of state and non-state actors, especially in the digital sphere. The intrusive powers of the Pegasus spyware to access private communications and sensitive data stands in sharp contrast to the Indian legal framework's protection of privacy. The right to privacy must be weighed against justifiable concerns for public order and national security because it is not an absolute right. Nonetheless, the disclosures regarding the possible mishandling of Pegasus have sparked discussions regarding the appropriateness and requirement of these monitoring techniques, thereby calling for a thorough investigation into whether these measures comply with constitutional requirements.

Thus, in light of the growing threats posed by the digital sphere, the Pegasus controversy offers a critical opportunity for the Indian judiciary, civil society, and policymakers to affirm and defend the inviolability of the right to privacy. The debates sparked by this controversy cover issues like surveillance oversight procedures, legal recourse, and how technology is changing the definition of privacy. India's approach to issues at the nexus of individual liberties, national security imperatives, and the moral application of technology will be greatly influenced by how the country interprets and protects the right to privacy as it navigates the complexities of this digital age.

WHAT IS PEGASUS SPYWARE :

The highly controversial and sophisticated spyware Pegasus was created by Israeli cyber security company NSO Group. It is intended to sneak into and monitor mobile devices—such as tablets and smartphones—often without the user's awareness or agreement. Pegasus is renowned for its ability to remotely access and manage a variety of device functions, such as gathering private information, listening in on conversations, and even turning on the camera and microphone. Pegasus is unique in that it can take advantage of "zero-click" or "no-click" vulnerabilities, which allow the spyware to infect a device without the user having to do anything like click on a malicious link. Because of this, it is especially powerful and challenging to identify.[4]

Governments and law enforcement organizations[5] have been pitched Pegasus as a weapon against crime and terrorism. Its misuse potential, however, has caused serious concerns because reports indicate that it has been used to target politicians, journalists, human rights activists, and other dissenting voices. The claims of abuse have sparked discussions about how to strike a balance between the needs of national security and individual privacy rights. The controversy surrounding the Pegasus spyware began when reports surfaced claiming that governments from all over the world, including India, had been using Pegasus to survey people of interest digitally.

IMPACT OF THIS SPYWARE ON THE RIGHT TO PRIVACY :

The Pegasus spyware has had a notable and worrisome effect on people's right to privacy. Privacy rights have been seriously threatened by spyware's ability to enter devices and gather sensitive data without the knowledge or agreement of persons. [6]The lines separating private and public domains have been blurred by its indiscriminate and clandestine actions, which has violated people's right to privacy over their personal information. Because people may be reluctant to communicate honestly and openly out of concern for being watched, Pegasus's intrusive nature has had a chilling impact on free speech. This self-censorship undermines the fundamental tenets of a thriving society by impeding the free exchange of ideas and inhibiting democratic conversation.

Furthermore, a wide spectrum of people, including journalists, activists, politicians, and dissident voices, may be the focus of Pegasus's surveillance use. This has sparked worries about the improper use of surveillance for goals pertaining to politics or power, which can be harmful to civil liberties, human rights, and the democratic process. Pegasus's scandal has also highlighted the need for stronger legislative protections and supervision

[3]

ipleaders&rlz=1C1CHZN_enIN935IN935&oq=iplead&gs_lcrp=EgZjaHJvbWUqCggAEAAYsQMYgAQyCggAEAAYsQMYgAQyBggBEEUYOTIHCAIQABiABDIHCAMQABiABDIHCAQQABiABDIHCAUQABiABDIHCAYQABiABDIHCAcQABiABDIHCAgQABiABDIHCAkQABiABKgCALACAA&sourceid=chrome&ie=UTF-8

[4] https://www.firstpost.com/tech/news-analysis/pegasus-spyware-a-complete-guide-to-how-it-can-be-used-to-infiltrate-your-phone-7585931.html

[5] https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/pegasus-spyware-what-it-and-how-does-it-work-2134001

[6] https://www.newsclick.in/An-Explainer-Pegasus-Spyware

procedures to guarantee that surveillance technology are applied sensibly, morally, and compliantly with the law. It has provoked discussions on how to best balance privacy rights with security requirements, leading to a reassessment of the wider effects of unrestricted digital surveillance.

In summary, the Pegasus spyware's impact on the right to privacy has shown how critical it is to protect people's privacy in a society that is becoming more digitally and globally interconnected. It has spurred conversations on the need for strict laws, openness, and accountability systems to stop misuse and guarantee that the development of technology does not come at the expense of basic human rights.

HOW CAN WE HANDLE INVASION BY THIS TYPE OF SPYWARE :

An integrated strategy incorporating technological, sociological, and legal measures is needed to handle spyware incursions and prevent such privacy breaches:

Robust Legal Frameworks: States must pass and implement comprehensive legislation that specifically addresses digital surveillance, data breaches, and invasions of privacy. Strict penalties for unlawful access to and misuse of personal data should be imposed under these regulations, together with explicit guidelines for the use of surveillance technologies. Transparency and Accountability: Mechanisms for transparent reporting and accountability should be in place for surveillance operations, particularly those carried out by government organizations. Monitoring by impartial authorities, thorough reporting, and frequent audits can all aid in guaranteeing that monitoring is done lawfully and for justifiable reasons.

Cyber security Precautions: Improving cyber security protections is essential to preventing unwanted access to systems and devices. Frequent patch management, encryption procedures, and software updates can assist protect against security holes that spyware frequently takes use of. Encryption from end to end: Strong end-to-end encryption should be prioritized and put into practice for communication platforms to avoid unwanted message and data interception. This guarantees that the contents are only accessible to the designated recipients.

User education can help stop spyware from being inadvertently installed by raising awareness of potential internet threats including phishing schemes and malicious malware. Higher educated users are more likely to recognize suspicious conduct and avoid it. Ethical Tech Development: Tech companies should prioritize ethics above everything else when creating and deploying surveillance technologies.

Tight guidelines and moral standards might be implemented to help lessen the likelihood of potential abuse. International Cooperation: Since spyware attacks often cross national borders, international cooperation is crucial. Governments and law enforcement agencies should work together to combat cybercrime and address issues related to surveillance. Strong Oversight: Third-party organizations like privacy commissions or ombudsmen can be vital in ensuring that surveillance operations comply with moral and legal requirements.[7]

WHAT'S HAPPENING AROUND THE WORLD?

The main program developed by the Israeli company NSO Group, called Pegasus, is making headlines once more because it can be used to eavesdrop on politicians, businesspeople, journalists, and in certain situations, prime ministers. According to a global alliance of news organizations, thousands of their most outspoken opponents, including journalists, activists, politicians, and business executives, had their phones compromised by spyware created by NSO Group. This included governments in Mexico, Morocco, and the United Arab Emirates.

Amnesty International and the Paris-based media charity Forbidden Stories got a leaked list of 50,000 phone numbers of possible eavesdropping targets, which they then shared with the reporting consortium that included The Washington Post and The Guardian. To verify that the victims were the intended targets of the NSO's Pegasus spyware—which has access to all of a user's data—researchers examined the phones of dozens of victims. New information about the government clients themselves, which NSO Group keeps under wraps, is also confirmed by the reports. One of the NSO's customers is Hungary, a member of the European Union where the 500 million citizens are expected to have a fundamental right to privacy from surveillance.[8] A leaked list of 50,000 phone numbers, which includes possible targets, was obtained by Forbidden Stories. The existence of the Pegasus spyware was verified through an examination of numerous phones. For the first time, the reporting reveals the number of people who are probably the targets of the invasive device-level surveillance by NSO. According to earlier reports, there were hundreds or maybe more than a thousand known victims.

2019 WHATSAPP HACK IN INDIA :

When it was discovered in late 2019 that WhatsApp had been compromised to hack several Indian activists, journalists, and bureaucrats, there were suspicions that the Indian government was complicit. Facebook, the parent company of WhatsApp, revealed on October 30, 2019, that Pegasus was used to target Indian government officials, attorneys, activists, and journalists. It was thought that the activists and journalists had been under surveillance for two weeks running up to the Lok Sabha elections. Coincidentally, in the lead-up to the Lok Sabha elections, a number of Indian numbers that were revealed in the Pegasus Project were added to the target list.

The Indian IT Ministry also requested a thorough answer from WhatsApp about the matter. In response, WhatsApp said that it had twice informed the

[7] https://www.thequint.com/explainers/pegasus-spyware-attack-and-affected-phones-explained

[8] https://techcrunch.com/2021/07/19/toolkit-nso-pegasus-iphone-android/

Indian authorities of the security breach: in May and again in September 2019. It confirmed that the spyware had targeted 121 people in all. [9]The Pegasus Project has discovered a leaked list of targets that includes some of the Indian people that Pegasus targeted via WhatsApp in 2019. These people include academic Anand Teltumbde, lawyers Nihalsing Rathod Jagdish Meshram from Nagpur, activists for adivasi rights Bela Bhatia, lawyer and activist Shalini Gera, activist Rupali Jadhav, and P Pavana, the daughter of the accused in the Bhīma Koregaon case.

Journalist Saurav Das filed a Right to Information (RTI) request in October 2019 to find out if the Indian government had bought or received a purchase order for the Pegasus spyware. "Please refer to your online RTI application dated 23.10.2019 received by the undersigned CPIO [Central Public Information Officer] on 24.10.2019," the Ministry of Home Affairs said. It is advised that the undersigned CPIO does not have access to any such information.

RECENT STEPS TAKEN IN INDIA :

The Cyber Surakshit Bharat Initiative was introduced in 2018 with the intention of educating frontline IT workers and Chief Information Security Officers (CISOs) about cybercrime and enhancing their ability to implement safety measures in all government ministries. The National Cyber security Coordination Centre (NCCC) was established in 2017 with the goal of monitoring incoming internet traffic and communication metadata, or the small bits of information tucked away inside each message, in order to identify and stop cyber attacks in real time. Cyber Swachhta Kendra: This portal was launched in 2017 to help internet users clean their computers and devices by removing malware and viruses. Indian Cyber Crime Coordination Centre (I4C): The government has just opened I4C. The National Cybercrime Reporting Portal has been made available throughout India. CERT-IN, the Computer Emergency Response Team - India: The nodal organization handles phishing and other cyber security concerns.
Law: The 2000 Information Technology Act.
The 2019 Personal Data Protection Bill.

WHAT CAN I DO TO BE BETTER PROTECTED?

While the majority of people are not likely to be the target of this kind of assault, there are still easy steps you can take to reduce your exposure to Pegasus and other harmful attacks. When using your device, only click on links from people and sources you know and trust. Pegasus is installed on Apple products via an Message connection. And a lot of crooks employ the same tactic for spreading malware as well as less sophisticated scams. The same cautions apply to URLs provided through other chat apps or emails.
Verify that all necessary updates and patches for your device are installed. Even though a standardized operating system gives hackers a firm foundation to work from, it's still your strongest line of defence. Don't rely on notifications if you use Android to learn about updates to the operating system. Since the maker of your gadget might not be offering updates, make sure you download the most recent version yourself. It might seem apparent, but you should restrict who has physical access to your phone. To accomplish this, turn on the device's face, finger, or pin locking. A selection of films on the Esafety Commissioner's website walk you through the process of setting up your device securely. Steer clear of free and public Wi-Fi, especially in hotels, especially if you're viewing private data. When you must utilize these networks, using a VPN is a viable option. When possible, turn on remote wiping capabilities and encrypt the data on your device.[10] You will know that your data will be secure even if your device is stolen or lost.

CONCLUSION :

Global debates about privacy rights have resurfaced as a result of the Pegasus spyware issue. Governments, tech firms, and civil society organizations are battling complicated problems related to cybersecurity, surveillance, and human rights. The main focus of the discussion is finding a middle ground between the rights to personal privacy and national security concerns. On the one hand, proponents contend that in an increasingly digital world, surveillance techniques like Pegasus are essential for fighting organized crime, terrorism, and other threats. They stress that in order to safeguard civilians and uphold law and order, robust cybersecurity measures are required. The employment of such instruments, according to governments, is both lawful and required under tight supervision to guard against misuse.

However, detractors have grave worries about the improper application and abuse of monitoring technologies. The Pegasus project exposed the suspected use of spyware to target political opponents, journalists, and activists, violating their right to free speech and privacy. To protect individual freedoms, calls have been made for increased accountability, transparency, and control of monitoring technologies.

The Pegasus spyware issue has intricate and complicated legal and ethical implications. It emphasizes how crucial it is to have thorough legal frameworks, strong oversight mechanisms, and international collaboration in order to guarantee that surveillance operations are carried out legally, in accordance with human rights principles, and to safeguard people's right to privacy. In conclusion, governments, IT businesses, and society at large should take note of the complex issues raised by surveillance technology in light of the Pegasus spyware incident. It is still crucial to strike a balance between the needs of national security and the basic freedoms of speech and privacy. This is a problem that calls for thoughtful thought, discussion, and worldwide action.

[9] https://thewire.in/media/pegasus-project-spyware-indian-journalists

[10] https://www.freepressjournal.in/business/pegasus-spyware-heres-how-you-can-protect-your-phone-from-malicious-software
Electronic