THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

August 5, 2021

The Pegasus Case Must be Used to Press for Change in Surveillance Laws

By: Vrinda Bhandari

To ensure comprehensive privacy for all Indians, we need to generate public pressure to make the Government of India reform the existing framework for surveillance and introduce a data protection bill in Parliament that is much tighter than the current draft.

The murky world of private spyware is now out in the open. Pegasus, an Israeli spyware meant to target terrorists, has reportedly been used against journalists, activists, and political leaders in India. The Pegasus attacks are a cause for worry because of their undemocratic use, unprecedented magnitude, and unreasonable invasion into the privacy of individuals, compounded by a complete lack of transparency and stonewalling by the government.

Pegasus gives governments or authorised law enforcement agencies the ability to infiltrate mobile devices through 'zero click' attacks, and take control of the target's phone; collect data; view contact lists, messages, and internet browsing history; remotely access the phone's camera and microphone; and track a target's location and movements. This is done without the knowledge and consent of the target, and, currently, there exist no known fixes for this malware.

The government has neither categorically admitted nor denied the use of Pegasus, stating instead that no "unauthorised interception" took place, and that India has an established framework for lawful surveillance.

However, the use of cyber weapon and military grade technology such as Pegasus goes well beyond the powers of interception, monitoring, and decryption (cumulatively "electronic surveillance") authorised under Section 69 of the Information Technology Act, 2000 (IT Act). Installing the Pegasus spyware on a target's phone is illegal and falls within the IT Act's prohibition of hacking (defined as the introduction of a "computer contaminant" or "computer virus"). Hacking is a criminal offence, and no exception has been carved out for national security reasons. The Pegasus infractions thus represent a case of illegal and unconstitutional surveillance.

Need for surveillance reform

At the same time, the Pegasus controversy presents us with an opportunity to overhaul our existing and opaque surveillance framework. Targeted electronic surveillance is legal in India. The government can, when it is "necessary or expedient" to do so, intercept, monitor, or decrypt information under certain circumstances relating to national security, public order, law enforcement, or criminal investigation purposes. Each surveillance order must be reviewed by a three-member executive review committee, comprising the cabinet secretary, legal secretary, and the telecom secretary of the union government. While upholding the constitutionality of the existing surveillance regime under the Telegraph Act in 1997, the Supreme Court clarified that prior judicial scrutiny of surveillance action was not necessary, and executive oversight provided sufficient procedural safeguards.

A lot has changed since 1997. First, our understanding of privacy has evolved after the Supreme Court's privacy decision in *Puttaswamy* (2017) to incorporate notions of dignity, autonomy, self-determination, and consent. Privacy provides us protection from intrusive observation, the unauthorised uses of personal information, and gives us the ability and 'breathing room' to think freely. As Justice Subba Rao recognised in his famous dissent in *Kharak Singh*, that was subsequently approved in *Puttaswamy*, "the shroud of surveillance" serves as a "psychological restraint" upon an individual and "perforce engender inhibitions" in her, where she cannot think or act freely.

Simultaneously, while surveillance is not new, the nature of surveillance has changed. Surveillance today is both *wider*, covering a larger section of society, and *deeper*, being more invasive. This is a result of expanding technological capacity and increased cooperation between the state and private actors, as we have seen in Pegasus. The US Supreme Court acknowledged this change a decade ago::

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical'. This is because traditional surveillance methods required time and money, were difficult to scale, and had to function on limited police resources. Modern day surveillance techniques, on the other hand, reveal more information, especially when

surveillance is carried out over a prolonged time period.

Second, empirical research suggests that the government of India's review committee will be unable to provide sufficient protection to check the unauthorised use of surveillance powers. Replies by the home ministry in 2014 under the Right to Information Act (RTI) revealed that the central government issued an average of 7,500 to 9,000 interception orders for telephones per month. This number is likely to have only increased since then. Interestingly, citing national security concerns the central government has refused to respond to recent RTI requests seeking similar aggregate figures of interception orders passed between 2016–18.

> *Surveillance today is both wider, covering a larger section of society, and deeper, being more invasive.*

Either way, a committee comprising three senior bureaucrats that meets once every two months cannot actually apply its mind to such a vast number of surveillance orders (15,000–18,000 every two months). Expecting the application of mind or due process at such meeting is "unrealistic", in the words of the Justice Srikrishna Committee Report on Data Protection (2018). This means the only protection afforded by the law against executive overreach fails in practice.

Third, as I have argued previously, judicial oversight is a constitutional imperative after the Supreme Court's judgment in the Aadhaar Case (*Puttaswamy II*) since executive oversight over executive surveillance orders fails the test of proportionality. Independent oversight over surveillance action — whether in form of judicial review or parliamentary oversight — is the norm in modern democracies such as the United Kingdom, Germany, South Africa, the United States, and Canada and is part of international human right principles (the 'Necessary and Proportionate Principles'). It flows from the requirement for rule of law and the importance of accountability and safeguards against excessive state action. According to the Justice Srikrishna Committee Report on Data Protection:

> Surveillance should not be carried out without a degree of transparency that can pass the muster of the Puttaswamy test of necessity, proportionality and due process. This can take various forms, including information provided to the public, legislative oversight, executive and administrative oversight and judicial oversight. This would ensure scrutiny over the working of such agencies and infuse public accountability. Executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both. (p 125, *emphasis supplied*)

Various petitions are pending before the Supreme Court since 2019, challenging the constitutionality of the existing surveillance framework based on these arguments. However, despite pleadings being complete, no substantive hearing has taken place.

Need for improved legal protections during trial

Surveillance reform is one part, albeit an important part, of the story. To ensure improved privacy protections for all citizens, we need to make changes to other parts of the criminal justice system as well.

Currently, illegally obtained evidence is admissible in courts in India, as long as it is "relevant". Courts have held that "even if a document is procured by improper or illegal means, there is no bar to its admissibility if it is relevant and its genuineness is proved." Extending this rationale to the operation of electronic surveillance would reduce the incentive of law enforcement agencies to comply with even the bare minimal level of procedural safeguards enshrined in the IT Act and the Interception Rules, 2009. This likely increases the risk of privacy violations by the state and reinforces a 'crime control' model, where the state prioritises reduction of crime and efficiency in the criminal justice system over individual liberty and freedom.

> *[I]t is imperative that we amend our laws to ensure that evidence obtained illegally... or improperly...should not be admitted as evidence.*

In contrast, the 'due process model' focuses on the primacy of an individual, and seeks to limit state power in order to establish a fairer criminal justice system. Privacy scholar and researchers such as Neil Richards or Evan Selinger advocate a similar approach where they argue that surveillance is not meant to be a frictionless process and that introducing inefficiencies and transaction costs in a surveillance framework separates democracies and rule of law cultures from police states.

Puttaswamy, with its nuanced understanding of privacy and articulation of a strong proportionality test as a new standard for judicial review, arguably moves from a 'crime control' perspective to a 'due process' model. Gautam Bhatia explains this as a movement from

the "culture of authority" (where state authority and state action is rarely questioned) to a "culture of justification" (where every state action is expected to be justified).

Thus, for surveillance reform to be meaningful and to give proper effect to the due process model, it is imperative that we amend our laws to ensure that evidence obtained illegally (such as through hacking) or improperly (in violation of the statutory surveillance or data protection provisions) should not be admitted as evidence in criminal proceedings. This will introduce accountability into the actions of law enforcement agencies, thereby improving the rule of law and privacy for all citizens.

Reform of intelligence agencies

Pegasus is a spyware sold to sovereign governments or their authorised law enforcement agencies. Intelligence agencies in India, such as the Intelligence Bureau (IB), the Research & Analysis Wing (RAW) exist outside of all statutory, parliamentary, or judicial oversight mechanisms. The IB, in fact, traces its origin to a British government order of 1887, while the RAW was established pursuant to a government order in 1968. This allows them to operate with relative impunity, with few procedural safeguards in place to protect civil liberties. This is in stark contrast to intelligence agencies across the world, such as the Central Intelligence Agency (US), the MI5 and MI6 (UK), or the Federal Intelligence Service, Bundesnachrichtendienst (Germany) that have a statutory basis, and are subject to some — though arguably not enough — independent oversight.

In India, however, the statutory basis of even the Central Bureau of Investigation (CBI) is suspect, with the Gauhati High Court in 2013 striking down the government resolution constituting the CBI, and holding that the CBI is not a 'police force' under the Delhi Special Police Establishment Act. The Supreme Court immediately stayed the high court's judgment and the matter has been in cold storage over the last eight years.

> *[T]he PDP Bill represents a missed opportunity for surveillance reform, as it provides wide exceptions and exemptions to state law enforcement authorities.*

These issues are not new, and there have been several calls for intelligence reform over the last decade. In 2010, the then vice president, Hamid Ansari, made a case for intelligence reform, through parliamentary oversight committees and "an open system of public accountability". However, the government did not act on his proposals

One year later, in 2011, Manish Tewari, a Congress MP, introduced the Intelligence Services (Powers and Regulation) Bill as a private members bill to regulate the operation of intelligence agencies such as the IB, RAW, and the National Technical Research Organisation (which functions under the control of the prime minister) and establish an intelligence ombudsman. The bill prohibited these intelligence agencies from taking any action that furthered the interests of any political party, coalition of parties, or similar interest group. Unfortunately, the bill lapsed. After that no similar bill has been introduced in parliament by any government in power, whether the Congress or the BJP.

In 2012, following the Mumbai terror attacks of 2008, the Institute of Defence Studies and Analyses published *A Case for Intelligence Reforms in India*, arguing for introducing a law "laying down the charters, functions and duties of intelligence organisations" and for providing a "legal basis for different tiers of accountability — executive, financial and legislative." However, its recommendations were also ignored.

So here we are, more than 10 years later, relitigating the same issue. Unless we fundamentally change the operating structure and incentives available to intelligence and law enforcement agencies, and introduce transparency and accountability in their functioning, we will always be left with more questions than answers in the aftermath of cases such as the Pegasus scandal.

Personal Data Protection Bill: A solution?

The passage of the long-awaited data protection law is expected to improve the state of affairs in India. In fact, many have argued that the proposed Personal Data Protection Bill, 2019 (PDP bill) would have provided those affected by the Pegasus malware with an avenue to seek legal redressal.

However, as I have written previously, the PDP bill represents a missed opportunity for surveillance reform, as it provides wide exceptions and exemptions to state law enforcement authorities. Despite the Justice Srikrishna Committee Report expressly acknowledging that the absence of inter-branch oversight over executive intelligence actions (such as surveillance) was "not just a gap

that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional", neither his draft PDP bill, 2018 nor the PDP bill, 2019 engage with this issue.

On the contrary, Clause 35 of the PDP bill is very vague and provides broad exemptions to law enforcement and intelligence agencies in India. It allows the state to exempt these government agencies from the entire provision of the PDP bill simply if it is "expedient" (read convenient) or "necessary" to do so in the interest of national security, public order, friendly relations with foreign states, or to prevent the commission of certain offences. Moreover, the government can order this exemption without any judicial or parliamentary approval.

What does this mean in practice? On the application of the exemption, law enforcement agencies (i) are under no obligation to process our personal data and our sensitive personal data in a "fair and reasonable" manner; (ii) they need not follow principles of data minimisation, collection limitation, or use limitation that focus on collecting and using only information that is necessary; and (iii) they do not even need to comply with basic security safeguards to ensure that the data is not leaked.

> [P]inning our hopes on the PDP Bill, 2019 to provide an adequate remedy or ensure accountability and transparency in a future Pegasus-style case may prove to be a hopeless exercise.

Similarly broad exemptions are provided in Clause 36 to state and private actors who process personal data for the prevention, detection, investigation, or prosecution of "any offence or any other contravention of any law." This broad phrasing can theoretically also include any civil law contraventions such as breach of contract or a speeding ticket.

Notably, there is no statutory requirement enshrined within the PDP bill that the actions of law enforcement agencies while invoking such exceptions must meet the tests of necessary and proportionality as required by *Puttaswamy.* Additionally, the independence of the proposed regulator, the Data Protection Authority, is also undermined, since the constitution of the seven-member-committee is left to the discretion of the government, as the selection committee that will choose members will comprise three bureaucrats, including the cabinet secretary.

Given these factors, pinning our hopes on the PDP bill to provide an adequate remedy or ensure accountability and transparency in a future Pegasus-style case may prove to be a hopeless exercise. Where does that leave us?

What next?

Surveillance, by its very nature, is covert and secretive, and there is no scope for an individual subjected to surveillance to approach a court of law, either prior to, during or subsequent to acts of surveillance. As citizens of this country, we are being forced to place our trust in the checks and balances in the executive oversight of executive action directing surveillance.

What options does that leave people whose phones have been infiltrated with the Pegasus malware or whose names appear on the list as potential targets.

They can file a police complaint against an unknown accused for the hacking of their phones . Nevertheless, given the sensitivity of this case, and the lack of any clear statements by the government, it is unlikely that a police investigation will lead to much action. More importantly, however, a criminal investigation will not provide any redress for the harms and mental trauma caused due to the illegal surveillance and, therefore, may not be a satisfactory or adequate remedy. A parliamentary inquiry may also face some impediments. This leaves the judiciary, the protector of our fundamental rights.

> *[A] parliamentary democracy is based on a degree of trust between the citizens and the elected government. The Pegasus scandal has somewhat undermined this trust.*

Our constitutional courts such as the high courts or the Supreme Court can direct the government to produce all the documentation relating to the use of Pegasus on the affected parties. It can establish an independent special investigation team (SIT) to investigate the use of Pegasus on Indian citizens, or it can direct the government to take suitable steps to prevent Pegasus-style malware attacks on Indian citizens in the future.

The edifice of a parliamentary democracy is based on a degree of trust between the citizens and the elected government. The Pegasus scandal has somewhat undermined this trust. Knowledge of the existence of a state surveillance apparatus and advanced spyware such

as Pegasus will modulate human interaction and create a chilling effect, irrespective of its actual use.

At the same time, however, we must use the opportunity to create and maintain public pressure on the government to reform the existing surveillance and intelligence framework and pass an improved data protection law to ensure the privacy of all Indians. These are surely ideas whose time has come.