Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Democracy is in Blood and Pegasus holds the Smoking Gun

Abhimanshi Singh[a]

[a] Law Centre II, University of Delhi, New Delhi, India

Received 13 April 2022; *Accepted* 27 April 2022; *Published* 02 May 2022

Democracy is in blood, And Pegasus holds the smoking gun. Pegasus may not leave any virus traces on compromised devices, but it does leave permanent scars on democratic systems across the world. In the new era of the Internet, Clive Humby, a data science entrepreneur, said, "Data is the new Oil," but now it appears that data is no longer the new oil, but it is the world's most valuable as well as an explosive resource which can endanger even democracy. The Israeli malware Pegasus was used to target thousands of people throughout the world, according to a global collaborative investigation study[1]. At least 300 people are thought to have been targeted in India, including two serving Ministers, three Opposition figures, one constitutional Authority, several journalists, and business people. This research paper will explore Pegasus spyware, its origin, how it intrudes on a device, the use of Pegasus, and techniques that are being used to steal information. This study report also discusses snooping, Indian data protection and snooping laws, regulations from other countries, and what the Government should do in present circumstances. There is a need for revamp of India's surveillance regime, which should include surveillance ethics and take into account the moral implications of how surveillance is carried out. A comprehensive debate is required before the Personal Data Protection (PDP) Bill, 2019[2] Is passed. So that the law may be assessed against the pillars of fundamental rights, digital economic growth, and national security.

Keywords: *data protection, democracy, malware, snooping, surveillance.*

[1] 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*, July 19, 2021) <https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/> accessed April 05 2022

[2] Personal Data Protection Bill, 2019

INTRODUCTION

Pegasus is a word that came from Greek Mythology which means a **white Color Horse-like** creature who has wings. But today, in the era of the internet and data, Pegasus is dreadful software spyware that secretly gets into your smartphone or computer and gives your data to another person. It is a modern way of spying. Pegasus attacks covertly and, once infected, can access the camera microphone and can do virtually anything like reading private WhatsApp chats and SMS, recording calls, monitoring the numbers that have been called, and can access photos, get location by tracking your GPS. It can access passwords and contact details. It can extract all data to give to someone else. Snooping is its ulterior motive and will become your worst enemy. Data has become a new currency for exchange in the new era of cheaper internet.

ORIGIN OF PEGASUS

Pegasus spyware was created by an Israeli Company named The NSO Group. N-Niv Carmi, S-ShalivHuli, and O-OmriLavie are the founders of the company. In August 2016, Pegasus' iOS hack was discovered. Ahmed Mansoor, an Arab human rights campaigner, received a text message promising "secrets" concerning torture in UAE jails if he clicked on a link. Mansoor forwarded the link to Citizen Lab, which investigated with the help of Lookout and discovered that if Mansoor had followed the link, his phone would have been jailbroken and spyware installed, a kind of social engineering. The attack was related to the NSO Group, according to Citizen Lab. Researchers disclosed that Pegasus was accessible for Android as well as iOS during Kaspersky Lab's 2017 Security Analyst Summit; Google refers to the Android version as Chrysaor, the winged horse Pegasus' sibling. It has similar functionality to the iOS version, but it attacks in a different way. If it fails to get root access (equivalent to jailbreaking in iOS), the Android version asks the user for permissions that allow it to gather at least some data. Only a few Android smartphones were affected at the time, according to Google.

The New York Times and The Times of Israel both reported in 2013 that the United Arab Emirates appeared to be utilizing this spyware. From 2012 to 2014, it was utilized in Panama

by former president Ricardo Martinelli, who established the Consejo Nacional de Seguridad (National Security Council) to oversee its implementation. Several lawsuits filed in 2018 claimed that NSO Group assisted clients in using the software and so participated in multiple human rights violations perpetrated by its clients.

HOW DOES PEGASUS ENTER INTO YOUR DEVICE?

It was history when a link was sent through SMS/mail and once needed to click on the link to allow the spyware to enter into the device. But Pegasus is different from other spyware; there is no need to send a link. It requires only to send a Whatsapp message or give a missed call to the targeted device. It just needs a phone number of a person to attack their device. It can infect Android and, surprisingly, is able to infect all IOS versions as well, which is best known for its privacy and safety, through a zero-click message which does not require any interaction from the target.

USE OF PEGASUS

Although NSO claims that they made this software for government agencies to fight crime and terrorism, the forensic method report shows that this is not true. The Mexican government claimed that it had used it to capture Mexican Drug Lord El Chapo, but on the other side of the allegedly leaked data, it claimed that the Mexican Government used the spyware to monitor a journalist. The reporter exposed the government corruption scam and was later found dead. The Washington Post reporter was allegedly assassinated by the Saudi Arabian Government. Now an agency found that the reporter had a Pegasus spyware on his phone. Forbidden Stories and Amnesty International, a non-profit media organization based in France, obtained leaked records of more than 50,000 phone numbers, which were selected by NSO clients for snooping. As Project Pegasus will show, many of them are not afraid to target human rights defenders, businessmen, journalists, political rivals, and even heads of state as the target of this intrusive technology. According to the analysis of these records by Forbidden Stories and its partners, at least 10 NSO clients have selected the phone calls of approximately 180 journalists in 20 countries/regions. These government clients range from democracy (India and Mexico) to autocracy (Bahrain, Morocco, and Saudi Arabia), all over the world, from

Hungary and Azerbaijan in Europe to Togo and Rwanda in Africa. As Project Pegasus will demonstrate, many of them are not afraid to target this intrusive technology against journalists, human rights defenders, political opponents, businessmen, and even heads of state.

TECHNIQUES THAT ARE BEING USED TO STEAL INFORMATION

Many kinds of techniques are being used by cybercriminals to get information about others. Spoofing and snooping are most common in them. In spoofing, cybercriminals send messages disguising themselves as genuine persons or entities. Technically spoofing criminals hide their identity. It can be done by using a bogus email id or fake computer I.P. address. Snooping is unauthorized or unwarranted access to a person's or company's data. It is not limited to gaining data during transactions but also covers the observance of someone else's emails, reading chats, or monitoring someone's activity through some sophisticated snooping software.

IS SNOOPING ILLEGAL IN INDIA?

Section 69 of the Information Technology Act, 2000[3], And section 5[4] of the Telegraph Act, 1885, empower union and state governments to "intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to above or for investigation of any offense." It means that it can only be done by the Government, not by anyone else, and only in the interest of India's sovereignty and integrity. The Government has given roughly ten entities the Authority to spy on civilians. In the interest of state security, public order, India's sovereignty, integrity, and good ties with foreign governments, the new Personal Data Protection Bill of 2019 allow the Government to exclude its agencies from processing personal data. In the ***Public Union for Civil Liberties v Union of India (1996)***[5]The Telegraph Act lacks

[3] Information Technology Act, 2000, s 69
[4] Telegraph Act, 1885, s 5
[5] *Public Union for Civil Liberties v Union of India* AIR 1997, SC 568

procedural safeguards, according to the Supreme Court, and observed that "*tapping is a serious invasion of an individual's privacy. It is no doubt correct that every Government exercises some degree of the surveillance operation, but at the same time, citizens' rights to privacy have to be protected*".

OTHER INSTANCES OF SNOOPING IN INDIA & WORLD

Snooping has been continuous for many decades, although the modes have varied. One of the major scandals in the USA involved president Richard Nixon from 1972-to 74. On June 17, 1972, the Watergate scandal erupted. Early in the morning, when five burglars were captured at the Democratic National Committee's office in Washington, D.C.'s Watergate complex. The robbers were linked to President Richard Nixon's reelection campaign when they were caught listening on phones and taking documents. Nixon tried everything he could to conceal the crimes, but after Washington Post reporters Bob Woodward and Carl Bernstein revealed his role in the plan, Nixon resigned on August 9, 1974. The Watergate scandal changed American politics forever, causing many individuals to distrust their leaders and cast doubt on the presidency. In the 1970s, S.C. started investigating numerous cases of wiretapping. In its report, the Second Press Commission, established by the Morarji Desai government in 1978, mentioned this ailment, saying, "very infrequently, the Press in general, and its editorial echelons in particular, have to suffer from telephone tapping." However, the first landmark case came before S.C. when the NGO 'People's Union for Civil Liberties' petitioned the Court for accountability after a news magazine called 'Mainstream' published a report in 1991 regarding the Government's unauthorized interception of over 300 phones. On December 18, 1996, the Supreme Court issued a decision in which it adopted Kapil Sibal's suggestions for a strong procedural safeguard to prevent snooping. The Supreme Court found that the right to privacy is a part of the right to life and that the Indian Telegraph Act's five reasons are valid that a government can use to intercept telephone conversations or messages would not be used unless "a public emergency has occurred or the interest of public safety so requires." According to the Supreme Court, such occurrences should not be kept hidden and should be made public to a sensible individual. In Indian politics, snooping on individuals is nothing new. Not only people but also high constitutional authorities have been subjected to illegal surveillance by at least two Congress prime ministers in the past. According to the former joint

director of the Intelligence Bureau (I.B.) Maloy Krishna Dhar's book Open Secrets, India's Intelligence Unveiled, former Prime Minister Indira Gandhi was the first leader to authorize illegal surveillance. The intelligence service spied on all of her friends and recorded their conversations. The I.B. also kept a close check on Maneka's editorial board, which was in charge of the magazine. Snooping scandals have surfaced in India throughout the years as a result of the release of a range of materials. It could be the leaking of interception orders, which caused then-Karnataka Chief Minister Ramakrishna Hegde to quit in 1988; the physical presence of intelligence personnel (which resulted in the Chandra Shekhar government's demise in 1991); the audiotape leak (Tata Tapes, initially reported in 1997 by The Indian Express); or the leak of whole transcripts from a target placed under authorized interception on pen drives (Radia Tapes, 2010).

Other incidents occurred, such as the leak of a secret letter written by then-Finance Minister Pranab Mukherjee to then-Prime Minister Manmohan Singh, informing him that his office was suspected of being bugged((2011, as reported by The Indian Express); and the "snoop gate" in Gujarat (2013), in which audio records of alleged conversations of a woman architect were allegedly leaked, purportedly at the behest of then-Chief Minister.

In addition, Income Tax officers recovered Blackberry Messenger (BBM) chats from the laptop of meat exporter Moin Qureshi. (2014, The Indian Express).BBM services were thought to be impermeable to snooping at the time, much as apps such as Whatsapp, Telegram, and Signal, which guarantee end-to-end encryption, were believed to be safe until now.

LAWS IN INDIA DEALING WITH DATA PROTECTION

Information Technology Act, 2000

Section 43A[6] of the I.T. Act creates a legal responsibility on a body corporate (such as a firm, sole proprietorship, or different affiliation of people involved in industrial or expert activities) that possesses, deals, or handles any sensitive information, private statistics, or records in a computer resource that it owns, controls or operates to pay damages with the aid of using manner of compensation, to the individual affected if there's any wrongful loss or wrongful

[6] Information Technology Act, 2000, s 43A

advantage to any individual triggered due to the negligence in enforcing and maintaining reasonable protection practices and strategies to shield the records of the individual affected. As per section 72A[7] of the I.T. Act, any person (including a middleman) who, while providing services under the conditions of a legal contract, has secured access to any material carrying personal information about another person with the intent of causing or knowing that he is likely to cause wrongful loss or wrongful gain reveals, without the assent of the concerned person, or in breach of a legal contract, such action to any other person, shall be punished with incarceration for a period which may extend to three years, or with the penalty which may extend to five lakh rupees, or with both. I.T. Rules give the right to people with regard to their sensitive personal information and make it compulsory for any entity to publish an online privacy policy. It also gives people the right to access and rectify their information and makes it obligatory for an entity to get consent prior to disclosing sensitive personal information except in the case of law implementation, which provides individuals the ability to revoke consent.

Indian Copyright Act

Section 63B[8] The Indian Copyright Act provides that any person who knowingly makes use of an infringing copy of a computer program shall be punishable for a minimum period of six months and a maximum of three years in prison."

It is important to note that the Indian courts recognize copyright in databases.

Indian Penal Code

Data privacy breaches are not particularly addressed in Indian criminal law. Liability for such violations must be derived from related crimes under the Indian Penal Code. For example, dishonest misappropriation or conversion of movable property for one's own use is punishable under Section 403 of the Indian Penal Code.[9]

[7] Information Technology Act, 2000, s 72A
[8] Indian Copyright Act, 1957, s 63B
[9] Indian Penal Code, 1860, s 403

Data Protection Bill 2019[10]

The Supreme Court 2017 in the Puttaswamy Case[11] held that Under Article 21[12]The right to privacy is a basic right that flows from the right to life and personal liberty. The Government constituted a committee led by Justice B. N. Srikrishna to look into numerous privacy issues. The Committee presented the Ministry of Electronics and Information Technology with a draft of the Personal Data Protection Bill, as well as its report. The Ministry of Electronics and Information Technology introduced the Personal Data Protection Bill 2019 in the Lok Sabha on December 11, 2019. The Bill differs from the draft Proposal in various ways. For example, as social media intermediates, the Bill has created a new class of key data fiduciaries. Intermediaries will be among them, allowing people to interact online. Furthermore, the Bill broadened the scope of government exemptions, allowing the Government to direct data fiduciaries to give it any non-personal or anonymized data for improved service targeting. The Bill governs personal data, including the acquisition, processing, and storage of such information. Data fiduciaries are individuals or entities who decide on the means and purposes of data processing. The Bill governs both the private and public sectors when it comes to personal data. It also governs international corporations that process the personal data of Indian citizens. In the interests of national security, public order, India's sovereignty, integrity, and good ties with foreign governments, the Central Government may provide exemptions to any of its agencies from processing personal data. Individuals with respect to their personal data have certain rights under the Bill, such as obtaining confirmation of whether their personal data has been processed, requesting data correction or erasure, requesting data transfer to other fiduciaries, and restricting continued disclosure of their personal data. Any processing of personal data is possible only with the consent of the data subject. However, personal data can be processed without the agreement of the data subject in specific instances, such as when the state is needed to provide benefits to the individual, to conduct legal proceedings, or respond to a medical emergency. The law proposes establishing

[10] Personal Data Protection Bill, 2019
[11] 'Judgment of the Court in Plain English (I)' (*Supreme Court Observer*) <https://www.scobserver.in/court-case/fundamental-right-to-privacy/judgement-of-the-supreme-court-in-plain-english-i> accessed April 06 2022
[12] Constitution of India, 1950, art. 21

a Data Protection Authority to oversee the processing of personal information. Experts in the fields of information technology and data protection will make up the Authority. A complaint can be made to the Authority by anyone. It will be possible to appeal its decision to an Appellate Tribunal. The Supreme Court of India hears appeals from the tribunal.

LAW IN OTHER COUNTRIES CONCERNED WITH PRIVACY

As data is traveling around the world through a borderless network, data protection has become a global concern, and it has become more imperative for the Government to come up with data protection laws. Around 130 countries have data protection laws as of January 2021.

United Kingdom

The United Kingdom is administered by the Data Protection Act 2018, which includes provisions of the EU GDPR. Data subject rights, "special category" personal data, data protection costs, data protection offenses, consent from youngsters, and enforcement are the highlights of the Data Protection Act 2018. Article 5[13] of the UK GDPR lays out seven key principles that are at the heart of the general data protection system. "Lawfulness, fairness, transparency," "purpose limitation," "data minimisation," "accuracy," "storage limitation," "integrity and confidentiality(security)," and "accountability" are the broad concepts. Failure to follow the principles could result in exceptional fines. Infringements of the basic principles for personal processing data are subject to the highest tier of administrative sanctions, according to Article 83(5)(a)[14]. A punishment of up to £17.5 million, or 4% of your entire global yearly turnover, whichever is higher, could be imposed.

United States of America

Instead of having single legislation for data protection, the country follows a sectoral approach for data protection and relies on sector-specific and state laws. There are around 20 sector-specific and more than 100 laws at the state level. California alone has 25 laws concerning privacy issues. The California Consumer Privacy Act(CCPA)[15] sets out four rights for residents of California that enhance their power over their personal data: right to notice, right to access,

[13] General Data Protection Regulation, 2016, art. 5
[14] General Data Protection Regulation, 2016, art. 83(5) (a)
[15] California Consumer Privacy Act, 2018

right to opt-in or out, and right to equal services. Any institution or corporation that collects their personal data must comply with CCPA. In Virginia, Consumer Data protection will come into effect on January 1, 2023. After the enactment of this law, all business entities must have to take the users' permission to process their data. Consumers have the right to request, inspect, correct, and delete personal data under the law. The Privacy Act of 1974, the Privacy Protection Act of 1980, the Gramm-Leach-Bliley Act of 1999, the Health Insurance Portability and Accountability Act of 1996, and the Fair Credit Reporting Act of 2018 are the most important national legislation.

Australia

Australia's Privacy Act 1988[16] is the most important privacy statute that applies to both the public and private sectors. This Act is based on 13 Australian Privacy Principles (APPs), which include data collection, use, and disclosure, data quality, openness and anonymity, and the rights of data subjects. Aside from that, state privacy regulations and sector-specific data protection rules govern data protection. Institutions that collect, use, or disclose health data, for example, are subject to special Health Privacy Principles. The Information Privacy Act 2009 will also apply to organizations in Queensland that personal process data.

Argentina

Argentina's Personal Data Protection Act 2000[17] applies to anybody or anything in the country who works with personal information. It stipulates that data can only be acquired with the consent of the person and that the subject has the right to access, correct, and delete their data. The country is seeking to update its data protection legislation to comply with the GDPR.

France

To better accommodate the GDPR and its new requirements, France's Data Protection Act 2 replaces the Data Protection Act (Act No. 78-17). The Data Protection Act of 2016 establishes standards for data controllers, processors, and recipients when it comes to personal information. According to the Act, all data processing must be done legitimately, for a valid

[16] Privacy Act, 1988
[17]Argentina Personal Data Protection Act, 2000

purpose, and fairly, with just the bare minimum of data being acquired. The Data Protection Act 2 also establishes a number of rights for data subjects, including the right to know the name of the data controller, as well as the right to gather or transfer data.

Germany

Germany has long been and continues to be a leader in privacy protection, with strong regulations that provide greater protection than many other countries. The country's Federal Data Protection Act 2017 (Bundesdatenschutzgesetz – BDSG)[18] replaced the Federal Data Protection Act of 2001 and worked in tandem with the GDPR to define the broad obligations of data collectors and processors. The BDSG's regulations apply to both private and public entities that acquire or handle personal information (with several exceptions). The BDSG's main components are the designation of a PDO, credit check and score requirements, employment-related data processing rules, and criminal law provisions. The BDSG also covers legislation on data transfers, subject rights, informed consent, and other topics.

JUDGMENT OF SUPREME COURT DEALING WITH RIGHT TO PRIVACY

The importance of data increases exponentially as people generate it by consuming inexpensive internet, and here privacy comes into question. This has been raised many times in the Supreme court. Initially, the Supreme Court's view regarding privacy was different. In ***M.P.Sharma v Satish Chandra, District Magistrate***[19] the Supreme Court ruled unanimously that "*the right to privacy is not a fundamental right.*"In ***Kharak Singh v the State of UP***[20] The Supreme Court ruled that our Constitution does not safeguard our right to privacy. But with the passage of time, perception of the Supreme Court has changed. In ***Rajagopal & Ors. v the State of Tamil Nadu***[21] the right to privacy is implied in the right to life and liberty given to inhabitants of this country by Article 21," the Supreme Court wrote. It is a "right to solitude." A citizen has the right to protect his or her own privacy, as well as the privacy of his or her family, marriage, reproduction, maternity, child-bearing, and education." In ***People's Union***

[18] Federal Data Protection Act, 2017
[19] *M.P.Sharma v Satish Chandra, District Magistrate* (1954), AIR 300
[20] *Kharak Singh v State of UP* (1963), AIR 1295
[21] *Rajagopal & Ors. v the State of Tamil Nadu* (1995), AIR 264

for Civil Liberties v Union of India,[22] The Supreme Court attempted to resolve the issue of telephone tapping by establishing precise standards for the use of executive surveillance power. The Court further evolved the notion of privacy to include personal communications, holding that "*the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy.*" To the general reader, it may appear reasonable that this expanding idea of privacy has expanded to include internet conversations.

In **Justice *K.S.Puttaswamy (Retd) v Union Of India***[23]The Supreme Court's nine-judge bench overturned the M.P Sharma and Kharak Singh cases, unanimously recognizing that Article 21 of the Constitution guarantees the right to privacy as an integral aspect of the right to life and personal liberty. The Court also acknowledged that the right was not absolute but that it might be limited if it was established by law, corresponding to a legitimate state goal, and was commensurate to the goal it aimed to achieve.

INDIA'S RECENT INITIATIVES

Cyber Surakshit Bharat Initiative

It was launched in 2018 with the purpose of enhancing cybercrime awareness and increasing the capacity of Chief Information Security Officers (CISOs) and frontline I.T. staff across all government departments to implement security measures.

National Cyber Crime Coordination Center (NCCC)

The NCCC was established in 2017 to analyze internet traffic and communication metadata in order to detect real-time cyber threats (which are little pieces of information buried inside each communication).

Cyber Swachhta Kendra

This system was launched in 2017 to assist internet users in eliminating viruses and malware from their computers and devices. The Cyber Swachhtakendra (Botnet Cleaning and Malware Analysis Centre) is part of the Indian Government's Digital India initiative, which aims to

[22] Public Union for Civil Liberties (n 5)
[23] *Justice K.S. Puttaswamy (Retd) v Union Of India* (2018) Writ Petition (Civil) No. 494/2012

create a secure cyber space by detecting botnet infections in India and notifying, enabling cleaning, and securing end users' systems to prevent further infections. The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center) was established to meet the goals of the country's "National Cyber Security Policy," which aims to create a secure cyber ecosphere. This center works in close partnership with Internet Service Providers and Product/Antivirus Manufacturers.

Indian Cyber Crime Coordination Center (I4C)[24]

I4C was recently founded by the Government. The I4C is a seven-part system that incorporates a cybercrime reporting portal, threat analysis, capacity building, research and innovation, a cybercrime management ecosystem, and a cooperative cybercrime investigation platform for law enforcement agencies. The portal allows for the reporting of all cybercrimes, with a focus on crimes against women and children, including child pornography, child sex abuse material, and internet materials related to rapes/gang rapes.

LACUNA IN INDIAN LAWS

India's existing data privacy regulations are significantly more restrictive. The two primary statutes that control data privacy are the Information Technology Act of 2000 (I.T. Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. (Privacy Rules). The current data protection legislation in India indicates a gap that the Government must solve. The Rajya Sabha Bill introduced in 2019 was a step in the right direction. It was the first personal data protection law in the country. This bill seeks to repeal section 43A of the Information Technology Act, which is one of only two provisions dealing with the subject. Despite the fact that privacy is widely acknowledged as a basic human right, India's legal system has failed to give enough protection to its citizens. As a result, consumers are finding it more difficult to understand how and what information is being saved, recorded, and shared. For example, the recent software version update by WhatsApp created much hue and cry. To avoid further data breaches, strict adherence to data

[24] 'Amit Shah opens cybercrime facility' (*The Hindu,* January 10, 2020) <https://www.thehindu.com/news/national/amit-shah-opens-cybercrime-facility/article30537165.ece> accessed April 08 2022

protection rules is required. History serves as a stark reminder of how readily data may be abused.

WHAT DOES INDIA NEED TO DO?

Snooping has been a harsh reality since Chanakya's time, and it has evolved more as human beings establish themselves as a statesman and political unit. The government recognized it in compelling situations, but while doing so, it constituted a great threat to democracy. Pegasus may not leave any traces of infection on compromised smartphones. However, it has the potential to weaken the roots of democracy which is the independence of the people. It's a frightening demand for surveillance legislation change. The first flaw is that the sanctioning officer, the home secretary, is on the same level as the heads of ten other agencies who are authorized to do surveillance in compelling circumstances. Furthermore, the oversight system is inadequate, with the Cabinet secretary and two additional secretaries making up the committee. To restore public faith in the system, the number of cases of rejection by the oversight committee or refusal of sanction to intercept should be made public. In other words, the oversight committee's decision-making process must be transparent. This unhampered power of interception needs parliamentary or judicial oversight. This Authority can be used in circumstances of public safety, criminal inquiry, and national security. The Supreme Court's 2017 privacy decision makes it mandatory that such interventions meet the proportionality, necessity, and legality requirements. The Opposition's non-compliance with Parliamentary functions is not a correct way to deal with the issue. What works for one political party when it is in power will not work while it is in Opposition. Thus, all parties must work together, with the Government committing to begin surveillance reform. After examining the benefits and drawbacks of judicial and parliamentary monitoring, the Opposition should join this collaborative effort to draught the idea of a new regulation or directive. Intelligence agencies should be brought under parliamentary oversight by introducing legislation. It will benefit all parties, including the victims.

CONCLUSION

Privacy has both beneficial and unpleasant characteristics. The disadvantage is that it prohibits the Government from interfering with a citizen's life and liberty. Because of its positive content, the Government is obligated to take all reasonable precautions to preserve an individual's privacy. National security is critical, but the blindfolded pursuit of it can jeopardize human rights and civil liberties. The use of surveillance has serious privacy implications. However, the list of people targeted suggests that national security is being used as a pretext in India to repress political and societal dissent. The Pegasus discoveries represent a direct assault on Indian democracy and citizens. Was the Government directly involved in the surveillance of a small number of Indian activists, politicians, journalists, and others? Was the surveillance carried out at the request of a private party? With the Government in denial, the mystery can only be solved by a commission of inquiry led by a sitting Supreme Court judge...In the current circumstances, the judiciary is the only institution that can hold the Government accountable. In recent years, our Supreme Court's track record on significant issues of defining importance to our national life has been, at best mixed. What it decides to do or not do today will have an impact on India. The possibilities in front of it are both plain and stark. One is to give the current government carte blanche to convert India into a surveillance state. The other option is to halt the Government's progress and restore to the people the gift of a free and liberal state that the Republic's founding fathers bestowed upon them. Indians have the right to demand that the truth behind Pegasus spyware and its alleged misuse must be exposed, and citizens' right to privacy must be safeguarded without jeopardizing national security concerns. Ultimately democracy must blossom in legal text and in the life of the people.