INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Dec 2023
ISSN: 2582-6433

PEGASUS SPYWARE CASE ANALYSIS.

AUTHORED BY - SUBHASHREE S[1]

INTRODUCTION:

Just think, you are having a conversation with your family or life partner and there is someone who secretly listens to it, watches you through your mobile camera and knows everything about your online activities. Sounds terrific, right?

Pegasus spyware invented in 2010 by an Israeli Technology firm known as NSO (Stands for Niv, Shalev and Omri, the names of the company's founders), whose revenue as of 2020 was $243M. The use of Spyware itself isn't bad as it's used for national security and criminal activities identification as it is claimed that this spyware is being sold only to vetted intelligence agencies and governments. But its misuse is of great concern as it affects basic fundamental rights.

In late 2019 the Pegasus spyware exploitation came into limelight, which created unrest globally. This issue has wider aspects to be taken into consideration as more 50+ countries activists, politicians, etc. have been snooped. This results in violation of international conventions and human rights.

This article covers the case in California court which brought the exploitation into limelight, and case in Indian supreme court, and how this spyware works and what precautions and preventions can be taken as an individual.

BACK GROUND:

The use of spyware can be traced back to 2012 used in Panama, then in 2013 in UAE. But it's malafide use started in 2016 where it was targeted against human right activists in UAE.

In 2018, Pegasus found a case targeting journalists and activists in 45 countries globally and several lawsuits were filed.

[1] IV Year, B.B.A.LL. B(H.), School of Law, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai. Email id: subhashree7018@gmail.com , Ph: +91 6384678313.

ISSN: 2582-6433

In 2019, Facebook messenger platform, WhatsApp case in California Court brought intensity to the Pegasus exploitation issue, whereby using zero-click method, attacks 45 countries activists and journalists have been snooped, which include people from India.

Recently, in 2021 in India, The Wire[2], an online news reporting agency, published the Pegasus Project's finding, which contains a detailed list of individuals such as politicians, journalists, activists who are snooped.

And the last development in regards to Pegasus is that of numerous cases filed in the Supreme Court of India against the malafide use of Pegasus.

OVERVIEW OF SENSATIONAL PEGASUS CASE IN CALIFORNIA

Case Name: WhatsApp Inc. v. NSO Group Technologies Limited[3]

Background of the Case:

On Oct 29,2019 WhatsApp filed a case against NSO in United States District Court for the Northern District of California as WhatsApp is based in Menlo Park, California. The case moves as the defendant that is NSO used its spyware called Pegasus and snooped by infecting malware in the devices through WhatsApp of around 1400 WhatsApp users between the period of April and May 2019.It was established that more than 100 of them are journalists, activists, politicians. Through this NSO got remote access and control of information as to messages, calls, and locations.

In this aspect the plaintiff alleges for violation of Sec 1030 of Computer Fraud and Abuse Act, Sec 502 of California Comprehensive Computer Data Access and Fraud Act, breach of contract and wrongful trespass in the property.

Defendant's only intention that can be carved out form the case is to dismiss that case without being heard. And for the same defendant relied on contending regards to subject matter jurisdiction, personal jurisdiction and failure to join indispensable parties.

[2] https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance, Last accessed on 09/01/2024

[3] https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/, Last accessed on 09/01/2024

ISSN: 2582-6433

Court's Decision:

Court made a clear stand on its decision and ruled in favour of WhatsApp. Court held that, w.r.t subject matter jurisdiction NSO cannot be considered as foreign officials, so no sovereign immunity can be given. Then w.r.t to personal jurisdiction court held that though they did not agree to this court's jurisdiction but it's intentional action to cause harm. Finally, the contention of failure to join indispensable parties court held that those governments are not necessary parties to the case. And the plaintiff's contentions of all are agreed upon by court except for trespass to the property as WhatsApp is not able to prove the real damage caused.

Status of the Case:

After the District court verdict, NSO moved for appeal to the US Supreme Court. The argument that NSO made in appeal was of two-fold, that is it acted on behalf of unidentified governments thereby assisting law enforcement and intelligence agencies and secondly, this lawsuit against it will undermine the foreign government investigation potential.

But the court did not give heed to NSO arguments and rejected NSO's appeal to dismiss the case by November 2021.

Aftermath of the Decision:

U.S Government during the Month of November of 2021 blacklisted NSO and another Israeli company, for supplying spyware which is being misused. And this paved the way for other countries to be cautious, and one of which is India. Litigations also commenced in India w.r.t to Pegasus and revealed potential journalists, activist, and politicians who are in the target list of spyware attack and brought a big question on various fundamentals rights along with questions bombarding towards the government.

ROUTE OF PEGASUS TOWARDS INDIA

Revelation of Pegasus Project

On 18th July 2021, the Pegasus Project made by Wire[4] along with 16 other media organisations made a groundbreaking revelation on 50,000 people phone numbers in the target list of the clients of NSO. The people in the lists belong to either the categories of head of the states, journalist,

[4] https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance, Last accessed on 09/01/2024

ISSN: 2582-6433

students, lawyers, politicians among others. Yet it is important to note that the revelation does not confirm the successful targeting, it requires forensic examination.

But Wire along Amnesty International forensically examined that 10 Indians phone numbers were snooped. It has revealed 161 names who were targets or potential targets for surveillance by clients of the NSO Group, which includes journalists such as M.K. Venu: A founding editor of The Wire, Sushant Singh: Former Indian Express journalist who writes on national security, Vijaita Singh: The Hindu journalist who covers the home ministry, Politicians includes Rahul Gandhi: The Congress party leader, Prashant Kishor: An election strategist who has worked for several political parties, and Activists, lawyers and academicians includes Hany Babu M.T.: Professor at Delhi University, Rona Wilson: A prisoners' rights activist, Arun Ferreira: A lawyer and more.[5] This brought a question of concern that whether the Indian government purchased this spyware. NYT report[6] claims that India Bought Pegasus as Part of Larger $2 Billion Deal with Israel in 2017.

Aftermath of which Minister for Information Technology Ashwini Vishnaw in Lok Sabha spoke that the Project is an attempt to malign India's "democracy and its well-established institutions "and that there are sufficient checks and balances and the project is baseless. Additionally, he stated that India has rigorous legislation such as the Indian Telegraph Act, 1885[7] and the IT Act,2000.[8]

In this period that is between July-August 2021, there were many cases filed in Supreme Court w.r.t to Pegasus Spyware which are clubbed and heard are one case.

PEGASUS CASE IN INDIA:

Case Name: Manohar Lal Sharma Vs. Union of India (UOI) and Ors[9]

Citation: MANU/SC/0989/2021

Hon'ble Judges/Coram: N.V. Ramana, C.J.I., Surya Kant and Hima Kohli, JJ.

Facts:

[5] https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance,Last accessed on 09/01/2024
[6] https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html, Last accessed on 09/01/2024
[7] https://dot.gov.in/act-rules-content/2442, Last accessed on 09/01/2024
[8] https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf, Last accessed on 09/01/2024
[9] https://indiankanoon.org/doc/39021018/, Last accessed on 09/01/2024

ISSN: 2582-6433

The gist of the case revolves around the spyware called Pegasus alleged to be infected in the devices of citizens of India, specifically activists, politicians and journalists. So, individuals claimed to be direct victims and public interest litigation on public interest have been filed. Individuals worried that either foreign government or certain agencies within India are using Pegasus without following proper legal procedure and alleged that inaction of government in this matter. This case gains its importance because of major fundamental rights such as right to privacy and freedom of speech and expression violation if allegations are proved. This case further involves aspects of national security and rigorous legal framework for surveillance.

Issue:

Two primary issue that can be derived from this case are:

- Whether the government has used spyware to violate an individual's privacy.
- Whether national security supersedes right to privacy, if so to what extent?

Laws Involved:

- Constitution of India,1949 specifically Article 19[10]which deals with Freedom of Speech and expression and Article 21[11] which in its derived form has right to privacy.

Major Argument of the petitioners:

- The very core argument is with respect to the right to privacy which was held in the case of K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1 that the use of Pegasus spyware by infecting it into individuals' devices violates right to privacy.
- Counsels of the petitioners also contended that government inaction to this issue of cyber-attack and that specifically the direct victims requested for an independent investigation agency to find out the truth.
- The counsels argued that the government should not conceal information in the name of national security which renders injustice.
- The counsels of journalist's petitioner raised concerns with regard to planting of false evidence on devices.
- Counsels pressed on interim reliefs and to uphold the fundamental rights.

[10] https://indiankanoon.org/doc/1218090/, Last accessed on 09/01/2024
[11] https://indiankanoon.org/doc/1199182/, Last accessed on 09/01/2024

ISSN: 2582-6433

Major Arguments of the Respondent:

- Solicitor general representing the union of India completely denied the allegation on the ground that the petitioner's contention does not have any factual basis and it is conjecture.
- Respondents emphasised on national security concerns with respect to certain information that petitioners asked for.
- Counsels submitted that as the surveillance laws in India are rigorous, there is no chance for illegal surveillance.

Court's Analysis:

- The court with respect to right to privacy, emphasised the importance of right to privacy in the digital era and that it is not an absolute right and it has reasonable restrictions. Furthermore, it strikes balance between right to privacy and national security by stating that surveillance can be done only by following the rules established by law. And that where spying or surveillance of individuals are done it is violation of right to privacy. Court stated that surveillance will have chilling effect on freedom of press
- When the union of India submitted a limited affidavit, the court emphasised that it acknowledged the limit of judicial review in national security but states that necessary information for the case to proceed needs to be produced. Further it classified that the state cannot always use "national security" as a reason without proper scrutiny. Despite that the government refused to submit an exhaustive affidavit.
- Moreover, the court highlighted the importance of upholding the constitutional principles and rule of law, avoiding the involvement into political debates.

Decision:

- Court formed an expert committee with specific tasks and guidelines to conduct comprehensive inquiry and to submit a report which is overseen by a retired judge.
- Court clarifies that the committee engages in investigating the use of spyware, its impact on citizens and the actions taken by government, and recommendations on legal framework necessary with regards to surveillance and privacy.
- 8 weeks of time was given to submit the report and, in the aftermath, it was further extended and in July 2022 report was submitted.

ISSN: 2582-6433

Status of the Case:

The committee report which was submitted has examined 29 devices out of which 5 have malware but it is not Pegasus spyware. Moreover, committee recommended for rigorous surveillance and privacy protection law. Court further stated that it might upload the report on websites but as of now it is sealed and kept in custody of the secretary general.

The counsels of petitioner asked for the copy of the report emphasising right to know. Court is yet to revisit the matter and case is still pending.

Criticism around the committee's report:

When the committee was set up by the Supreme Court there was a huge expectation from petitioners as well as from the general public, with the intention that it discloses the original facts of the case. But it didn't do so, is what the existing opinions among the public. Supreme court instant of completely relying on this report as it does not clearly give any conclusion, court can ask the collaboration of expert organisations like Citizen Lab and Amnesty International's Security Lab to identify whether the malware in the 5 devices is of Pegasus and also to ensure that the committee's method of identifying this malware is of accurate. As this institution already discovered a way to detect the Pegasus spyware is its normal deduction method cannot be indeed in case of -Pegasus. Further non-disclosure of the report brings in the question of how reliable the experts committee's report is. Therefore, in order to render complete justice, it can be concluded that court have to revisit the report with help of international organisation and to urge government to submit exhaustive affidavit which is necessary for this case.[12]

Overall Inferences from Pegasus cases:

This Pegasus issue throws a reality to the world about how important it is to develop and modify law as and when technology develops. Further proves that information is wealth in the present era.

In India as there is always a backlog of cases and litigation in itself a time-consuming process, we are awaiting judgement. But let's sit back and think what is the scenario in the US, where the judgement has been passed. Despite the judgement still cases of spyware, to be specific of

[12] https://www.barandbench.com/amp/story/news%2Fno-pegasus-spyware-found-in-29-mobile-phones-examined-by-supreme-court-panel-some-other-malware-found-in-5-devices, Last accessed on 09/01/2024

ISSN: 2582-6433

Pegasus, are still prevailing. One such instance[13] is where Roman Gressier, an American Journalist, was targeted with this spyware.

So as a citizen of India, if one expects that the forthcoming judgement will protect the right to privacy with respect to spyware it would be an optimistic aspiration.

This shows that apart from having extensive legislation and pronouncing judgement, there is something more that has to be done. And this brings to the aspect of individuals action towards protecting themselves as much as possible.

So here comes a question: what else should be done to protect our information and to make sure that individuals are not being snooped.

Solution comes out to be simple: that each and every individual takes initiative to protect themselves. In order to understand this, two aspects need to be understood. That is how spyware is infected in devices and what steps can be taken by the users individually to protect themselves.

WAY FORWARD

UNDERSTANDING METHODS USED TO SNOOP

Generally, there are 3 methods used to infect the malicious spyware:

1. By user clicking URL or message:

In this type of method, the targeted device is being sent with a message or URL. In this case human interaction that is to say users' activity is expected by the attackers. Only if a user clicks to the message (SMS, iMessage, WhatsApp, email) or URL their device will be snooped.

2. By Zero-Click Attack:

It is also known as zero-click exploit. In this type of method without any need of integration from user side, the attackers can hack their target device. Here, a missed call in what's app or a message without notification will be sent where at the very time it reaches the target device it is being

[13] https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus, Last accessed on 09/01/2024

ISSN: 2582-6433

snooped. And it leaves no traces, that is the user will not even be able to see the missed call in WhatsApp which will also be automatically erased from the log. All it requires is the vulnerable app or operating system installed.

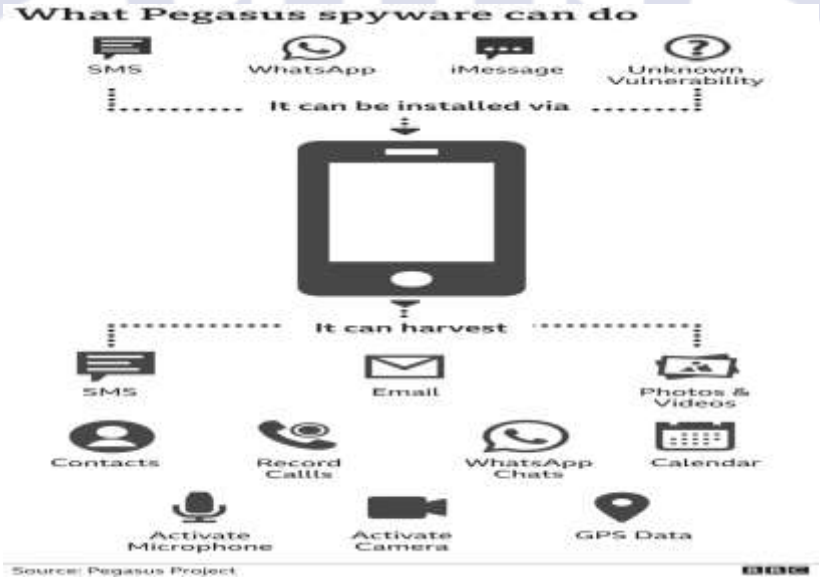
This method is dangerous because it is very difficult to be traced or to be identified. Pegasus spyware uses this method to attack its target, where it puts basic rights such as freedom to speech and privacy in question.

3. By Network Injections:

This is one of the other methods used by Pegasus and Spywares in general. But it is considered to be more complex than that of the other two, as here it requires the user that is the target to browse the unprotected website during their normal online activities. Once they visit, the injection software can intercept the transaction and trigger an infection, but here it is necessary to monitor the target internet traffic until they access the site which is not fully protected.

Pictorial representation for clear understanding:

Source: Pegasus project[14]



[14] https://www.bbc.com/news/technology-57881364, Last accessed on 09/01/2024

ISSN: 2582-6433

HOW TO DETECT AN INDIVIDUAL CAN IDENTIFY THAT THE DEVICE IS SNOOPED[15]

The below mentioned are a few ways which can be noticed and easily noticed by the user. But for it to be considered as evidence a forensic analysis is needed:

- Reduction in device Speed:

This means that device can be either phone, laptop etc. suddenly becomes slower than usual. Generally, we tend to ignore this problem just by considering it as a mere problem as phones get old or their capacity is decreased. We should not have this mindset as we should be aware that in this era information is wealth.

- Device shuts down itself occasionally:

This means when a phone or any device gets switched off without any usual reasons such as lack of charge or on scheduled time, then definitely it gives a sign that there is some external factor which is connected with the devices which must be checked.

- Unusual battery drain:

Generally, there is a specific reasonable duration or period till which a battery of every device will have life your device shows any abnormal battery drain where you need to charge your device's battery more often than usual, it is necessary to be noticed.

- Unknown files or folders:

When your device has an unusual and unfamiliar folder don't leave it as it is. It is always better to delete if we find it rather than taking it casually. As many times by installing files spyware will be injected into a device.

- Automatically redirected to unknown websites:

During usual use of a device, if a user gets redirected to other websites without him being clicked then there is a high chance of getting hacked and snooped. This happens when a user clicks on any link that a site has as an advertisement because the attackers get access through that activity of the user.

[15] https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8, Last Accessed on 09/01/2024

ISSN: 2582-6433

- Irrelevant pop-up ads:

This means when while browsing through the internet the user might face excessive advertisements popping up as of which will usually be irrelevant. And also, there is a high chance that adds pop up even if the user uses devices offline for instance in gallery. So, this requires high attention.

- Heating of devices even when not in use:

Generally, devices tend to get heated if they are used excessively or for a long duration of time. But it needs to cool down after the stoppage of use after some time. But if the device is hot even after that it indicates that some application is running in background, which can also be an application which is of unknown thus it needs to be addressed.

- Surge in data usage:

When there is a sudden increase in the usage of data of the device it might be due to the unknown operation of any applications. Therefore, this can also be a trigger warning that should make a user alert.

Have eye for suspicious messages or emails:

As this is the most obvious way to identify as the attacker who uses message method where they need the target user to click on a message or URL tries to send spam mails and message. This indicates that the user's device is being targeted for cyber-attack.

- Have an Anti-Malware software installed:

This helps in frequent check on the devices for any malware devices and also it makes sure that any spyware is not installed as it shows alter notification before user downloads an app which has spyware.

If any of this behaviour is established by your device the relatively easy way to determine whether your device is infected or not is to use Amnesty International Mobile Verification Toolkit. Though it won't confirm or disprove of the infection but it determines the indicators of compromise.

ISSN: 2582-6433

WAYS FOR PREVENTION:

There are essential preliminary things that need to be followed for better protection rather than for prevention as there can be no absolute solution, especially when attackers use zero-click exploits.

- Don’t not open unsecured URLs:

Most of the time malware are injected only by way where the user unknowingly clicks an unsecured URL and if users are being cautious not to do so they can be protected from all kinds of general cyber-attack except that of zero-click attacks. So only open trusted links and especially avoid unsubscribe links from suspicious sources as they first try to frustrate the user with spam mails then they send an email with link to unsubscribe, where by clicking it, they install the malware in user’s device.

- Frequent reset of device to remove non-persistent malware:

There is malware which do not persist, meaning they don't survive phone rest but get re-introduced as needed. In order to prevent this regular rest of the device is necessary.

- Regular update of version:

It is necessary to update your device of its version as it may fix bugs and security vulnerabilities. Sometimes manufacturers provide withy notification but most of the times it's not the case, so try and search yourself for updates.

- Avoid generic or physical passwords:

Most of the time the date of birth or the person's name will be set as a password. It is always better to use high security passwords and to avoid patterns, fingerprints as this reduces security and paves way for other third parties to access your device without your knowledge of your password.

- Avoid public networks such as wifi:

This is the most common way used by attackers as people tend to use services which are available for free more often. In case due to circumstance the use of public WIFI is necessary then try to avoid accessing sensitive information.

ISSN: 2582-6433

- Make sure to encrypt your data:

Enable remote-wipe feature wherever it is possible or encrypt your data so that even if your phone is lost, your data will not be lost as either you will be able to delete it without the other person accessing it else, it is protected in such a way that other person cannot access it even when he has access to your device.

- Separate device for personal and work purposes:

Wherever it is possible have different devices for different purposes along with sim and email id as this will ensure that your sensitive information is not accessed in your work device and might enhance the protection and less possibility of getting scooped of personal data.

- Your device as your own spy:

Especially your phone can be used to locate you and your confidential source. Therefore, it is always recommended that you don't take your phone during your meet and ensure to meet in a common neutral place and guard by CCTV for security purposes.

CONCLUSION:

This comprehensive analysis on Pegasus cases brought a clear understanding of how important the information is in this era and despite it being considered as a fundamental right it being violated by the governments itself for its own sake serves as a warning signal for every individual to safeguard their information. Simultaneously it is necessary to understand the importance of spyware as well because if it is used for an intended purpose for which it is produced, that is for national security purposes and to protect from terrorism it is one of the best tools to safeguard the country as a whole. So as a very known notion that technology has its own boon and bane it is up-to the person using it. Despite the judgement rendered in the US with respect to Pegasus still there is a continuing use of spyware which we understood from one instance as mentioned earlier. So, extrapolating this to the Indian context shows that individuals' efforts are necessary to safeguard their own information rather than judicial pronouncements. These Pegasus cases might bring the picture in mind that only a few important people's devices will be snooped but definitely that is not the case. Everyone's information is a wealth, be it a common man or elite. Therefore, it is essential for all classes of people to follow all precautions and prevention methods to safeguard their information.