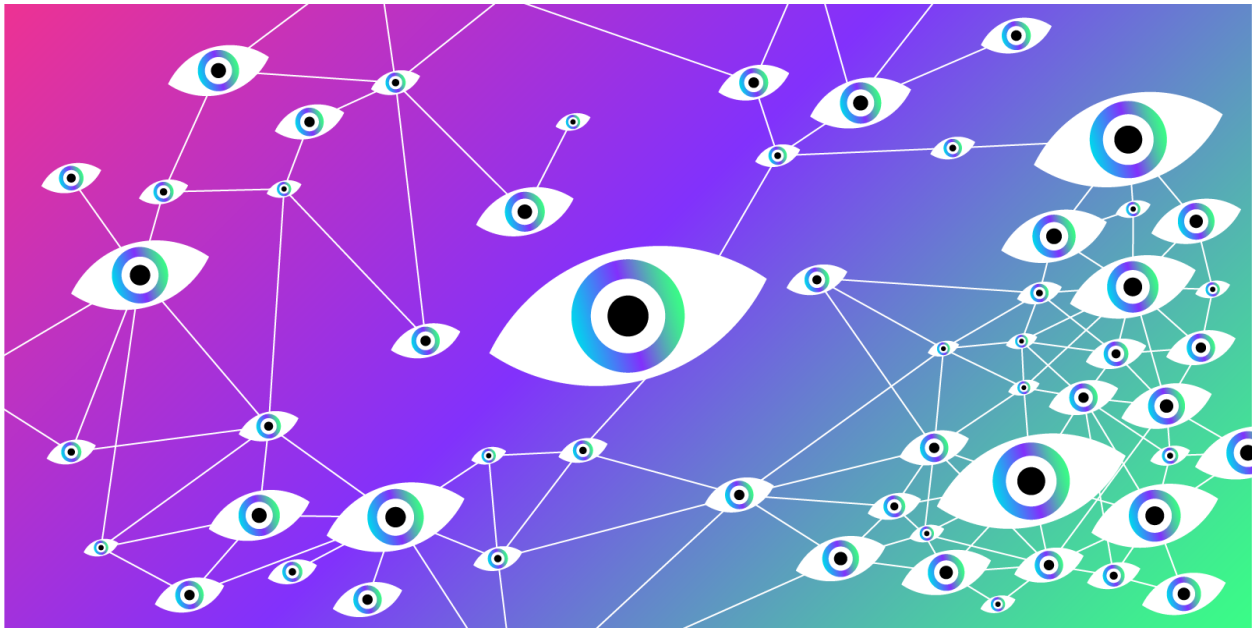

Policy explainer brief: the Pegasus Project revelations in India

Implications and necessary next steps

Introduction

In light of the global exposé by the Pegasus Project regarding the NSO Group's hacking software "Pegasus", and in anticipation of the hearing on this subject called by the parliamentary committee on information technology on July 28, 2021, this brief aims to serve as a ready-reckoner on the Pegasus Project; the issues that need to be raised in Parliament; and the necessary steps that need to be taken to protect fundamental rights.

*This brief is divided into five sections. The **first section** provides a brief overview of the Pegasus Project and its revelations. The **second section** explains how Pegasus spyware works and why its use is a cause for alarm for rights and democracy in India. The **third and fourth sections** focus on next steps including the need for surveillance reform; a list of suggested questions that need to be answered in Parliament; and summary recommendations with respect to immediate measures. Annexure I contains a list of additional references; and Annexure II has a flowchart explaining how Pegasus is installed and the data it can harvest.*

The Pegasus Project and its revelations regarding India

The Pegasus Project is a journalistic investigation into the Israeli surveillance company NSO Group and its clients by a consortium of international media organisations. According to NSO Group, its clients are states and state agencies.

The leaked database contains 50,000 numbers, including more than 300 Indian numbers, believed to be potential targets listed by NSO Group's clients. Out of a sample of 67 phones examined by Amnesty International globally, forensic analysis showed traces of Pegasus activity in 37 phones. Of these 37 infected phones, 10 are Indian, which indicates that at least 10 Indian numbers were targeted with Pegasus.

The more than 300 Indian numbers in the database include those used by ministers, opposition leaders, journalists, the legal community including a sitting Supreme Court judge, businesspersons, government officials, scientists, rights activists, and others. The background of these potential and proven targets in India suggests that they, in all likelihood, have no link with any "national security" investigation, which is the purpose the government most commonly and indiscriminately cites to justify surveillance. In a report by The Indian Express, a fortnight before the Pegasus Project was made public, the NSO Group had itself acknowledged the human rights risks and potential misuse of its spyware by states and state agencies for reasons unrelated to national security or law enforcement.

How Pegasus works and why it is a cause for alarm

Pegasus is essentially a hacking software, or spyware, available for hire. There are two more widely known methods through which Android or iOS devices can be infected with it:

(a) method requiring interaction with the owner: emails or text messages, often tailored for the specific target, to trick the target into clicking on a malicious link. This is called "spear-phishing" - which was used by the earlier version of Pegasus in 2016 and following years; and

(b) method requiring no interaction with the owner: this often includes exploitation of "zero day" software vulnerabilities, i.e., flaws in the operating system or connected apps that the device's manufacturer or software developer is not aware of. The device user need not perform any action or click on any link for Pegasus to be installed. For example, it could be installed simply by placing a call on the target device, even if the call is not answered. These are called "zero-click" attacks - i.e. the attacks were made without any explicit sign to (such as a missed call) or act required (such as clicking a malicious, disguised link - sometimes called "spear phishing'') of the targeted individual.

The spyware can access on the device everything that the owner of the device can. The personal and sensitive data that it can copy and harvest includes emails, text messages, contact books, location data, photos, and videos. The phone's microphone and camera can be activated to covertly record the user. (*See the Pegasus Project flowchart in Annexure II.*)

Amid all the revelations and denials surrounding the Pegasus Project, the forensic analysis conducted by Amnesty International's Security Lab on a number of smartphones confirming infection by Pegasus, and NSO Group's claim that its clients are **only states and state agencies**, suggest that **at least one, if**

not more, of these statements must be true, and that in itself is cause for concern and reflects a need for urgent action:

> (a) Indian government agencies are using private surveillance technology to secretly gain access to sensitive data on people's personal devices, purportedly in exercise of authority under existing surveillance laws that in fact do not permit hacking, which is what Pegasus spyware does;
>
> (b) The Indian government is employing such hacking mechanisms for surveillance covertly and illegally without any grounding in law; or
>
> (c) People in India are being spied on by foreign governments who are NSO's clients and there is an absence of a transparent, effective, and independent investigation by Indian authorities.

Each of these scenarios severely undermines privacy and free speech, and represents an urgent need for surveillance reform.

Concerns are aggravated by the fact that, as the Press Club of India noted "This is the first time in the history of this country that all pillars of our democracy — judiciary, parliamentarians, media, executives and ministers — have been spied upon".

The threat that Pegasus, or any other deeply invasive surveillance tools, potentially pose to fundamental rights and democracy is, to put it mildly, alarming and debilitating. Unauthorized or covert access that does not comply with strict standards of legality, necessity and proportionality, to even one of the categories of sensitive personal information mentioned above is damaging and should be impermissible. When pieced together, the fragments of information can give the attacker a full and detailed picture of the target's life, including its most personal details and those of everyone the target interacts with. This severely jeopardizes the rights to privacy and free speech, protected by the Indian Constitution, and forming the foundations of India's democracy.

Surveillance reform

The government's response to the Pegasus Project, while failing to directly answer whether the government has any links with NSO, emphasises that surveillance in India takes place for national security purposes under established laws that have adequate safeguards. **This is not true**.

India's surveillance regime under the Indian Telegraph Act and the Information Technology Act lacks sufficient checks and balances. It enables centralization of powers in the hands of the Executive in a completely opaque manner devoid of independent oversight and accountability. Further, there is ineffective implementation of even the limited safeguards that are provided. Hacking, which is what Pegasus enables, is illegal under the Information Technology Act, without exceptions for the government.

There ought to be independent judicial oversight over the government's surveillance powers, as is necessary in other major democracies. Additionally, the scope and implementation of such powers must undergo periodic parliamentary scrutiny, and be limited through narrowly defined circumstances and stringent disclosure requirements. Without such checks and balances to ensure

accountability, limitless surveillance and unwarranted invasion of privacy for broadly stated and unverifiable purposes cannot be contained. Laws need to be reformed to ensure that surveillance is only authorized in accordance with strict standards of legality, necessity, and proportionality recognized by the Indian Supreme Court. There is also an urgent need to establish a transparent grievance redressal mechanism, independent of the Executive, and judicial remedy that individuals who have been subjected to surveillance may avail of.

Further, the incoming Personal Data Protection law grants ample discretionary powers to the government without the necessary limitations, and cannot be meaningfully cited as a step towards surveillance reform. The current draft does not sufficiently protect citizens' privacy against surveillance and must be amended.

Questions that need to be raised by policymakers

1. **Does the Government of India, any state government, any government agency, or any Indian security service have any dealings with the NSO group? Have there been any such dealings in the past?**
2. **Has the government or any of its agencies otherwise used, or licensed the use of, Pegasus spyware for any purpose?**
3. **What action is the government taking to respond to the revelations made by the Pegasus Project to ensure that the fundamental right to privacy is protected?**
4. **Will a transparent, independent, and effective inquiry be established to look into the dangerous surveillance practices that have come to light through the Pegasus Project?**
5. **What is the policy of the Union Government regarding government hacking? How do the existing provisions on hacking under the IT Act apply to government agencies, police, and any private parties they may use to access digital records or digital communications?**
6. **What is the policy of the Union Government regarding government hacking? How do the existing provisions on hacking under the IT Act apply to government agencies, police, and any private parties they may use to access digital records or digital communications?**
7. **When, and in what manner, will the surveillance regime in India, including provisions in the Indian Telegraph Act and the Information Technology Act, be reformed to protect against invasion of privacy by unwarranted surveillance devoid of judicial oversight and remedy?**

8. **How will the Personal Data Protection Bill be modified to ensure that adequate safeguards are in place against secret surveillance as well as the government's discretionary powers to demand access to personal data?**

9. **What laws apply to surveillance technology/hacking-for-hire firms that operate in India? Does the government have a record of the firms operating in India?**

Summary recommendations

1. **Lawmakers must urgently establish an independent inquiry into the government's possible use of Pegasus, or any other secret surveillance tool;**

2. **In accordance with calls by international human rights groups, including the Office of the United Nations High Commissioner for Human Rights, Parliament must insist on an "immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place;"**

3. **Parliament should prioritize the need for surveillance reform to preserve and protect the fundamental right to privacy as recognised by the Supreme Court and in accordance with international human rights principles;**

4. **Parliament must scrutinise the Personal Data Protection Bill and seek modifications that meaningfully limit the government's discretionary powers and protect data privacy without broad exceptions;**

5. **The government must support independent investigations by authorities across India, as well as ongoing initiatives by committees of Parliament, and enable them to function effectively and without obstruction; and**

6. **Individuals who may have been impacted by Pegasus should be provided judicial remedy and a meaningful opportunity to be heard in any investigations. Independent investigations by parliament and inquiry commissions should be made available for public scrutiny.**

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact:
Raman Jit Singh Chima | Asia Pacific Policy Director | raman@accessnow.org