# PEGASUS: SURVEILLANCE IN OUR TIME; LAW AND IMPACT

Abhishek Singh Bhandari, Law Centre II, Faculty of Law, Delhi University

## ABSTRACT

Pegasus spyware, named after a mythical winged horse from Greek mythology, although not divine in nature, yet, confers a god like power of being omniscient to the bearer. A leaked data revealed a list of phone numbers which were believed to be individuals of NSO's client's interest. Identification of some of the numbers appeared on the list was shocking as most of them belonged to journalists, social rights activists, lawyers, politicians. Profession of individuals whose name appeared on the leaked list and NSO's statement of providing Pegasus spyware service only to governments indicates the government's involvement in the alleged surveillance. Use of this spyware can lead to denial of the right to privacy and freedom of speech which are basic human need guaranteed by our Constitution. Thus, it is pertinent to question the legality of use Pegasus spyware for which deliberate study of The Telegraph Act and Information Technology is required. There are laws to direct the interception of messages in very specific circumstances under the Telegraph Act and Information Technology Act but not clear enough.

Another important question is what degree of impact it would have on the privacy and freedom of speech rights, psychology, and government-citizen relationship. Such incursion into the privacy of citizens by the government would only diminish the trust and faith of people in governmental institutions which could be extremely detrimental for democracy.

## Introduction

We are in an era of technology where almost every task is completed within a fraction of a second with the help of technology. It has made our life smooth and is an integral part of the development of civilization. But with the warmth of the fire, there is always the danger of burning. Our dependency on technology also makes us susceptible and vulnerable to fraud, misinformation, and manipulation to such an extent which we never could have expected before the social media boom. For instance, HACKING, operating, or accessing data or information of a person without his consent by a third party, is a common term in today's world has a plethora of consequences on our society. In today's world information is everything. For the government, information of their subjects i.e., public works as a tool to execute effective measures to provide safety and protection against the people with malicious or criminal intent. For companies, selling their goods and services, having information about their consumers help them to create, produce and provide customer-compatible products which is the backbone of their businesses. All of the social networking apps in our smartphones work as a black hole hungry for information which intimates the apps parent companies about what we like to eat, which clothes we prefer, where we like to go etc. This information is then sold to other companies to create a market that now knows about the needs, preferences, and economic conditions of the consumers and which leads to targeted ads. This much is old and already known to most of the people and to some extent acceptable also. But recent surveillance attempts by a spyware software called Pegasus which is alleged to be only in possession of the governments take information gathering and surveillance to a whole different level. The Guardian unveiled the unethical and malicious use of this spyware to snoop phones and computers of many socially important people, especially Human rights activists, Journalists, and Politicians around the globe. It is not the first attempt to violate the right to privacy of individuals, in 2013 similar numerous global surveillance programs were revealed by Edward Joseph Snowden an American former computer intelligence consultant, who was an employee and subcontractor for the Central Intelligence Agency (CIA). His disclosures revealed that the National Security Agency (NSA) with the cooperation of telecommunication companies was running many surveillance programs in the name of national security.

## Origin of Pegasus and its characteristics

The Pegasus spyware creation of an Israeli-based cyber intelligence firm NSO group has been

designed to retrieve all data by hacking into the phones or computers without the consent of the user and then delivering it to the third party spying on you. However, the parent company claims it to be designed to use against terrorists and serious criminals and that they only give this service to military and government agencies. The government's silence on this implies that either it is the one who is spying on the citizens of the country or someone about whom the government has no idea, which is more concerning.

The investigation conducted by The Guardian at the side of sixteen alternative organizations discovered widespread and continued misuse of NSO's hacking spyware, Pegasus. The leaked list consists of 50,000 phone numbers that are believed to be of individuals of NSO's client's interest. The presence of numbers in the list does not reveal whether a device was infected with Pegasus or subjected to an attempted hack. However, the consortium believes that the data is indicative of the potential targets NSO's government clients identified in advance of possible surveillance attempts. Forensic analysis conducted on a small number of phones whose numbers appeared in the list proved that half of the phones were subjected to the Pegasus spyware. Pegasus spyware was first discovered by researchers in 2016 when a human rights activist from the United Arab Emirates received a text message that was actually a phishing setup. After analysis, it was found that had he opened those links, his phone would have been infected with the malware, named Pegasus.

Spear phishing is a technique used by hackers to trick the targeted person to click on the malicious content sent by them to gain access to the target's phone.

In 2019 this spyware again surfaced as WhatsApp revealed that NSO's spyware had been used to send malware to more than 1400 phones by exploiting a zero-day vulnerability.

A zero-day vulnerability is a computer-software vulnerability that subsists in the device and is unknown to the manufacturers.

In the 2019 attack, the version of the Pegasus spyware used was more effective and efficient than in 2016. Devices were infected only by WhatsApp calls, whether you answer it or not. It followed the zero-click method i.e., the device owner isn't required to click on the message, mail, link, etc to give any input to make the malware work. Once your phone has contracted pegasus spyware, your phone will become a pen text for a third party who can now access your text messages, contacts, email, photos, and even passwords of all your accounts. The access is

to such an extent that the third party can even turn on the mic and camera of your device very conveniently and can turn your beloved phone against you by using it as means of surveillance tool.

**Legality of Pegasus**

Indiscriminate spying by the means of Pegasus spyware has come up as a major threat to the right to privacy. Recently it was accentuated by the Supreme Court that surveillance and spying conducted on an individual, whether by state or by any external agency, directly infringes the right to privacy. Till now Central government has refused to give any detail whether they are using the alleged spyware software or not. It was stated by the Central government in its limited affidavit that it is better for national security that terror organizations do not know which software has been used to combat terror. Nowadays it has become expedient for the government to use it as a ground to escape accountability. How the courts are supposed to safeguard the rights of the citizens if government keeps escaping answering its questions on the pretense of national security.

Some may assume that surveillance by using Pegasus spyware can be authorized under the provisions regarding interception of phones but the mere assumption is no answer. The prominent question which arises here is that whether government agencies can be authorized under the contemporary provisions of law. To answer this question, it is important to understand that there is a stark and very crucial distinction between the interception of a piece of information sent through a device and a device operating as a spy cam to record one's actions and communications which were not sent through the said device.

**Telegraph Act**

Section 5(2) of the Telegraph Act, 1885 provides the basis for the interception of telephone calls or phone-tapping by the Central or State government or any officer specially authorized on this behalf. Constitutionality of section 5(2) of the Act was challenged in the Supreme Court by the People's Union for Civil Liberties and in the judgment Supreme Court upheld the constitutionality of the provision while suggesting it to be armed with extra teeth in the form of procedural safeguards which were later codified in Rule 419A of the Telegraph Rules, 2007.

It is the objective of section 5(2) of the Telegraph Act to carry out interception, prevent transmission and ensure disclosure of messages. According to section 3(3) of the Telegraph

Act, the term 'message' is defined as any communication sent by telegraph or given to a telegraph officer to be sent by telegraph or to be delivered. Thus, it is clear from section 5(2) of the Telegraph Act that it can only authorize an order to intercept any information made through one device to the other but it does not visualize the compilation of contents created in the device and not sent by telegraph or to anyone else while subjecting the user to ceaseless surveillance. It also does not envisage the recording of conversations made in the vicinity of the device but not through it.

**Information Technology Act**

Rules under section 69 of the Information Technology Act, 2009 confers Central and State governments the power to intercept, monitor, and decrypt any information on a computer resource. The government is only authorized to use the power under this section when it is necessary for protecting the security interest of the country, the security of the state, sovereignty, and integrity of India, and friendly relation with foreign states or public order or for preventing incitement to the commission of an offense. Information Technology Rules,2009 on interception, monitoring, and decryption provides the meaning of interception, monitoring, and decryption. According to this Act, interception is defined to mean the acquisition of any information to make the contents of the information available to a person other than the sender, recipient, or intended recipient of the communication. Thus, it is crystal clear that only those contents of the information can be intercepted that form any part of some communication through a computer resource and not of actions and conversations made in the vicinity of a computer resource. So, it implies that in some certain circumstances government can have eyes and ears on messages and media shared through electronic devices but it cannot turn those electronic devices into eyes and ears to what happens in the surrounding of the devices.

**Pegasus a need or excessive power**

In this modern era, it is normal to be equipped with new and nuanced ways to combat terrorism or crime, but does it mean that our present provisions of the law are obsolete or effective in providing the result we expect it to deliver. Before delving into the matter of whether Pegasus spyware is needed or not, it is important to know the objective behind the birth of it and whether it is useful in the way it is claimed to be. The NSO Group, creator and service provider of Pegasus spyware, claims it to be created to put a stop to terrorism by its novel surveilling and

data accessing features. But it is ubiquitously known that even an amateur in this modern world is aware of the fact that smartphones can be used to retrieve data and to put someone under partial surveillance. It would be an ignorant approach of thinking to expect that a person planning to terrorize a country or world would use hackable devices. If the government or government agencies are looking at Pegasus spyware as an effective way to curb terrorism, then it would be a waste of the hard-earned money of taxpayers. But recent reports and investigations suggest otherwise. It is clear, that Pegasus spyware has not been in use the way it is claimed by its parent company, NSO group. It has been used to infect devices of not only criminals but journalists, activists, politicians, lawyers, and retired judges for surveillance. It is difficult to believe that Pegasus spyware is in possession of a non-governmental organization because if it would, the consequences would have been much direr. Pegasus spyware bestowed government unprecedented power over the narratives of its citizens, consequently, almost all people allegedly under the surveillance radar were the dissenters and critiques of the government. At present, according to the reports of the New York Times, spying by Pegasus on 10 iPhones is $650,000 and on 10 Android users is $500,000. So, it is contented by some people that due to its high charges, the government cannot use it on a larger scale. It is true but, the government doesn't require widespread surveillance to change the narratives in its favor. We must also not forget that the smartphones we are using were too expensive at their inception with limited technology but they got cheaper, better, and widely accessible with time. Imagine what would be the extent of surveillance if software engineers succeed in making a cheaper and better version of Pegasus spyware, privacy and freedom of speech and expression will be under greater threat. Thus in a democratic world or country, we surely do not require the government to have such excessive power over us.

**Impact on social and legal rights**

- **Right to privacy and freedom of speech**

  These are the fundamental rights guaranteed by the Constitution of India under Article 21. The existence of spyware like Pegasus is a major threat to these fundamental rights. Not only the act of spying but mere fear of being put under surveillance can have severe psychological effects on an individual. It is a basic human need and incursion into privacy can result in the gradual development of emotional and psychological problems, including anxiety, paranoia, broken trust, and depression. The incursion into privacy is both an

ethical and legal issue. Continuation of invasion of privacy by the government may lead to people losing their trust in the government, which would only exacerbate the relationship between the government and its citizens.

Freedom of speech is guaranteed under Article 19(1)(a) of the Constitution of India, which enables a person to talk and express his opinion freely. We all enjoy conversations with our friends and our loved ones, which obviously sometimes can become intimate. It can be very personal and fear of it to be heard by someone other than to whom it was made can cause unmeasurable stress to an individual. This fear of being heard has very much become possible by the advanced surveillance features offered by Pegasus spyware. Hence, it restricts an individual from enjoying its right to freedom of speech and expression.

- **Right to dissent**

Liberty of thought, expression, belief, faith, and worship is enshrined in the preamble of the Constitution of India. Clauses (a) to (c) of Article 19(1) of Constitution promises-

1. Freedom of speech and expression
2. Freedom to assemble peacefully and without arms
3. Freedom to form associations or unions

These three freedoms are the wheels through which dissent can be expressed. Dissent is essential in a democracy. In a democracy, every person should be able to express or present his opinion without fear of being persecuted or targeted by a powerful regime. India is one of the biggest democracies in the world with an organized and commendable constitution, despite that, forensic analysis of some phones whose numbers appeared in the leaked list showed successful infection hack and Pegasus activity on the device. It is difficult to rule out the possibility of these dissenters being crushed by a government equipped with a weapon like Pegasus. It would only weaken the democracy of the country as it is only if there is discussion, disagreement, and dialogue that we can arrive at better ways to run the country.

- **Chilling effect**

It has been confirmed by The Wire that at least 40 journalists were either targeted or potential targets. Forensic analysis conducted on the phones of 7 journalists showed that the phones of 5 journalists were successfully infected by the Pegasus spyware for surveillance. Journalism is an essential part of democracy. A journalist not only disseminates information but also makes people aware of their rights and questions the

government on their policies and decisions on behalf of the general public. For any authoritarian government, a journalist with dissenting comments about their policies would be like a thorn in the flesh and now such a government has a perfect weapon (Pegasus spyware) in its arsenal. Surveillance of such extent creates a chilling effect not only to the journalists but also on their sources, who before this would have come forward to act against the political interests of the party in government.

- **Lawyer-client privilege**

Lawyers are also heavily featured in the leaked data. Section 126 to section 129 of the Indian Evidence Act, 1872 provides for privileged professional communication between clients and legal advisors. It is the trust of a client that no information however embarrassing or legally damaging divulged by him to his legal advisor would be used by his legal advisor against him or without his consent, that encourages him to seek legal aid. If there were no protection to the professional communication between a client and a lawyer, no person would seek legal aid. But Pegasus spyware being in the picture, such privileged communication is not safe anymore. It endangers the legal aid promised by our Constitution to every individual, as it is possible that a third party, who has snooped your lawyers' phone, is listening to the conversation between you and your lawyer.

## Conclusion

Year after year, progressing technological advancements will spew out more nuanced Spywares than this one, we must remain vigilant and aware of the rights bestowed to us by the Constitution. There are appropriate laws to ensure the protection of the right to privacy but with fast technological advancements and increasing complexity, our laws need to be amended in order to give strict and clear interpretation regarding the pertinent provisions of law. Bold scrutiny in the application of Pegasus spyware is required to understand the extent to which it had or has been applied for surveillance.