Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG POLICY BRIEF

Pegasus, Privacy and National Security

Authors

D S Hooda
Abhimanyu Ghosh

Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.
nso GROUP
PEGASUS

Volume VI, Issue 29

AUGUST 18, 2021

Delhi Policy Group
Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org

Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG Policy Brief Vol. VI, Issue 29
August 18, 2021

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Authors

Lt. Gen. Deependra Singh Hooda (Retd.), PVSM, UYSM, AVSM, VSM & Bar, Senior Fellow for Military Strategy, Delhi Policy Group
Brig. Abhimanyu Ghosh (Retd.), Senior Fellow for Cyber Security and Digital Technologies, Delhi Policy Group

The views expressed in this publication are those of the authors and should not be attributed to the Delhi Policy Group as an Institution.

Cover Photograph:

Source: The Print

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org

Pegasus, Privacy and National Security

By

D S Hooda and Abhimanyu Ghosh

Contents

Pegasus, Privacy and National Security

by

D S Hooda and Abhimanyu Ghosh

Introduction

A huge storm has broken out over the leaked database of names and numbers, purportedly targeted by the surveillance tool Pegasus sold by the Israeli company NSO. On August 5, a Bench of the Chief Justice of India N.V. Ramana and Justice Surya Kant observed that the allegations of the government using Israel-based technology to spy on civilians, journalists, ministers, parliamentarians, and activists were "no doubt serious", provided the news reports were true.[1]

While the issue is sub judice, it has raised questions regarding the possible misuse of this military-grade software sold with the express approval of the Israeli Defence Ministry. Concerns have also been expressed due to the potential abuse of surveillance tools for ulterior political motives that violate privacy and human rights.

This paper argues that while the empowerment of intelligence and security agencies to fight criminals and terrorists is the sovereign duty of any nation, cyber tools, like any other military weapon system, should be regulated to prevent their abuse and collateral damage to civil society. The debate on privacy vs. national security also needs to move beyond binaries. In contrast to what is the common perception, strengthening individual privacy could in fact help improve national security. Global norms need to be deliberated and adopted by the international community, duly harmonised with national laws.

The Genesis of the Controversy

On July 18, Forbidden Stories, a Paris-based non-profit media organisation, and Amnesty International, revealed a list of phone numbers of journalists, activists, and political leaders allegedly targeted by the Pegasus tool. The investigation was named the 'Pegasus Project' by a consortium of 80 journalists from 17 media outlets in 10 countries, including The Wire, The Guardian, and The Washington Post. The leaked database of 50,000 names with 300 numbers in India included the mobile phone numbers of at least 65 business executives, 85 human rights activists, 189 journalists, and several diplomats, military chiefs, and senior politicians from 34 countries — including the French President, Emmanuel Macron, the South African President, Cyril Ramaphosa, and the Pakistani Prime Minister, Imran Khan.[2]

A diplomatic and political row erupted in several countries including India, France, Hungary, South Africa, Rwanda, and Morocco. France has instituted a series of investigations to be carried out into the use of the Pegasus spyware that allegedly originated in Morocco. Israel has set up a senior inter-ministerial Task Force led by its National Security Council to investigate the allegations that the spyware has been abused on a global scale. On July 29, it was learnt that Israeli investigators had raided the office of the NSO Group.[3]

There are also counter-claims. Morocco has denied spying on any foreign leaders and has filed defamation claims against Amnesty International and Forbidden Stories.[4] Rwanda has categorically denied that it targeted the South African President's phone and claimed that it does not possess the technical capacity to carry out espionage on such a scale.[5] Neither India nor Pakistan have explicitly commented on claims that Delhi may have selected Imran Khan for surveillance.

In an interview, the CEO of NSO, Shalev Hulio, said, "We don't have and have never had any ties to the list that was published." NSO maintains that it sells its technologies solely to law enforcement and intelligence agencies of "vetted governments" for "preventing criminal and terror acts." Hulio observed that the "Israeli cyber sector is under attack" and "forming a consortium like this of journalists from all over the world and bringing Amnesty [International] into it – it looks like there's a guiding hand behind it."[6]

The Indian government has denied any allegations of snooping on citizens. It has repeatedly stated that India has an established protocol for the lawful interception of electronic communication as per relevant rules under Section 5(2) of Indian Telegraph Act, 1885 and Section 69 of the Information Technology (IT) Act, 2000. However, the government has not commented on whether or not it had purchased or used Pegasus spyware in India. An Indian Express calculation worked out the initial expenditure for Indian targets to be well over Rs 56 crore.[7] Therefore, it may be inferred that surveillance at the scale reported can only be undertaken by State agencies or another nation.

Technology Behind the Tool

Reported abuse of the global telephone system for tracking and monitoring is not something new, but it is difficult to investigate. When a device is tracked or messages are intercepted, there may not be traces on the target's device for investigators to find. The Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, has revealed that the Pegasus spyware exploits weaknesses in the global mobile phone system to snoop on calls, texts, and the location of phones. NSO customers can purchase a system that they connect to their local telecommunications companies' infrastructure or use a cloud that interconnects with telecommunications companies worldwide.[8]

As part of the 'Pegasus Project,' Amnesty International conducted a forensic analysis of only 67 phones out of 50,000 suspected targets. Of the 67 phones analysed, 23 showed signs of a successful Pegasus infection, and 14 showed signs of an attempted infection. The 23 infected phones were all iPhones. Of the phones that showed attempted infections, 11 were iPhones, and 3 were

Android phones. The duopoly of Apple-Android operating systems for these smartphones adds to the vulnerabilities. Amnesty believes that Pegasus operators used either a rogue cell tower or set up equipment at the site of the mobile operator to perform network injection to disguise its malicious data requests as legitimate ones. Pegasus also exploited the Apple messaging service iMessage to perpetuate zero-click attacks through Apple iCloud online data storage accounts made with Gmail and Microsoft Outlook email addresses.[9]

Privacy and National Security

The Pegasus affair raises several issues related to the ongoing debate concerning privacy vs. national security. It is a well-accepted norm that governments can intercept electronic communications to prevent or detect crimes and stave off threats to national security. When the Central Monitoring System was rolled out in India in 2013, an official directly involved in setting up the project said, "You can see terrorists getting caught, you see crimes being stopped. You need surveillance. This is to protect you and your country."[10]

Under the provisions of the Indian Telegraph Act and the IT Act, 2000, the government, under certain circumstances, is permitted to conduct surveillance of suspicious individuals. This is done after approval from the competent authority, usually the Union Home Secretary. In this digital age, with Artificial Intelligence and end-to-end encryption, it is incumbent on political and security executives to deploy technologies to understand threats and to address challenges.

On the other hand, the Supreme Court of India, on August 24, 2017, declared the right to privacy as a fundamental right protected under the Indian Constitution. This ruling puts greater scrutiny on the government's actions with regard to monitoring personal data and information. State agencies must generate trust among the civil society that technologies are not misused for unrestricted or mass surveillance with a political agenda.

There is a delicate balance to be achieved between privacy and national security. While these two are often seen as competing requirements, this is not necessarily always the case. It is essential to understand that the strengthening of individual privacy can also improve national security. Unfettered collection of personal data can reveal crucial information regarding attitudes, feelings, ideology, and beliefs of large sections of society. In the hands of an adversary, such information can be exploited for influencing mass behaviour and creating social disharmony. This is just one example of how weak privacy can hurt national interests.

A recent report by the Internet Freedom Foundation found that BSNL could be collecting and selling user data without the user's consent.[11] The fact that more than 50 percent of mobile network equipment used by BSNL comes from two Chinese companies, Huawei and ZTE,[12] who could be secretly accessing this data, is highly worrisome. This problem is not restricted to BSNL. In the absence of a data protection law, there is no restriction on who can collect what type of data.

Without the checks and balances of a legal framework, the security of personal data also remains lax. The World Economic Forum's Global Risks Report 2019 states that the largest data breach of 2018 occurred in India, where the "government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens."[13] More recently, Air India announced that data of 4.5 million passengers had been compromised. The stolen data included passengers 'names, date of birth, contact information, credit card details, passport information, Star Alliance and Air India frequent flyer data, and ticket information.[14] Such data is often sold to the highest bidder, posing a threat to national security.

Snooping on foreign governments has acquired a degree of legitimacy, though it is carried out clandestinely. The Snowden revelations exposed the massive scale of global surveillance conducted by the U.S. and the 'Five Eyes' intelligence alliance that also includes Australia, Canada, New Zealand and the United Kingdom. India also has a right to do what the other nations are doing. The danger arises when foreign tools are used for this purpose.

If Indian agencies are indeed using the Pegasus software, there is no guarantee that the information obtained will not be transferred to another entity. All companies are legally answerable to their parent country on matters of national security and cannot refuse their government's requests. Moreover, suspicions have existed that the Israeli government also views some information that the NSO collects.[15]

In March 2018, the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act, or "CLOUD Act." The CLOUD Act makes explicit that "a company subject to a country's jurisdiction can be required to produce data the company controls, regardless of where it is stored at any point in time."[16] China's National Intelligence Law of 2017 states that "any organisation or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law."[17]

As stated earlier, the privacy vs. national security debate cannot be viewed in black and white terms. Weak individual privacy provides opportunities to other nations to gather critical data that could be used to target our national interests. The problem is compounded if foreign companies are employed to collect crucial data. Not only is there the likelihood of this data being transferred abroad, but the government could also become vulnerable to pressure from foreign actors.

Finally, national efforts will need to be supplemented by global regulation. Research by the Citizen Lab has demonstrated that the surveillance industry is poorly regulated, and its products are prone to abuse.[18] The "self-regulation" that companies claim to practice does not seem to have stemmed the growing tide of abuse cases.

In a 2019 report on the surveillance industry to the United Nations Human Rights Council, the U.N. Special Rapporteur stated that "the private surveillance industry has thrived with low levels of transparency and public scrutiny and weak controls on transfers of technology." He called for "an immediate moratorium on the global sale and transfer of private surveillance technology until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-state actors use the tools in legitimate ways."[19]

It may be impractical to hope for a moratorium on the sale and transfer of surveillance technology. Still, an attempt could be made to lay down stricter rules for the sale of surveillance technology. The United Nations could take the lead in drafting the norms for acceptance by member states.

Recommendations

The Pegasus case is sub judice in India. Without going into the specifics of the case, it is established beyond doubt that surveillance technology needs to be regulated both nationally and globally. Norms need to be framed, not just for cell phone snooping but also for unethical surveillance by facial recognition and the use of biometrics. The following recommendations can be made in this regard:

- National laws need to be reinforced to limit surveillance, create institutional mechanisms for oversight of surveillance technologies, and for redressal of grievances.
- In India, due authorisation is seemingly in place under the IT Act with the provisions of executive oversight. However, any misuse of such authorisation should be investigated, and a framework for safeguards against abuse instituted.
- To prevent accusations of political misuse, there must be legal consent for agencies to access individual data. The approval for accessing electronic and phone data of suspects should be shifted from government officials to the courts. A Bill to provide parliamentary oversight over intelligence agencies should be debated in a bipartisan manner in the interests of national security.
- In the interest of privacy and security, a strong Personal Data Protection Bill needs to be legislated soon. Some reservations are already being expressed about the provisions of the draft bill being diluted by keeping numerous state agencies outside the ambit of the bill.[20] As has been pointed out, any weakening of personal data protection could have adverse implications.

- The United Nations should create a working group to draft the rules regulating the sale of surveillance technology. An attempt should thereafter be made to bring member states on board.

Conclusion

The Pegasus controversy brings home the point that national security and privacy should be balanced by proper regulations for oversight and transparency. It is the government's sovereign duty to empower security agencies with technologies to fight criminals, terrorists, and geopolitical adversaries. However, unchecked collection of personal data and its poor handling could jeopardise security. In India, the Personal Data Protection Bill should be enacted to generate trust that privacy will be respected and the violators of privacy laws will be punished.

Most importantly, India needs to develop indigenous capabilities so that foreign applications are not employed unhindered to harvest the data of Indian citizens, which is then transported across the border for creating repositories of state and commercial intelligence. National security is of prime importance and should be supported by indigenous technologies with adequate safeguards to protect the privacy and human rights of Indian citizens, as enshrined in the Indian Constitution.

***

[1] Rajagopal, Krishnadas. "Allegations Serious, Truth Has to Come out in Snooping Issue: Supreme Court." The Hindu. August 5, 2021, sec. National. https://www.thehindu.com/news/national/pegasus-allegations-serious-truth-has-to-come-out-in-snooping-issue-supreme-court/article35738465.ece.

[2] Washington Post. "Takeaways from the Pegasus Project," July 18, 2021. https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

[3] Williams, Dan. "Israel Appoints Task Force to Assess NSO Spyware Allegations - Sources." Reuters, July 21, 2021, sec. Technology. https://www.reuters.com/technology/israels-national-security-council-looking-into-nso-spyware-allegations-2021-07-21/.

[4] NDTV.com. "Morocco Files Defamation Suit Against Amnesty, French NGO Over Pegasus." Accessed August 12, 2021. https://www.ndtv.com/world-news/morocco-files-defamation-suit-against-amnesty-french-ngo-over-pegasus-2492690.

[5] Smith, Elliot. "Israeli Pegasus Spyware Saga Could Sow Diplomatic Rifts in Africa." CNBC, July 27, 2021. https://www.cnbc.com/2021/07/27/the-pegasus-spyware-saga-could-sow-diplomatic-rifts-in-africa-.html.

[6] www.israelhayom.com. "' Israeli Cyber Sector Is under Attack,' Says NSO Group Chief," July 23, 2021. https://www.israelhayom.com/2021/07/23/israeli-cyber-sector-is-under-attack-says-nso-group-chief/.

[7] https://indianexpress.com/article/india/project-pegasus-cost-of-putting-pegasus-in-phones-runs-into-crores-7414323/

[8] The Citizen Lab. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," December 1, 2020. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

[9]" Forensic Methodology Report: How to Catch NSO Group's Pegasus." Accessed August 12, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

[10] Kotoky, Anurag. "India Quietly Expands Surveillance System to Tap Phone Calls, Email." mint, June 20, 2013. https://www.livemint.com/Politics/J1jxvQ5Su9Su4pGLHDCepM/India-sets-up-new-surveillance-system-to-tap-phone-calls-em.html.

[11] Internet Freedom Foundation. "BSNL Is Injecting Code on to Your Browsers, and Here's What It Does. #SaveTheInternet," August 9, 2021. https://internetfreedom.in/taking-a-closer-look-at-bsnls-code-injections-savetheinternet-2/.

[12] The Indian Express. "Over 50% Equipment in BSNL Mobile Networks Chinese: Govt," September 18, 2020. https://indianexpress.com/article/business/over-50-equipment-in-bsnl-mobile-networks-chinese-govt-6600371/.

[13] World Economic Forum. "The Global Risks Report 2019." Accessed August 12, 2021. https://www.weforum.org/reports/the-global-risks-report-2019/.

[14]" Five Biggest Data Breaches That Hit India In 2021 - Jump Start Magazine." Accessed August 12, 2021. https://www.jumpstartmag.com/five-biggest-data-breaches-that-hit-india-in-2021/.

[15] Harris, Shane. "U.S. and E.U. Security Officials Wary of NSO Links to Israeli Intelligence." Washington Post, July 20, 2021. https://www.washingtonpost.com/national-security/2021/07/20/nso-israel-intelligence/.

[16]" The Purpose and Impact of the CLOUD Act." https://www.justice.gov/opa/press-release/file/1153446/download

[17] Kharpal, Arjun. "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice." CNBC, March 5, 2019. https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[18] The Citizen Lab. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles."

[19]" OHCHR | The Special Rapporteur's 2019 Report to the United Nations Human Rights Council." Accessed August 13, 2021. https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx.

[20] https://www.outlookindia.com/. "India Needs A Strong Personal Data Protection Bill Now: Justice (Retd) B.N. Srikrishna." Accessed August 13, 2021. https://www.outlookindia.com/website/story/india-news-there-is-no-doubt-that-pegasus-was-intended-to-be-sold-only-to-governments-justice-retd-bn-srikrishna/388921.

DPG

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org