ISSN :2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 6

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 Quarterly, 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.

 ISSN: 2582-6433

PEGASUS: A FUTURE OF NO PRIVACY

Authored By- Ayushi Upadhyay

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite"[1]

ABSTRACT

"The article provides a wholesome picture of how humans have become subservient to gadgets and digitalization. The most dangerous weapon in this technological era is spyware; and Pegasus is one such contrivance. This article examines the development, impact and concerns revolving around Pegasus with help of previous reports, publications, cases and statutes. The key finding of this article is focused on how this has emerged as a socio-legal affair in the society. It also comments on the involvement of Indian Government and the need for international awareness. At last it also discusses various legal aspects with the help of case laws."

KEYWORDS- Pegasus, Privacy, Fundamental Right, Technology, Government.

[1] David Shipman, *"Marlon Brando"*, ch.11 (Sphere, 1989).

 ISSN: 2582-6433

I. INTRODUCTION

It's 21st century already, humans have developed technology in a nick of time and which is still thriving incessantly as one of their finest inventions. The world is fenced by the technological web in which we are gravely entangled. One's life without these gadgets is maddening. From personal to professional, business to travelling, ordering food to getting medical assistance, almost everything is available online, even groceries!

"We all are dependent on technology" – an epiphany felt by almost every individual during this pandemic. But are these platforms safe? It's not only a question but a burning issue, since our reliance on such technology is inexorable and all our information from personal to professional are served on these cyberspaces, we have become most vulnerable to such cyber attacks.

Pegasus Spyware is one such software which has created a global wave in cyber space. It has been regarded as one of the 'most sophisticated tool to attack smart phones' and is even classified as the 'ultimate spyware' by many. Pegasus Spyware is named after the winged horse of Greek mythology. It is a Trojan horse computer virus which can 'travel through air' or sent 'flying through air'. The 'Trojan Spyware Alert' fake error message is a scam that pretends from Microsoft to trick people into thinking that their computer has been crashed or that a virus has been detected'[2]. This spyware can affect both android and iPhone devices.

Pegasus basically functions in three modes. At first a trap link is transmitted to the targeted person's phone which requires only a click for activation, or else it can also self-activate itself, leaving the victim oblivious of its presence, this is called 'zero-click' technology. This function gives Pegasus an upper hand from other malware which requires some or the other way of interaction to get ingrained. Once implanted, it can transfers the most basic information to the attacker including end-to-end encrypted messages, calendar events, passwords, intercept calls, gives control of mic and camera, browsing history, retrieved files and can even track the location of the victim. When entrenched, this malicious spyware is undefeatable.

It is owned by the NSO group, an Israeli firm, engaged in the business of building and selling surveillance software. The shares are divided among the founders Niv Carmi, Shalev Hulio and

[2] Stelian Pilici, *"Remove Trojan Spyware Alert Scam(Virus Removal Guide)"* , (September 25,2020), *available at:* https://malwaretips.com/blogs/remove-trojan-spyware-alert/ (last visited on October 9, 2021).

Omri Lavie (hence, NSO). Though this spyware has recently been discovered but its roots can be traced back to attacks UAE in 2013.

It was is 2016, when the Emirati Human Rights Activist Ahmed Mansoor received a series of SMS(Short Service Message) on his iPhone assuring "new secrets" of torture scenes in the prisons of United Arab Emirates if he clicked on certain URL. Mansoor immediately reached out to the Information Control Research Laboratory on the grounds of suspicion. After investigation if was transpired that the IP address was linked with NSO group and had Mansoor clicked on the certain URL, the spyware would have been implanted on the spot.

In January 2016, Carmen Aristengui, an investigative journalist in Mexico, started receiving messages with suspicious links after she published an investigation into property owned by former Mexican President Enrique Pena Nieto.[3]

This spyware has affected countries around the world. According to the revelations of Paris based organization Forbidden Stories and Amnesty International, around 50,000 Phone numbers of potential surveillance targets were reported. Some of the past instances are:-

i. December, 2020, Citizen Lab published a report detailing how government had used the Pegasus software to spy on or hack the phones of 36 Al Jazeera journalists.[4]
ii. In 2018, after the killing of Saudi Journalist and critique Jamal Khashoggi, Omar Abdulaziz, another dissident approached the court in Israel by way of filing a lawsuit, claiming that the NSO Group had licensed Pegasus to the Saudi government, which the government used to spy on him.[5]
iii. In Oct, 2019, WhatsApp filed a case suing NSO, claiming that the software operated by the firm had been used to attack its users. WhatsApp has requested the Department of Justice in the United States to launch an investigation.[6]

The Amnesty International filed a case against the NSO group which sought to force the Israel's Defense Ministry to revoke the security export license of the company. This was supported by the New York University of Law. On July 12, 2020 The Amnesty International released its press report stating that A Tel Aviv Court rejected its plea[7]. On this account Danna Ingleton, action Co-Director

[3] "Microsoft Exchange email hack was caused by China, US says", *The Daily Star*, (July 19, 2021) *available at* :https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/microsoft-exchange-email-hack-was-caused-china-us-says-2133991 (last visited on October 10,2021).
[4] *Available at:* https://sflc.in/anatomy-pegasus-spyware (last visited on October 15,2021).
[5] *Ibid.*
[6] *Ibid.*

of Amnesty Tech said "Today's disgraceful ruling is a cruel blow to people put at risk around the world by NSO Group selling its product to notorious human rights abusers."[8]

II. SCENARIO IN INDIA

Approximately 45 countries WhatsApp users' were affected by Pegasus including Pakistan, France, Cananda, Israel, India, Brazil, Singapore, South Africa and Switzerland, reported by the Citizen Lab. The operator was disguised under code-name of "Ganges" (deriving its name from the holy river in India) for targeting India, Pakistan and Bangladesh in the South East Asian region since June 2017. According to First Post report this operation targeted eight telecoms in India, including Airtel, MTNL and Hathway.

Pegasus marked its presence in India way back in late 2019 when it was revealed that WhatsApp of bureaucrats, journalist, activist, politicians who are considered as linchpin was invaded and hacked illegally, inculpating the government. On 20 May, 2019 WhatsApp submitted an incident report to the Indian Computer Emergency Response Team (CERT-IN) stating that it has "identified and fixed vulnerability which could which could have enabled an attacker to insert and execute a code on cellular devices"[9]

On December 11, 2019 in response to Unstarred Question No. 3686 which was asked in the Lok Sabha by Shri Anumula Revanth Reddy, the Hon'ble Minister for Electronics & Information Technology gave the following response:

"Government had been informed by WhatsApp of a vulnerability affecting some WhatsApp mobile users' through a spyware namely Pegasus. According to WhatsApp, this spyware was developed by an Israel based company NSO Group and it has developed and used Pegasus spyware to attempt to reach mobile phones of a possible of 1400 users' globally that includes 121 users' from India. Some statements have appeared based on reports in media, regarding breach of privacy of Indian citizens on WhatsApp. These attempts to malign the Government of India for the reported breach are completely misleading. The Government is committed to protect the fundamental rights of citizens, including right to privacy. The Government operated strictly as per provisions of law and

[7] Amnesty International, *" Israel: Court rejects bid to invoke notorious spyware firm NSO Group's export licence"*, (July 12,2020), *available at* : https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/ (last visited on October 15,2021).
[8] *Ibid.*
[9] Government of India, *"Withdrawal of WhatsApp security vulnerability warning from CERT-In website*", Ministry of Electronics and Information Technology, Unstarred Question No.-2747, Rajya Sabha, (12 December 2019)

laid down protocols. There are adequate safeguards to ensure that no innocent citizen is harassed or his privacy is breached[10]*"*

In July, *The Wire* reported that there were at least 300 Indian Phone numbers in the leaked global list of 50,000 numbers, including the name of a sitting Supreme Court Judge[11]. Some prominent names under the radar of Pegasus includes, Rahul Gandhi (opposition leader of the Congress Party), Pravin Togadia (Former International Working President, VHP), Ashwini Vaishnav (Union Minister for IT and Railways), Abhishek Banerjee(MP from West Bengal and National Secretary of Trinamool Congress), Ashok Lavasa (Former Election Commissioner), MK Venu (The Wire), Late Syed Abdul Rahmaan Geelani (DU Professor and Human Rights Activist), Prashant Kishore(Election Strategist), Jagadeep Chokkhar (Head, Association for Democratic Reforms) , employees of the U.S. Centers for Disease and Prevention, Delhi and the list follows.

Rahul Gandhi on July 19, 2021 tweeted, " *we know that he's been reading – everything on your phone*" implicitly attacking the Government. The Prime Minister was framed by the Opposition Party of "treason", emphatically stating that he compromised national security. The Indian Government was also accused of illegally spying on their neighboring countries, though no evidences were put against it. One peculiar thing was the name of Ashwini Vaishnav of Bhartiya Janta Party (BJP) in the list of potential targets, though he even called it out as an "attempt to malign the Indian democracy". Giving fodder to gossip was Government's refusal to discuss this issue in Parliament albeit its gravity which raised several questions, which included suspicions regarding Government's involvement in the 'spy scandal'.

This issue is alarming as it brings in the question of national security. Cyber-terrorism is new tool for the modern terrorist, hacking into the Government system of a country and crippling the military is cup of tea if access is provided. Not only can the terrorist group gain control over what is utterly impossible to approach but also makes the nation vulnerable in the international sphere. Paradoxically, success in "war on terror" is likely to make terrorist turn increasingly to unconventional weapons like cyber-terrorism[12].

---

[10] *Supra* note 5.

[11] The Wire Staff, *"Pegasus Project: 174 Individuals Revealed By The Wire On Snoop List So Far",* (August 4,2021), *available at* : https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance (last visited on October 19,2021),

[12] Gabriel Weimann, *"United States Institute of Peace: Special Report"*, 1200 17th Street NW, Washinton, DC 20036 (2017).

III. LEGAL ASPECT

The Greek philosopher Aristotle spoke of a division between the public sphere of political affairs and the personal sphere of human life. The dichotomy may provide an early recognition of a "confidential zone on behalf of the citizen".[13] Aristotle's distinction between the public and private realms can be regarded as providing a basis for restricting governmental authority to activities falling within the public realm. On the other hand, activities in the private realm are more appropriately reserved for "private reflection, familial relations and self-determination."[14]

John Stuart Mill in his essay, 'On Liberty' (1859[15]) denoted the need of separating the private zone from public in order to preserve the liberty of citizen.

Even the history is packed with many evidences that calls out for privacy, the right to let alone.

Privacy is a universal right. This right is enshrined in Article 12 of Universal Declaration of Human Right (UDHR), [16]Article 17 if International Covenant on Civil and Political Rights (ICCPR)[17], Article 16 of the Convention of the Rights of the Child (CRC)[18], Article 7 and 8 of the Charter of Fundamental Rights of European Union, 2012 which provides for respect for private and family life, home and communication and protection of personal data and its collection for specified legitimate purpose.

On 24th August 2017, overruling the decisions of ***M.P Sharma v. Satish Chandra, District Magistrare, Delhi[19]*** (constituting 8 judge bench) and ***Kharak Singh v. State of Uttar Pradesh[20]***(constituting 6 judge bench), unanimously delivered a historic decision in ***K.S. Puttasawamy v. Union of India*** [21]recognizing Right to Privacy as a fundamental right guaranteed to every individual by the Constitution of India, under Article 21 in particular Part III of the Constitution. In its judgment the Supreme Court clearly mentioned that this issue reaches out to the foundation of a constitutional culture based on the protection of human rights and enables court to revisit the basic principles on which our Constitution has been founded and their consequences for

[13] Michael C. James, "A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe", *Connecticut Journal of International Law"*,Vol.29, Issue 2, p.no. 261 (Spring 2014).
[14] *Ibid.*
[15] John Stuart Mill, "*On Liberty (1859)",* p.no.13, (Batoche Books Limited 52 Eby Street South Kitchener, Ontario N2G 3L1 Canada, 2001).
[16] The United Nations, 1948, art. 12.
[17] International Covenant on Civil and Political Right, 1966, vol.999, art.17.
[18] Convention on Rights of the Child, 1989, vol. 1577, art.16.
[19] 1954 AIR 300.
[20] 1963 AIR 1295.
[21] (2017) 10 SCC 1.

a way of life it seeks to protect. The court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world.[22] They also overruled the ***ADM Jabalpur*** [23]case which called for temporary suspension of fundamental rights during the proclamation of emergency and called into question the judicial reasoning in the ***Naz Foundation*** [24]case that had suggested that the 'minuscule minority' LGBTQ community was not entitled to a right to privacy. This decision has connected out privacy jurisprudence over the years with our international commitments and established out conformity with comparative laws around the world.[25]

Though Right to Privacy is not an absolute right, it is subjected to some restriction, according to a report by mondaq, The Supreme Court was at pains to clarify that the fundamental right to privacy is not absolute and will always be subjected to reasonable restrictions. It held that the State can impose restrictions on the rights to privacy to protect legitimate states interest but it can only to do so by following the three-pronged test summarized below:

(a) Existence of a law that justifies an encroachment on privacy;
(b) A legitimate state aim or need that ensures that the nature or the content of this law falls within the zone of reasonableness and operates to guard against arbitrary state action; or
(c) The means adopted by the state are proportional to the objects and needs sought to be fulfilled by the law.[26]

Section 43 of Information Technology Act (referred as IT Act) provides for the penalty and compensation for damage to computer, computer system if in any case without the permission of the owner or in-charge of computer, computer system or computer network or resource *inter alia* (1) access or secures access to such network or computer; (2) downloads, copies or extracts any data, or database held or stored in any removable storage medium; (3) implants any virus or contaminant; (4) damages or causes to the computer in any way; (4) disrupts or causes disruption; (5) denies or causes denial of access to the authorized person; then such person is punishable for imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.[27]

[22] *K.S. Puttaswamy v. Union of India,* Supreme Court of India Civil Original Jurisdiction, Writ Petition (Civil) No. 494 of 2012.
[23] 1976 AIR 1207, 1976 SCR 172.
[24] 2009 SCC Del 1762.
[25] Trilegal, "*India; Supreme Court Declares Right to Privacy a Fundamental Right"* , (31st August 2017), *available at* : https://www.mondaq.com/india/privacy-protection/625192/supreme-court-declares-right-to-privacy-a-fundamental-right (last visited on October 19,2021).
[26] *Supra,* note 24.
[27] The Information Technology Act,2000 (Act 21 of 2000), s. 43.

The Personal Data Protection Bill was introduced on December 11, 2019 by Mr. Ravi Shankar Prasad, Minister of Electronics and Information Technology on Lok Sabha, the bill provided for the "protection of the privacy of individuals relating to personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in processing data, laying down norm for social media intermediary, cross-border transfer accountability of entities processing persona data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto."[28]

Privacy is indispensable for autonomy which shields individual's dignity. Invading someone's privacy is akin to making them a human puppet. One is prone to powerlessness and to the feeling helplessness. Imagine a world without any protection to privacy; it would be as if you are walking on the edge of a cliff tied down to rope which is not under your control. This spyware not only hinders privacy of a person, but at stake is also the liberty. You cannot express anything or act, similar to being kept as a hostage, monitored day and night. It snatches away our Right to Freedom and Speech, yet another Fundamental Right guaranteed by the Constitution.[29]

The Indian Government has launched various schemes and initiatives to enhance national security, some of the vigilant efforts includes:

(1) Cyber Surakshit Bharat Initiative – with an aim to spread cybercrime awareness, this scheme was launched in 2018 which focuses on developing safety measures for Chief Information Security Officers (CISOs) and frontline IT staff of almost all government departments.

(2) National Cyber Security Coordination Centre (NCCC) – it was implemented by Indian Computer Emergency Response Team (CERT-IN) in 2017, it was set up to detect any kind of cyber threat on web traffic, and it even monitors all communications between the Government and Private Service providers.

(3) Cyber Swachhta Kendra- introduced in 2017, it is a part of Government's Digital India Initiative. It functions to annihilate viruses or any infection which might harm the system.

(4) Indian Cyber Crime Coordination Centre (l4C)- the outlay of this project was Rs.415.86 Crores. It protects the system against the misuse from terrorist or extremist attack.

[28] The Personal Data Protection Bill, 2019.
[29] The Constitution of India, art. 19.

 ISSN: 2582-6433

Looks into cybercrime throughout the country. This project has several components such as :- National Cybercrime Threat Analytics Unit (TAU) ; National Cybercrime Reporting; Platform for Joint Cybercrime Investigation Team; National Cybercrime Forensic Laboratory (NCFL) Ecosystem; National Cybercrime Training Centre (NCTC); Cybercrime Ecosystem Management Unit; National Cybercrime Research and Innovation Centre.

(5) Computer Emergency Response Team- India (CERT-IN)- formed on 2004, it deals with cyber issues such as hacking and phishing.

Though chances to mouse-trap a huge crowd is very unlikely but prevention is better than cure, therefore one must take some serious measures personally while using any gadget such as avoiding free Wifi services in any public or private places; expunging unnecessary data and enabling remote-wipe feature whenever required; not tapping on any web-link sent through unknown sources; limiting access to your phone through pin, finger-lock, face-lock, whatever is applicable; upgrading your phone whenever necessary and installing VPN could be useful. Multifarious videos explaining how to configure devices securely are available on Commissioner's E-safety website, which is easily accessible.

IV. CONCLUSION

It takes less than five minutes for the attacker to implant the spyware and infect the person's device, without the knowledge of the user. Just how dangerous it would be give your control to a complete stranger without you knowing about it. This is what this malefic spyware does. Now, not only individuals but the "largest democracy" in the world is falling prey to a spyware developed by a private company.

For decades the surveillance agencies has been accused for its clandestine nature of working, sometimes being exposed in the public. The software industry has always claimed their assistance to Government but has failed miserably in attaining public trust. The rate at which this spyware is being used is not only violating human rights across the globe but is quite staggering. This issue should be addressed at the international platform, seeking participation and strenuous efforts from more and more countries.

The functioning of this spyware is *ultra vires* of the principles established in ***K.S. Puttasawamy v. Union of India*** [30]. The breach of privacy has led to a worldwide rage. It is disheartening to see that the Indian Government has refused to address this issue and has left the questions concerning their involvement and use untouched. Though this issue is pending before the Hon'ble Supreme Court, which has recently formed an Independent Committee of technical experts that will enquire and investigate into this matter thoroughly, stating that Centre cannot always let go of such issues wherever national security is concerned. A bench comprising of Chief Justice NV Ramana and Justices Surya Kant and Hima Kohli stated that there has not been any denial by the Centre regarding this matter. The Committee will also give recommendations and amendments as and when required. According to the report by *The Indian Express* the bench on selecting the Committee members said, "It would be appropriate to state that in this world of conflicts, it was an extremely uphill task to find and select experts who are free from prejudices, are independent and competent. Rather than relying upon any Government agencies or any, we have constituted the Committee and shortlisted expert members based on bio-data and information collected independently."[31]

As citizens who are open to these vulnerabilities without adequate accountability from the government, we need to start pushing for a surveillance reform and the need for a judicial

[30] *Supra* note 22.

[31] Ananthakrishnan G, "SC orders independent probe into Pegasus, says Govt can't get free pass every time 'national security is raised", *The Indian Express* (27th October 2021).

oversight in our surveillance framework. As of now everything is done by the Executive, including the review or the interception Orders. There is a critical need for judicial oversight of all interception rders like there is in the United Kingdom. The surveillance orders must be reviewed and approved by a judge before it can be enforced.[32]

Since we have unconditionally rooted ourselves to technology and gadgets, it is somewhat unfeasible to imagine life without it. There are manifold prospects of cutting-edge technology but the consequences comes in free, and even a little default can result into adversity. There is a need of awareness among people about their privacy rights, accurate knowledge can help in highlighting the fact that indirectly we are being deprived of freedom of speech and expression, and as rightly said by George Washington, *"If freedom of speech is taken away then dumb and silent we may be led, like a sheep to the slaughter house."* [33]With an ever increasing dependency and screen time, it is very likely that users' like us are more prone to fall for this spyware. Albeit the fact that the Government has launched various schemes keeping in mind safety of the citizens, risks are always susceptible. Demanding accountability from the Government has visibly become a futile effort. Thus, our safety rests in our own hands.

[32] *Supra note* 5.
[33] George Washington, First U.S President, address to the officers of army, (March 15, 1783).