The Pegasus Hack–II: Secrecy for Snooping in Public Procurement?

CCG NLU, DELHI *on* JULY 30, 2021

7 MINUTE READ

By Gunjan Chawla

The recent revelation of the Pegasus hacks has re-ignited public discourse on privacy, surveillance, and intelligence reform. As the proposed Personal Data Protection Bill, 2019 makes wide exemptions to military, intelligence, and law enforcement agencies for the collection and processing of citizens' data, data protection laws in their current form will be limited in their potential to enforce meaningful procedural safeguards and oversight of State surveillance.

Although these conversations are not new, we must continue to have them. At the same time, it is important not to miss the forest of State-run cyber-surveillance programmes for the sprawling branches of the Pegasus tree. That the global cyber-surveillance industry thrives on State secrecy – is no secret.

While the need for and significance of surveillance reforms cannot be over-emphasised, data protection or privacy law in itself may not succeed in ensuring that the Government is prohibited or restrained from acquiring Pegasus-like spyware. Nor will they ensure that the Government is obligated to disclose that such technologies that risk undermining basic fundamental freedoms of its citizenry have been procured by it, with the intent of deployment by law enforcement and/or intelligence agencies. In an earlier piece about the Pegasus Hack, the Centre for Communication Governance at NLU Delhi (CCG-NLUD) had addressed issues in international frameworks for export controls designed for dual-use technology and their limitations in providing a meaningful remedy to the aggrieved.

In this piece, the author argues that Parliamentary legislation and oversight on public procurement processes, classifications, and procedures is far more likely to address the root of the multi-faceted problems we are faced with, in the wake of Pegasus. Yet, public commentary or critique on the far-reaching consequences of such provisions is hard to come by. This is despite the fact that multiple estimates peg the share of public procurements by Government departments and agencies as accounting for 20-30% of India's national GDP.

The argument proceeds as follows. First, we highlight the central provision that enables the Government to keep such concerning acquisitions of technology in the dark, away from Parliamentary and public scrutiny. Second, we examine the far-reaching implications of this somewhat obscure provision for the cybersecurity industry in India and the public at large. Finally, we explain how this State-sanctioned secrecy in the procurement of spyware – whether from foreign or Indian vendors – could potentially deprive the aggrieved targets of surveillance through Pegasus, of meaningful legal remedy before the courts.

Executive Regulations on Public Procurements and 'National Security'

In the absence of a Parliamentary enactment, public procurements in general, are governed by the overarching principles and procedures codified in the General Financial Rules, 2017 (GFR). These rules were first issued after independence in 1947 and later revised in 1963 and 2005.

Rule 144 of the GFR mandates that every authority procuring goods in public interest shall have the responsibility and accountability to bring efficiency, economy, and transparency in matters relating to public procurement and for fair and equitable treatment of suppliers and promotion of competition in public procurement. It also sets out certain 'yardsticks' with which procuring agencies must conform – and some are more problematic than others.

One of the most significant changes introduced in the 2017 iteration of the GFR, is the introduction of a 'national security exception'. Under these new provisions, Ministries/Departments may be exempted from the requirement of e-procurement and e-publication of tender enquiries and bid awards, which is mandatory as a general rule. This may be permitted:

1. In individual cases where confidentiality is required for reasons of national security, subject to approval by the Secretary of the Ministry/Department

with the concurrence of the concerned Financial Advisor, [Rule 159(ii)] and
2. In individual case[s] where national security and strategic considerations demand confidentiality, after seeking approval of the concerned Secretary and with the concurrence of Financial Advisors [Rule 160(ii)].

This indicates that the 'national security exception' is intended to apply to non-military procurements, expanding the realm of secrecy in procurements far beyond military matters with direct adverse consequences for the civilian realm of affairs. This is supported by the fact that the procurement of goods for the military is excluded from the scope of the GFR by Rule 146. This rule prescribes that the procurement of goods required on mobilisation and/or during the continuance of military operations shall be regulated by special rules and orders issued by the Government from time to time.

Thus, the acquisition of spyware as a product to enhance India's cybersecurity posture—which can easily be proved to implicate strategic considerations that demand confidentiality—could be exempted from mandatory obligations of e-procurement through the central portal and e-publication of the tender enquiry as well as the bid award, after approval from the concerned Secretary and/or Financial Advisors. Although the rule also obliges the Finance Ministry to maintain statistical information on cases where such an exemption is granted, and the value of the contract, whether or not such statistics are amenable to public disclosure through Right to Information (RTI) applications remains unclear at the time of writing.

What are the implications for the Cybersecurity Industry?

In addition to spyware and malware, we can expect that even legitimate cybersecurity products and services, when procured by Government, could also be caught within the above-mentioned clause for exempting an 'individual case where national security and strategic considerations demands confidentiality'.

Given the current state of India's information security, the acquisition of legitimate cybersecurity products and services will and should be conducted across Ministries including but not limited to the Ministry of Defence or even law enforcement.

The demand and market for cybersecurity products and services in the country are burgeoning. These exceptions could also be invoked by the relevant ministry/department to keep the identity of vendors of cybersecurity products and private sector partners for the development of surveillance and other cyber capabilities outside the public domain.

The invocation of such regulatory provisions to keep details of the vendors of cybersecurity products and service providers confidential may create information asymmetries about the Government's needs and preferences among private players in the market. This will not be conducive to creating a competitive market for cybersecurity products and services. These asymmetries can then distort the market with far-reaching implications for the health and growth of the cybersecurity and IT industry at large.

It also militates against the objective of promoting fair competition and transparency in the public procurement process. Adopting the right blend of rules to encourage competition in the industry is crucial to fostering a healthy ecosystem for the cybersecurity industry in India, which is still in its infancy.

Will the courts protect us?

In other words, through the 2017 amendment of the GFRs, the Government of India's executive branch gave to itself–the power to procure goods and services 'in the interest of national security'– while remaining sheltered from the public gaze. This was the first time such a provision was inserted into the GFR – the language of its 2005, 1963, and 1947 iterations make no mention of 'national security' whatsoever.

It is pertinent to point out that the term 'national security' is an extra-constitutional one – it does not occur anywhere in the Constitution of India. Instead, the Constitution refers only to 'security of the State' or 'defence of India', or 'sovereignty and integrity of India'. In recent years, the Executive has co-opted the term 'national security' as a catch-all phrase to encompass everything from serious threats of cross-border terrorism and acts of foreign aggression, to issues like organised protests which were traditionally considered as falling under 'public order' – a category clearly distinguished from 'security of the State' as early as 1966 by the Supreme Court of India in *Ram Manohar Lohia v. State of Bihar* AIR 1966 SC 740.

A more recent order of the Supreme Court dated December 14, 2018, in *Manohar Lal Sharma v. Narendra Damodardas Modi* (The Rafale Case) underlines the Court's reluctance to hold the Executive accountable for procurements and public spending in domains like defence. The Court stated,

> *"We also cannot lose sight of the tender in issue. The tender is not for construction of roads bridges et cetera it is a defence tender for the procurement of aircrafts. The parameters of scrutiny would give far more leeway to the government keeping in mind the nature of the procurement itself." – the Supreme Court order stated.*

Additionally, the emergence of the Supreme Court's "sealed cover" jurisprudence, although recent in its origins –is a testament to the growing shadow of secret executive action pervading the judicial sphere with opacity as well. In this context, it is relevant that recent coverage of the award of the "all-India tender" for the provision of a video conferencing platform for the Supreme Court of India does not yet disclose which entity or corporation was awarded this contract.

Coming back to Pegasus, should the aggrieved persons targeted with this spyware seek judicial remedy, Section 123 of the Indian Evidence Act, 1872 prohibits

Government officials from providing evidence "derived from unpublished official records relating to any affairs of State, **except with the permission of the officer at the head of the department concerned, who shall give or withhold such permission as he thinks fit.**" (emphasis added)

This means that if a case relating to procurements exempted from e-publication is brought before courts, the appropriate authority to give or withhold permission for disclosure to the court would be the same Secretary and Financial Advisors who permitted the procurement to be exempted from publication requirements in the first place. Section 124 further prohibits compelled disclosure of official communications made to a Government official in confidence.

And thus, the conspiracy of silence on potentially criminal acts of Government officials could easily escape judicial scrutiny. This will invariably create a challenging situation for individuals impacted by the use of the Pegasus spyware to effectively seek judicial redressal for violation of their right to privacy and hold the government accountable.

Without an explicit acknowledgment from the Government of the fact that the spyware was in fact procured by it – questions on the legality of procedures that resulted in its targeted deployment against citizens and judicial remedies for violations of due process in the criminal investigation remains a moot point. In their current form, the applicable rules permit the Government to enable secret procurement of goods and services for non-military purposes under the GFR's 'national security exception', and also permits the Government to disallow disclosure of this information in judicial proceedings.

Given the lower level of judicial scrutiny that such procurements will likely be subjected to, the doctrine of checks and balances and the doctrine of separation of powers necessitates that appropriate parliamentary mechanisms be set up to ensure effective oversight over all government procurements. Presently, the legal framework for procurements is comprised almost exclusively of executive-issued regulations. Constitutionalism requires that no organ of government should be

granted or allowed to exercise unfettered discretion and is always held accountable by the other organs of the government.

This is an essential element of the Rule of Law and can only be ensured by way of a Parliamentary enactment on procurement procedures and concomitant disclosure requirements as well as effective Parliamentary oversight mechanisms to enforce accountability on public spending incurred for procurements in the name of national security.

*

This article was first published on CCG-NLUD's blog. It has been cross-posted with the author's permission.

More reading on Pegasus

- A decade-old Bill had proposed to regulate surveillance by govt agencies; this is what it said
- A Guide To The NSO Group's Pegasus Spyware In India
- Members Of Parliament React To Pegasus Spyware Controversy Amidst Monsoon Session
- 'Illegal And Deplorable': How Pegasus Spyware Targets In India Are Reacting
- Amazon Web Services shuts down infrastructure linked to Pegasus vendor NSO Group
- Pegasus spyware: How do we rein in State surveillance? Here's what experts had to say

- Sign up for our Daily Newsletter to receive regular updates
- Stay informed about MediaNama events
- Have something to tell us? Leave an Anonymous Tip
- Ask us to File an RTI
- Sponsor a MediaNama Event

DISCOVER MORE

pegasus | pegasus project issue india 2021 | personal data protection bill 2019 | surveillance

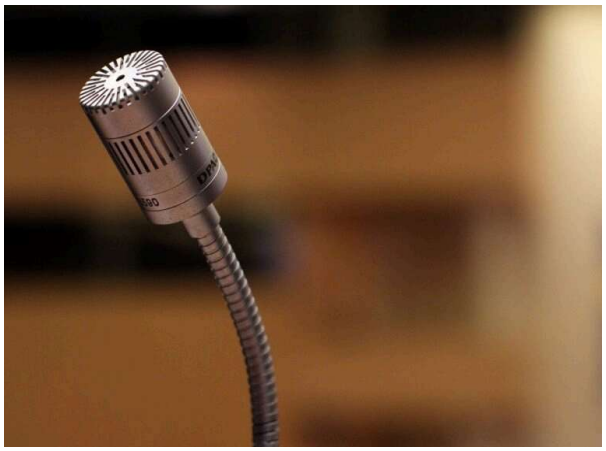
Related Posts:

Pegasus spyware: How do we rein in State surveillance? Here's what experts had to say

Everything that the NSO Group has said so far on the allegations against Pegasus

Congress MP moves adjournment motion in Parliament to discuss Pegasus spyware and Indian govt's alleged role in it

NSO Group's Pegasus used to hack phones of US State Department officials: Report



What a former UN Special Rapporteur told the expert committee investigating Pegasus in India

West Bengal's Commission of Inquiry on Pegasus seeks information from public, lists submission requirements

MEDIANAMA

MediaNama is the premier source of information and analysis on Technology Policy in India. More about MediaNama, and contact information, here.