PEGASUS AND THE RIGHT TO PRIVACY

Neha Mishra, Assistant Professor, Amity Law School, Amity University, Haryana

ABSTRACT

Every once in a while, news reports of unauthorized surveillance and cyber-crimes threaten the foundation of democracy. This time around, Pegasus spyware an Israeli NSO Group, is making headlines for infiltrating the mobile phones of several high-profile individuals in India without their knowledge to extract and transfer information. In the context of ever-increasing concern regarding surveillance due to technological advancement that impinges upon basic fundamental rights by enabling the State to monitor the lives of its citizens more easily and at retreating cost, the paper attempts to cover various facets of this issue. The paper begins with a brief introduction followed by explaining the Pegasus Project. It then discusses in detail the legal provisions that deal with interception and surveillance in India and gives an overview of the evolution of the right to privacy jurisprudence which is one of the fundamental challenges to illegal surveillance. The paper then highlights the conundrum of the right to privacy and state surveillance and in what ways it raises grave concerns for a civilized democratic society. The paper concludes with possible suggestions.

"There will come a time when it isn't "They're spying on me through my phone anymore. Eventually, it will be 'My phone is spying on me'."

-Philip K. Dick

INTRODUCTION

The right to privacy is a fundamental human right accepted throughout the democratic world. Available to every citizen though in varying degrees, privacy is effectively a limited right. In India, the current state of surveillance is distressing and alarming. Pegasus is the recent example of widespread and continuing abuse of software which has accessed leaked database of several phone numbers provided by government clients of an Israeli spyware firm called NSO but manufacturers insist are only for use against criminals and terrorists. The sheer magnitude of this unauthorised surveillance has shocked the civil society. Surveillance is justified in narrowly defined situations when it is essential and proportional to a legitimate goal however, national security is given primacy over individual liberties. Not only the existing and proposed legal framework fails to protect our right to privacy but also individuals are unaware of the extent of surveillance conducted by the Government. This calls for an extensive deliberation on legal and constitutional critique on to what extent State surveillance in India is justified that it doesn't encroach upon the right to privacy of individuals.

PEGASUS PROJECT

Paris-based media non-profit Forbidden Stories and Amnesty International accessed leaked database of numerous phone numbers across the world targeted by a sophisticated spyware called Pegasus. The data was shared by them with global media organizations as part of a collaborative investigation called Pegasus Project. Pegasus is a spyware capable of infiltrating smartphones that run on both iOS and Android operating systems and turning it into surveillance devices, developed and licensed by an Israeli company called NSO Group. Amnesty International observed that even after issuing security updates, iOS and Android devices were breached. As per reports, over 40 journalists, 2 Union Cabinet Ministers, 3 opposition leaders, a sitting Supreme Court judge and a Constitutional authority, government officials, business persons, and scientists were potential targets in India.

The method of attack in Pegasus is called **zero-click attack** that doesn't require any action by

the user. Simply by giving a missed WhatsApp call, the spyware can hack a device. Once the spyware enters the device, it installs a module to track call logs, read emails, messages, access photos, videos, internet history, calendar, activate the microphone and camera and even gather location data to send the information to the attacker in an unauthorised manner. It alters call logs so that the user has no awareness of what happened. Also, it can be installed manually on a device or over a wireless transceiver. It self-destructs and removes all traces, in a case for more than 60 days it fails to connect with its command and control server or it detects that it was installed on the wrong device or SIM card. Israeli Defence Ministry stated that Pegasus and other cyber products are exported "exclusively to government entities" and are **solely for the purpose of preventing and investigating crime and counter terrorism.**

The response of the Indian government so far has been complicated as it has neither denied nor confirmed the allegations and also asserted that in India surveillance has to be legally authorised. Even the NSO Group has denied all media reports that its Pegasus software is associated to mass surveillance and claimed that sales of all its technology are approved by the Defence Ministry of Israel.

PRIVACY AND SURVEILLANCE LAWS IN INDIA

In India, communication surveillance is primarily covered under two laws, namely the Telegraph Act, 1885 that deals with interception of calls and the Information Technology Act, 2000 that deals with surveillance of electronic communication.

Under **Section 5(2) of the Telegraph Act** government can intercept calls in specific situations such as in the interest of sovereignty and integrity of India, friendly relations with foreign states or public order, State security and preventing incitement to the commission of an offence. These restrictions are also mentioned under Article 19(2) of the Constitution on free speech however, they are imposed in cases of "**public emergency or in the interest of public safety."** Since the terms hadn't been defined, the Supreme Court interpreted them to mean "the prevalence of a sudden condition or state of affairs affecting the people at large calling for immediate action" and "the state or condition of freedom from danger or risk for the people at large", respectively.

Further, grounds for selecting a person for surveillance and the extent of information to be gathered have to be recorded in writing. 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, unless their transmission has been prohibited under this subsection. In the case of ***Public Union for Civil Liberties v. Union of India***[1] the Supreme Court observed a lack of procedural safeguards in the provisions of the Telegraph Act and held that ***"Right to hold telephone conversation in privacy of one's home or office without interference can be claimed to be right to privacy since telephonic conversations are often of an intimate and confidential nature. Thus, tapping is a serious invasion of the privacy of an individual. It is true that every Government exercises some degree of surveillance operation as a part of its intelligence outfit but at the same time right to privacy of citizens has to be protected."*** This judgment of the Court formed the foundation for **introducing Rule 419A in the Telegraph Rules in 2007** and later in rules prescribed under the IT Act in 2009. Rule 419A reads that direction for interception under Section 5(2) maybe issued only by Union or State, Home Secretary, or in unavoidable circumstances by another authorised officer.

The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and **Section 69 of the IT Act** were enacted to extend the legal framework for electronic surveillance. Section 69 of the IT Act offers a much broader and vague scope than the Telegraph Act as the only condition required for engaging in electronic surveillance is for 'investigating an offence'. This draconian provision offers the government complete opacity regarding interception, monitoring or decrypting information without any judicial oversight. However, the provision doesn't permit the government to install spyware or hack mobile devices and in fact, hacking of mobile device is explicitly criminalised under **Section 66 read with Section 43 of the IT Act**.

India is a signatory of the Universal Declaration of Human Rights (Article 12) and the International Convention on Civil and Political Rights (Article 17) both of which recognise privacy as a fundamental right. **As Bruce Schneier states *"Privacy is an inherent human right and a requirement for maintaining the human condition with dignity and respect."*** After a bumpy start in **MP Sharma**[2] and **Kharak Singh**[3] cases in which it was held that the right to privacy is not protected under Constitution, jurisprudence on privacy evolved and the

[1] Public Union for Civil Liberties v. Union of India AIR 1997 SC 568.
[2] MP Sharma v. Satish Chandra (1954) SCR 1077.
[3] Kharak Singh v. State of UP (1964) 1 SCR 332.

decision stands over-ruled. ***In R Rajgopal v. State of Tamil Nadu[4] court held that "Right to privacy is part of right to life and liberty enshrined under Article 21 of Constitution. Any right enshrined under Article 21 can't be curtailed except according to the procedure established by law which must be fair, just and reasonable. KS Puttaswamy v. Union of India[5]*** declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and other fundamental rights guaranteed under part III of the Constitution. The case deliberates on the reasons for which privacy is essential and could mean to be violated in instances of surveillance. It requires that any instance of surveillance must be legitimate, proportionate and necessary. However, surveillance conducted using Pegasus spyware, which is awfully intrusive, doesn't conform to any of those requirements, especially when less intrusive alternatives are accessible to the government.

CHALLENGES TO THE RIGHT TO PRIVACY AND STATE SURVEILLANCE

In a modern globalised world, privacy is a privilege granted to individuals to protect their choices, actions and private opinions shared in a personal sphere from being exposed or scrutinised by the world at large. Indian Constitution under Article 21 pledges to protect this virtue wherein privacy of one's home and confidentiality of communication form the basic standards. More than a mere negative right to be let alone,[6] privacy produces conditions essential for human intimacy while facilitating the exchange of ostracized or unconventional ideas without dread of consequences. Surveillance impacts intellectual privacy which is the liberty to cultivate ideas without being monitored and also informational privacy which includes ideas of secrecy, control and anonymity.[7] Since there is an imbalance of power between the State and citizens, it is expected that State will have higher privacy as compared to private citizens. Another reason could be the concentration of power, monopoly over violence and the possibility of its misuse by the State. Many law enforcement authorities like the Intelligence Bureau, Central Bureau of Investigation and Research and Analysis Wing lack statutory basis and mostly function with minimum accountability. On these lines, the State-citizen asymmetric power dynamic heightens with surveillance and may even lead to

[4] R Rajgopal v. State of Tamil Nadu (1994) 6 SCC 632.
[5] KS Puttaswamy v. Union of India (2017) 10 SCC 1.
[6] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 193-95.
[7] R v. Spencer (2014) 2 SCR 212.

blackmail, discrimination and selective enforcement. This risk deepens in case of secret surveillance.

The Personal Data Protection Bill, 2018 lays various exemptions when data processing is exempt from almost all obligations and safeguards under the Bill, one such significant exemption is under Section 42 which provides that processing of personal data in the interest of the security of the State shall be exempt from obligations of Bill as long as it is authorized by law; in accordance with the procedure established by law, made by Parliament; and is necessary for and proportionate to, such interests being achieved. The three tests are as per the formulation of the Court in Puttaswamy case, thus are a welcome step. However, Justice Srikrishna Committee final Report on the Bill observed that ***"National security is a nebulous term, used in statutes of several jurisdictions to denote intelligence gathering activities that systematically access and use large volumes of personal data" and that "key question is what safeguards can be instituted to ensure that use of this ground is restricted to genuine cases of threats to national security."*** Thus, the question arises, are the safeguards under Section 42 enough?

The Bill missed an opportunity for bringing key surveillance reforms which might render the safeguard under Section 42 to be inadequate. The Bill failed to propose the much-needed amendments to present surveillance provisions under the Telegraph Act and the IT Act. There is a lack of judicial oversight or ex-ante judicial determination of whether a proposed surveillance measure conforms to the conditions mentioned under Section 42. It is of relevance as in several cases, individuals are unaware of any surveillance activities on them and thus the possibility of post-facto challenging the invocation of 'security of State' exemption or non-compliance with Section 42 is marginal. According to Section 42, State is exempted from complying with all accountability and transparency measures in the Bill and the Bill doesn't prescribe any regulatory, parliamentary or executive oversight thus, imposing no obligation on State to disclose the number of surveillance operations undertaken, kind of sensitive information collected, duration of storing such personal data and the procedure followed for destructing the same. It is a settled principle that illegally obtained evidence is admissible in court as long as State can demonstrate its relevance and genuineness.[8] This renders the

[8] RM Malkani v. State of Maharashtra (1973) 1 SCC 471.

safeguard mentioned under Section 42 of no avail as the Bill is silent on the aspect of illegally obtained evidence thus leaving little incentives for law enforcement agencies to abide by rules.

CONCERNS

Pegasus spyware enables deep intrusion into the devices of people resulting in insights into all aspects of their lives thus crossing the red line with total impunity. The very existence of a surveillance system in a democracy regardless of its actual use impacts the right to privacy and liberty of citizens and the exercise of freedom of speech and personal liberty guaranteed under Articles 19 and 21 of the Constitution respectively. **United Nations High Commissioner, Michelle Bachelet stated that *"Various parts of UN Human Rights system, have repeatedly raised serious concerns about the dangers of authorities using surveillance tools from a variety of sources supposed to promote public safety in order to hack the phones and computers of people conducting legitimate journalistic activities, monitoring human rights or expressing dissent or political opposition."*** Surveillance software is linked to the arrest, intimidation and even killing of journalists and human rights defenders in the past. It triggers fear, paranoia, causes people to censor themselves from exchanging unorthodox and controversial ideas and creates an aura of distrust in the privacy of their own homes. Kharak Singh case explained how surveillance places psychological restraints that conditions our minds and affects their freedom to think and express freely in a way that impacts their personal liberty. Surveillance promotes authoritarianism in government functioning as it permits the executive to exercise a disproportionate amount of power on citizens and affects their personal lives. Without human rights-compliant regulatory frameworks, there are too many risks that surveillance tools could be used to intimidate critics and silence dissent. In the absence of sufficient information on the current surveillance conducted, victims are denied constitutional remedies available under Articles 32 and 226 of the Constitution. Also, there is a lack of transparency relating to government orders under Section 69 of the IT Act. In the age of technology, the capacity of the State to encroach upon the private sphere of individuals has intensified. In Puttaswamy[9] capturing the dangers of technology upon privacy, Kaul J notes that ***"The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance***

[9] Ibid 5.

in ways that are unimaginable." A comprehensive data protection law that addresses the loopholes in existing frameworks for surveillance is yet to be enacted.

WAY FORWARD

To stay safe, users must ensure that software in devices is updated and all apps are installed directly through the official store. Suspicious emails or texts should not be clicked. Companies that develop and distribute surveillance technologies are responsible for evading human rights abuses and must take instant steps to mitigate and remedy the harm their products are causing and carry out "human rights due diligence" to guarantee that they don't participate in such disastrous consequences now or in the future. States have a duty to protect individuals from privacy rights abuses by companies and thus must ensure that businesses meet their human rights responsibilities by becoming more transparent in their design and use of products and putting in place effective accountability mechanisms. Governments should not only immediately stop using surveillance technologies in ways that violate human rights but also take concrete actions to protect against such invasions of privacy by regulating the sale, distribution, use, and export of surveillance technologies created by others and ensure strict oversight and authorization. Indian surveillance regime should be reformed by incorporating the ethics of surveillance and deliberate the moral aspects of how surveillance is employed. Surveillance reform is the need of the hour. Not only the existing legislations are weak but there is also a need for holistic debate before the Personal Data Protection Bill, 2019 is enacted as the Bill fails to consider surveillance and offers wide exemptions to government authorities. **Marty Rubin** correctly states that ***"The right to privacy is the pre-eminent right of any democracy."***