International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 24-09-2021, Accepted: 09-10-2021, Published: 25-10-2021
Volume 7, Issue 5, 2021, Page No. 187-191

Pegasus: partnering with the apartheid

Srividya Iyer G, Abirami A B
SASTRA Deemed to be University, Thirumalaisamudhram, Thanjavur, Tamil Nadu, India

Abstract
Most of the offenses against the body involve physical violence. But one of the most prevailing and growing offenses with the same gravity is cybercrime. In the digital era, information and communication technology is helping billions to build the gap between people. But we do not realize that the gap is becoming so thin that every person is becoming capable of stepping into another's shoe, infringing their privacy and even lowering the dignity of another. In such a case, Pegasus spyware is one of the major issue of the nation by partnering with the apartheid. This paper provides the study on Pegasus spyware, it's impact on privacy and its ill effect on the state interest. The advancements in technology are intended to provide better living, but the same technology is being misused in various walks of life without any physical bounds. When this became a burning issue in India, various provisions were established in Penal provisions, Information Technology Act, 2000 and Privacy laws seeking protection to the victims. But these laws fail to meet the growing cybercrime rate. This paper throws a light on laws governed to protect the privacy of the people and at the same time also the gaps in law are indicated. This paper aims to bring out the effect of Pegasus on privacy and the challenges to the democracy. Various cases are analysed to conclude.

Keywords: privacy, national interest, surveillance tool, journalism, democracy

Introduction
In the 21st Century, in the world of computers everything is digitalized. Technology has made our lives much easier. But just as a coin has two sides, technology has its own dark side as well. Spyware- a technological beast has ripped apart our privacy. Spyware is malicious software which breaks open into our device and steals our sensitive data and forwards the same to an unauthorized third party. This paper would primarily deal with Pegasus: the spyware.

Pegasus: The Technological Beast
Pegasus: the spyware has been developed by NSO, an Israel based group. The spyware was primarily developed for aiding the government to battle against terrorism. The founder of the spyware stated that its purpose was "*to develop technology that would provide law enforcement and intelligence agencies with direct remote access to mobile phones and their content – a workaround to the increasingly widespread use of encryption in the digital environment*".
In 2016 it adopted the "mobile- first mechanism/ Spear pishing mechanism". In this mechanism the user would receive a text message which when clicked upon would lead to data hack. This is possible in android, iphone and wireless also. Ahmed Mansoor, a human right activist received messages which stated that upon clicking the link, the activist would be forwarded to a page which throws light on the tortures faced by prisoners in UAE. The activist got suspicious and contacted Citizen Lab which confirmed the same to be spyware developed by NSO group [1].
In 2018 the Citizen Lab stated that around 45 countries have been targeted by the same.

Version 2.0
The recent spyware is of such a nature that clicking on any link isn't necessary. It operates on a mechanism called "Zero- Day Vulnerability". The target receives a text or call and upon receiving itself the spyware automatically installs itself in the targets' mobile and starts to track the personal information of the target. It hacks all sensitive data of the target.

Extent of Acessibility
a. What can be accessed and how can it be accessed?
- "***Unlimited access to target's mobile devices:*** *Remotely and covertly collect information about your target's relationships, location, phone calls, plans, and activities whenever and wherever they are*
- ***Intercept calls:*** *Transparently monitor voice and VoIP calls in real-time*
- ***Bridge intelligence gaps:*** *Collect unique and new types of information (e.g., contacts, files, environmental wiretap, passwords, etc.) to deliver the most accurate and complete intelligence*
- ***Handle encrypted content and devices:*** *Overcome encryption, SSL, proprietary protocols and any hurdle introduced by the complex communications world*
- ***Application monitoring:*** *Monitor a multitude of applications including Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)*
- ***Pinpoint targets:*** *Track targets and get accurate positioning information using GPS*
- ***Service provider independence:*** *No cooperation with local Mobile Network Operators(MNO) is needed*
- ***Discover virtual identities:*** *Constantly monitor the device without worrying about frequent switching of virtual identities and replacement of SIM cards*
- ***Avoid unnecessary risks:*** *Eliminate the need for physical proximity to the target or device at any phase"* [2]

b. What can't be accessed?
It is not well established that it can access other applications in the target's phone.

Pegasus: An Undetected BUG?

The spyware remains asymptomatic. However it can be detected in the following ways: [3]

- Amount of data usage
- Apps which you did not install running in the background
- Battery drain
- Crashing of other application
- WhatsAap alerts for updates.
- Signs of rooters
- System slows down
- Unknown WhatsApp missed calls
- Applications which use camera and microphone without authorization.

Issues In Detection

The above suggested methods are merely suggestive. But mostly Pegasus deletes the call history in WhatsApp, uses Command and Control to reduce data consumption, and can't be detected by antivirus software or forensic analysis. Thus it is indeed the most sophisticated spyware.

Cases revolving around the same

Calfornian Case

In 2019 WhatsApp filed a suit in California against NSO group for using WhatsApp as a medium of spyware attack. The NSO group was not served with notice. The court served notice of default. The same was objected by the group. Another suit in 2019 was initiated by NSO against WhatsApp in Israel for blocking private Facebook accounts. WhatsApp argued that NSO has breached the California Comprehensive Computer Data Access and Fraud Act by breaching privacy on WhatsApp. In July 2020 the Californian court pronounced in favor of WhatsApp.

Indian Case

On October 30, 2019, Facebook confirmed that Pegasus was employed to attack Indian journalists, lawyers, government officials, and activists. This was two weeks before the Lok-Sabha election. Allegations arose that the government is involved in the attack. In July 2021, the Pegasus Project stated that the Indian government has used it to spy on about 300 people between 2017-2019 [4]. Advocate M.L Sharma has filed a petition before the honorable SC seeking to probe into the matter using a special investigation team. The honorable apex court recently stated that "We are again reiterating that we are not interested in any manner or in any way to know the issues which are concerned about the security or the defense or any other national interest issue. We are only concerned, in the face of allegations that some software was used against some particular citizens, journalists, and lawyers etc, to know whether this software has been used by the government, by any method other than permissible under the law." [5] The case is still ongoing.

Other Spywares Which Shook Conscience

Pegasus is merely one of the several shades of spywares out there. We had witnessed several spywares in the past which shook the conscience of internet users. To name a few

Dropout Jeep

Dropoutjeep was developed for the sake of internal security by the National Security Agency. One German periodical named Der Spiegel threw light on the spyware. It published one of the reports of the US National Security Agency which stated as follows [6]-

"Dropoutjeep is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted."

CVE- 2019-11931

This attack ensued after the Pegasus attack. The spyware used MP4 file to target the user, when downloaded would lead to breach of data.

Exodus

One company named eSurv which has its roots in Italy developed this spyware. Motherboard discovered that it is one spyware which remained undetected in Google play store which portrayed itself to be a marketing app. When downloaded it stole all personal data. Any user who uses the same Wi-Fi as that of the target is exposed to risk. It was primarily aimed at Italian population.

Coolwebsearch

It used Microsoft windows to target the victim. It creates desktop shortcuts, leads to slowdown of internet. It redirects itself to suspicious websites and collects private information and edits trusted user sites as well.

P6-GEO-

This has been developed by an Israeli company named Picsix. The spyware intends to locate the targets' location.

GATOR-

The spyware tracked user's surfing patterns and thereby promoted marketing via advertisements.

Spyware Regulation around The Globe

United Kingdom

- Computer Misuse Act- Punishes illegal access to computer.

United States

The following remedies are available: [7]

- Trespass to chattels [8]
- Invasion of privacy [9]
- The Computer Fraud and Abuse Act [10]
- The Stored Wire and Electronic Communications and Transactional Records Act ("Stored Communications Act") [11]-
- The Wiretap Act [12].

India

- Sec 43- The Information Technology Act, 2000 [13] Penalty for damaging computer / system/ network without owner's/ authorized person's permission.
- Sec 66-The Information Technology Act, 2000 [14]- Punishment under Sec 43.

Violation of Right to Privacy

Communication surveillance in India takes place basically under two laws —

1. The Telegraph Act, 1885 and
2. The Information Technology Act, 2000.

While the Telegraph Act deals with interception of calls, the IT Act was enacted to deal with the monitoring of all electronic communications, following the intervention of the Supreme Court in 1996. A comprehensive law on data protection to fill gaps in existing supervisory frameworks still needs to be staged.

The Telegraph Act, 1885-

Section 5(2) of the Telegraph Act provides that

"On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order…"

Under this law, the government can intercept calls only in certain situations —

1. The interests of the sovereignty and integrity of India,
2. The security of the state, friendly relations with foreign states or public order, or
3. For preventing incitement to the commission of an offence.

These are the same restrictions imposed on free speech under Article 19(2) of the Constitution.

In order to impose these restrictions there is a condition precedent. That is *the occurrence of any public emergency, or in the interest of public safety.*

Additionally, a proviso in Section 5(2) states that

Even this lawful interception cannot take place against journalists. "Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

Information Tecnhology Act, 2000

Section 69 of the Information Technology Act and the Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 was put forth to expand the legal framework for electronic surveillance.

Under the IT Act, all electronic transmission of data could be intercepted. Therefore, in order to legally use Pegasus-type spyware, the government would have to invoke both the IT Act and the Telegraph Act.

In addition to the restrictions provided in Section 5(2) of the Telegraph Act and Article 19(2) of the Constitution, Section 69 the IT Act adds another aspect that makes it broader — interception, monitoring and decryption of digital information "for the investigation of an offence".

Significantly, it exempts from the condition precedent provided for by the Telegraph Act which requires "the occurrence of the public emergency in the interest of public security", which widens the scope of the powers provided for by law.

- **Rulings of the Apex Court**

The apex court has dealt with the issue in a plethora of judgments such as-

Public Union for Civil Liberties v Union of India (1996)

The Supreme Court noted the lack of procedural safeguards in the provisions of the Telegraph Act and established guidelines for wiretapping. In a PIL filed by CBI on the report of "wiretapping of politicians", the court noted that the authorities involved in the interception did not even keep adequate records and recordings of the interception. Among the directives issued by the court was the establishment of a review committee that can review the authorizations granted under section 5 (2) of the Telegraph Act.

The interception is a serious violation of the privacy of an individual. With the growth of highly sophisticated communication technologies, the right to a sold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is undoubtedly correct that every government, however democratic it may be, exercises some degree of operation as part of its intelligence equipment, but at the same time the right of citizens to privacy must be protected against abuse of the authorities.

The directives of the Court were used as the basis for the introduction of rule 419A [15] in the Telegraph rules, 2007, and then in the rules prescribed in the law on Information Technology in 2009.

K S Puttaswamy & Anr. v. Union of India & Ors.

In this case, *the right to privacy was declared a fundamental right and the Court emphasized the principle that "privacy is the highest expression of the sanctity of the individual"*.

In addition, he noted that any restriction on the right to privacy must comply with the "principle of proportionality and legitimacy".

None of these scenarios met the need for an oversight mechanism like Pegasus and this, in turn, reinforced the need for a strong privacy regime and draft privacy bill on data protection that would protect the rights of citizens and holds any agency that attempts to violate these rights, accountable.

Therefore, with the advancement of technology, it is easier for governments and private agencies to examine the privacy of individuals. There is no fine line between surveillance and data collection as the governments violate these rights under the pretext of terrorism and national security. It is absolutely necessary to clarify existing laws and adopt better laws that deal with data protection and privacy.

Currently, India's legal framework governing surveillance suffers from many gaps. The main problems are the centralization of powers with the executive and the lack of independent judicial control. In addition, the current control regime does not provide for an effective judicial remedy, independent of the executive power.

Moreover, the use of targeted surveillance must be carried out in accordance with the principles of legality, necessity

and proportionality recognized by the Indian Supreme Court and provided for by international human rights law.

Partnering with the Apartheid

It is considered that during the trip to Israel, the nation's leader signed up for the Pegasus malware which is now being used as a surveillance tool against journalists, opposition party leaders and other constitutional machineries.

The agency under the command of NSA Ajit Doval – National Security Council Secretariat – received a doubtful 311% budget increase in that financial year; those funds are speculated to have been used for the Pegasus [16].

As of now several petitions have been filed against the illegal spyware which violated the privacy of various sections of important people in the country. But the government has always been denying, oscillating and sometimes accidentally admitting it. If the allegations made to the Supreme Court are proven, then this would not only become a state sponsored crime of partnering with the apartheid but also the executive will be held contempt for violating the judgment of the Supreme Court relating to the right to privacy.

The Puttaswamy judgment provide for a disabling implication: i.e. unless there is an enabling legislation passed by the state to do all things that the Bill permits, and the way in which it permits, the state cannot be said to have those rights. So the state could not, for example, have snooped on any devices at all – even for "compelling state interest" – because there was no enabling framework that permitted it to do so." [17]

There must always be a balance between "compelling state interest" and the "dignity of the individual" in a democratic nation. But in India both the aspects are subject to hang on the air. On one hand the bargain for privacy legislation and on the other is that whether the action was for protecting the state interest or the interest of the ruling party.

When examining the names of the targets of the Pegasus project it was shown that those persons were normally not acquaintance of any terrorism or criminal behaviour. It clearly pictures that there was no state interest involved. The names of those members were somewhere or the other related as collaterals for political purposes. Journalists, key opposition leaders, constitutional functionaries like an Election, the former head of the CBI and a staffer of the Supreme Court were among the list. So ultimately there arises a question of whether all this is for "state interest" or "party interest".

Challenges to Democracy

Democracy as we know most importantly is for the people. But surveillance acts like these violates the privacy and personal lives of various individuals.

The NSO group claims that Pegasus spyware intended only to protect citizens and save lives against terrorism and various other criminals. But around 180 journalists, at least 40 of which in India, have possibly been targeted by the spyware [18].

The journalists should be able to perform their democratic functions safe and secured. Thereby they must protect and safeguard their sources. But this spyware is an unlawful and arbitrary surveillance on the journalists. It violates their right to privacy and the freedom of expression. It intrudes their personal life and also reveals most of the sensitive data.

Moreover, the Pegasus spyware undermines the principles of journalism, most importantly secrecy. Several journalists who were listed as potential targets have concerned over their sources. They were worried that sources will feel reluctant about working with them in the future, once the public learns that they were subjected to surveillance, putting individual journalists and, ultimately, investigative journalism, in a very difficult situation.

These spywares not only has adverse impact on the journalists alone. But also various other people like human rights defenders, secret agents who may resort to censorship have a huge impact. So when they are subject to surveillance, the freedom of the media becomes a question and the people who point out the wrongdoings are put to silence.

The Indian Supreme Court in Maneka Gandhi's case observed that "Freedom of press is the most cherished and valued freedom in a democracy and indeed democracy cannot survive without a free press". It would be interesting to know whether these observations by the Supreme Court were ever in the minds of the Executive when they authorised the surveillance of journalists and judges, among others. Thereby the whole concept of democracy is buried deep.

Conclusion

As the saying goes that "necessity is the mother of invention", we are in that stage of technological era where privacy belts should be fastened. Technological devices which are more immune towards such spyware should be developed. Users should be sensitised on such issues. To combat such spywares the following methods can be resorted to:

- Use e Mobile Verification Toolkit (MVT) to detect Pegasus.
- Install effective anti-virus.
- Never open any unknown link.
- Avoid using public Wi-Fi.
- Use strong passwords.
- Turn off your Wi-Fi and Bluetooth when not in use.
- Update your devices.
- Do not open spam emails.
- Use remote wipe features.
- Limit physical access of your device.
- Encrypt your data.

Further laws should be made stern to dissuade the evil as much as possible for we are all digital-sapiens.

References

1. 5th year, BBA.LLB(Hons.) SASTRA DEEMED TO BE UNIVERSITY, Thirumalaisamudram, Thanjavur.
2. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
3. https://www.firstpost.com/tech/news-analysis/pegasus-spyware-a-complete-guide-to-how-it-can-be-used-to-infiltrate-your-phone-7585931.html
4. https://www.safe.security/assets/img/research-paper/pdf/pegasus-spyware.pdf
5. https://economictimes.indiatimes.com/tech/trendspotting/what-is-pegasus-spyware-and-how-it-works/articleshow/84607533.cms?from=mdr
6. https://indianexpress.com/article/india/no-beating-

around-the-bush-did-govt-use-pegasus-illegally-supreme-court-7507021/
7. https://thehackernews.com/2014/01/DROPOUTJEEP-NSA-Apple-iPhone-hacking-tool.html
8. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1467&context=fclj
9. RESTATEMENT (SECOND) OF TORTS § 218 (1965);
10. RESTATEMENT (SECOND) OF TORTS § 652B (1977)
11. 18 U.S.C. § 1030(g)
12. See 18 U.S.C. § 2701 (2001);
13. 18 U.S.C. § 2520 (Supp. III 2003)
14. https://indiankanoon.org/doc/39800/
15. https://indiankanoon.org/doc/326206/
16. https://cis-india.org/internet-governance/resources/rule-419-a-indian-telegraph-rules-1951
17. https://www.deccanherald.com/national/nscs-fund-used-for-buying-pegasus-alleges-prashant-bhushan-1012046.html
18. Justice K.S. Puttaswamy (Retd) vs. Union Of India on 26 September, 2018
19. “protect citizens and save lives” (NSO GROUP)