24th July, 2021

NEWS JUICE

Intelligent Compilation from The Hindu, Indian Express & others along with News Background

NEWS HEADLINES

1. Infiltrated by Pegasus: Is your iPhone...

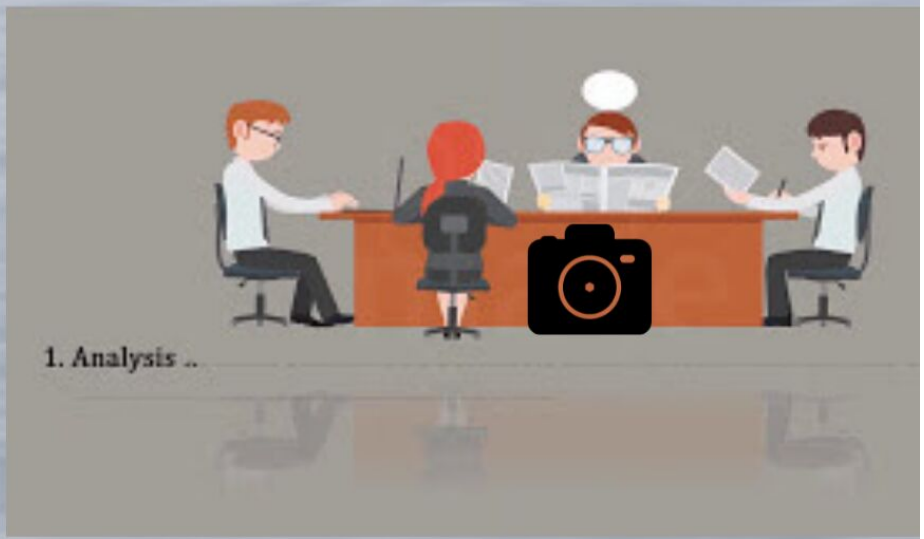
2.LIC's IPO and its customers

3. Azithromycin, out of favour as Covid-19 therapy

4. The laws for surveillance in India, and the concerns over privacy

What is News Juice?

BY PREPMATE



1. Infiltrated by Pegasus: Is your iPhone becoming less secure?

Relevant for GS Prelims & Mains Paper III; Science & Technology

With the revelations of the Pegasus Project investigation has come the realisation that for all of Apple's claims regarding the security of its phones, the iPhone is vulnerable to undetected infiltration.

How has Apple been targeted?
Forensic evidence suggests the Pegasus spyware developed by Israel's NSO Group used 'zero-click' attacks executed via Apple's iMessage and FaceTime communications apps, the Apple Music streaming service, and Safari web pages to infiltrate the iPhones of journalists and activists.

Once in, Pegasus gains full access to the targeted iPhone or Android smartphone's data, location, text messages, and contact lists, along with stored audio, video, and photo files. In effect, it gains, as a security expert put it, "often more control than the owner of the phone". Over the past few years, important people, and people who worry about the security of their devices, have moved to iPhones, especially since BlackBerry and Windows phones have faded into oblivion. So an attack targeting phones used by politicians, business leaders, and journalists will have a higher proportion of Apple devices.

How has Apple responded?
In a statement condemning the attacks, Ivan Krstic, head of Apple Security Engineering and Architecture, said: "Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."

How vulnerable (or not) are iPhones?
Independent security researcher Anand Venkatanarayanan said that Apple's claims about security enhancements notwithstanding, "there exist lots of smaller vulnerabilities". This, he said, makes it "easier for NSO to either procure or develop exploits on their own", which can sell for millions of dollars.

"NSO Group is a military-grade weapons manufacturer and just like any arms maker, they have to guarantee their customers that whatever they supply is going to work everywhere. And Android and iOS are the only two big markets out there," Venkatanarayanan said.

According to Venkatanarayanan, multiple zero-day vulnerabilities have been found on iMessage over the last year and a half. With iOS 14, Apple tried to secure iMessage with BlastDoor, a sandbox technology designed to protect only the messaging system. It

processes all incoming iMessage traffic and only passes on safe data to the operating system.

But as Amnesty International's forensic analyses of iPhones infected with the Pegasus spyware showed, the NSO Group's 'zero-click' attacks managed to bypass this. 'Zero-click' attacks do not require any interaction from the target, and according to Amnesty, they were observed on a fully patched iPhone 12 running iOS 14.6 until as recently as July 2021.

No device can claim to be 100 per cent secure, said ethical hacker and cybersecurity expert Nikhil S Mahadeshwar. "Every security has its own backdoor and even if the backdoor is private, there is a new methodology and a new technology to break that backdoor." Why, for example, does Apple have a bug bounty programme when it claims its iPhones are "unhackable", Mahadeshwar asked.

"There are two major ways through which the iPhone can be hacked — by jailbreaking, or via third party unauthorised iCloud backup, through which you can get to the user's iMessages, WhatsApp chats, and contacts," he said.

Apple sources said the company views security as a process — as part of which it quickly addresses critical vulnerabilities and provides security updates to users even on older devices. The sources said Apple had pioneered new protections like Pointer Authentication Codes and BlastDoor, and was working to improve these features to respond to new threats.

How does Apple stack up against Android?

Both operating systems are equally vulnerable — or secure. However, only iPhones keep the data logs that makes it possible to carry out the analysis that is needed to detect possible spyware infection. It is not easy to detect Pegasus on Android, given the logs tend to get deleted after a year or so.

Pranesh Prakash, Affiliated Fellow at the Information Society Project at Yale Law School, said both iOS and Android are "vulnerable to various security exploits, and have robust programmes to counter these kinds of security vulnerabilities". Spyware like "Pegasus have to keep evolving to different forms of security measures that Android and iOS take," he said.

Why are such attacks becoming frequent? (Earlier instances of surveillance involving Pegasus were reported a couple of years ago.)

Venkatanarayanan said the nature of the smartphone market, dominated by two operating systems — iOS and Android — make it easier for companies like NSO Group to carry out attacks. "If you find one vulnerability, you can hit a major chunk of users. The scale of this monopoly — or duopoly — is such that there's not much variability. Variability makes cyber offence operations harder," he said.

What can Apple do now?
Apple's reputation as a safe and secure device has been dented by the Pegasus revelations. Apple has since highlighted how its security team has grown by about four times in the last five years, and now comprises many top experts from threat intelligence specialists and offensive security researchers to platform defence engineers and "everything in between".
Tim Bajarin, tech analyst and chairman of Creative Strategies, said in an email: "…Apple needs to deal with this ASAP and serve as the example of correcting this exploit of their OS. Apple has weathered other security breaches in the past, and if they deal with it quickly and make sure this threat has been eliminated, they will regain their customers' views of Apple's security focus."

Source: The Indian Express

2. LIC's IPO and its customers

Relevant for GS Prelims & Mains Paper III; Economics

As investors wait for the mega public offer of Life Insurance Corporation later this year, LIC policyholders who have bought over 28.9 crore policies, too, have now got reason to be enthused. The government has said that up to 10% of the issue size in the IPO would be reserved for LIC policyholders. There could be a discount on the floor price.

What are the LIC rules on such reservation?
The LIC (Amendment) Rules, 2021 say that any reservation made by the Corporation in favour of its policyholders on a competitive basis in a public issue under Clause (a) of sub-section (9) of Section 5 should be made in a manner similar to that applicable to a reservation on a competitive basis for employees in a public issue under any regulation made and circular issued by the Securities and Exchange Board of India.

The allotment of equity shares to life insurance policyholders against any reservation made in their favour should be made in consultation with the stock exchanges concerned.

According to IPO norms, an issuer company can offer the shares to employees at a discount of a maximum 10% on the floor price at which the shares are offered to other categories.

LIC IPO: What's the status of the listing plan?
The Union Cabinet recently approved the disinvestment of equity in LIC. The process is on to appoint merchant bankers to launch the IPO. A panel headed by Finance Minister Nirmala Sitharaman will decide on the size of the share sale. The government has amended the LIC Act of 1956 for the proposed IPO. The LIC has appointed Arijit Basu, former MD of State Bank of India and former MD & CEO of SBI Life, who had led the move to get LIC listed on stock exchanges, as a consultant to help launch the IPO.

After the amendment, like any other listed company, the corporation, now governed by the Companies Act and SEBI Act (post-IPO), has to prepare its quarterly balance sheet with profit or loss figures and make public key developments. Budget amendments to the LIC Act have been notified and the actuarial firm will work out the embedded value of the insurer in the next couple of weeks.

How will policyholders benefit?

If the government offers a 10% discount to policyholders, then, by a conservative estimate, the post-issue market capitalisation is likely to be around Rs 10 lakh crore, and can go up to Rs 15 lakh crore once the embedded valuation is known. As per the new SEBI rule, on a Rs 10 lakh crore market capitalisation yardstick, LIC will have to make an issue of Rs 55,000 crore (Rs 10,000 crore plus 5% of Rs 9 lakh crore). If the market capitalisation is Rs 15 lakh crore, the IPO size would become Rs 80,000 crore.

While it may appear that LIC policyholders would get a lower bonus after the IPO than they are getting now, sources said it may not happen that way: The LIC will find new ways to continue offering the same bonus.

Pricing of the issue will be key, especially given the past experience with public issues of two general insurance companies — General Insurance Corporation of India Ltd and New India Assurance Co Ltd — that got listed in 2017. New India Assurance shares, initially offered in the range Rs 770-800, are now quoting at Rs 161, while the price of General Insurance Corporation shares have fallen from Rs 912 to Rs 174.60.

However, both companies issued one bonus share for every share held between June and July 2018. That means that if an investor had one share of GIC at Rs 912, he/she would be holding two shares worth Rs 174.60 each. That would still mean a loss of over 60% of his/her investment in the IPO.

Why is the LIC IPO important for the government?

The listing will be crucial for the government to meet its disinvestment target, especially when its plans to privatise two public sector banks and one insurance firm have not taken off yet. The government aims to mop up Rs 1.75 lakh crore in the current fiscal from minority stake sale and privatisation. Of this, Rs 1 lakh crore was to come from selling its stake in public sector banks and financial institutions, and Rs 75,000 crore as CPSE disinvestment receipts. The LIC IPO is expected to meet the shortfall in that target.

Why should investors look forward to it?

In LIC's size and reach, market participants see great potential for future growth. As the largest life insurer in the country with a total first-year premium of over Rs 1.84 lakh crore in the year ended March 2021, LIC commands a market share of over 66%. It has 2.9 lakh employees, and a network of 22.78 lakh agents. As of March 31, 2020 it had total assets of Rs 37.75 lakh crore and equity AUM of Rs 6.63 lakh crore.

Industry insiders say that even if the 22 lakh agents sell one additional policy in a year, it will add huge volume. Besides, LIC is the biggest institutional investor in India and has a huge investment portfolio that can generate big investment returns.

"Even a marginal per-employee-business-productivity improvement every year for the next few years would result in raising business volumes that are higher than the actual size of a few mid-sized insurance firms," said a market expert.

It is also important to note that while LIC will go for a corporate structure and will have independent directors, it will continue to have the sovereign guarantee that could provide a big comfort to FPIs and other investors. This means the government would provide it capital if the need arises.

For LIC, the challenge lies in bringing efficiency across the large agent network and also in maintaining its market share.

Source: The Indian Express

3. Azithromycin, out of favour as Covid-19 therapy

Relevant for GS Prelims & Mains Paper III; Science & Technology

At one stage, azithromycin was the most commonly prescribed outpatient therapy for Covid-19. A year into the pandemic, however, its use as a treatment option against Covid-19 has gone down, given the lack of evidence that it works. Now, a new study has shown that it does not have a role in the treatment of Covid-19; it only has a placebo effect.

Azithromycin and Covid-19

Azithromycin is a broad-spectrum antibiotic that is widely available. It is prescribed for various bacterial infection. Having been shown to reduce exacerbations in chronic airway diseases, it was widely prescribed for Covid-19 initially, including in India.

However, medical experts said its use has gone down since last year. It has also been taken out of national state guidelines for treatment of Covid-19.

The new findings

The study was published last week in the Journal of the American Medical Association. Researchers at the University of California, San Francisco and Stanford University recruited 263 participants, of whom 171 received a single oral dose of azithromycin while 92 received matching placebo. The randomised clinical trial of azithromycin vs matching placebo was conducted from May 2020 through March 2021.

Authors Catherine Oldenburg and others wrote that among the outpatients with SARS-CoV2 infection, treatment with a single dose of oral azithromycin compared with placebo

did not result in a greater likelihood of being free of symptoms at day 14. “Our study findings do not support the routine use of azithromycin for outpatient SARS-CoV2 infection,” the authors wrote.

India and azithromycin

In the early days of the pandemic, the treatment protocol from the Ministry of Health and Family Welfare had noted that there were no specific antiviral drugs proved to be effective against Covid-19, and had allowed physicians to consider hydroxychloroquine in combination with azithromycin for patients with severe disease and requiring ICU management.

While some state health departments include azithromycin in their guidelines issued three months ago as a drug that can be administered to patients in home isolation, it is no longer included in the clinical management protocol for Covid 19 issued in May this year by the Union Ministry of Health and Family Welfare.

At a virtual media briefing in April, AIIMS Director Dr Randeep Guleria had told The Indian Express that data did not support the use of hydroxychloroquine and azithromycin, and it is currently not in most guidelines. “There is no conclusive evidence that these drugs are of any benefit. However some people use HCQS as it may have some benefit and may not cause harm. The same goes for azithromycin, which is not used as an antibiotic, but as an immunomodulator. Both these drugs are used in some areas,” he had said.

Reducing its use

Dr Sanjay Pujari, member of the National Task Force on Clinical Research of Covid-19, said azithromycin has been shown to be non-efficacious by multiple randomised controlled trials. The proportion of use may have gone down at least in hospitalised patients, he said.

Pune-based infectious diseases consultant Dr Parikshit Prayag said the use of azithromycin was stopped a long time ago. And Dr D B Kadam, Chair of the Covid task force for Pune division, said azithromycin was in use last year as an antibiotic for atypical pneumonia and possible in vitro antiviral activity. Due to cardiac side effects the use of this drug has been stopped and is not part of any guidelines this year, he said.

Overuse concerns

The authors of the new study have said that if azithromycin does not have a role in the treatment of Covid-19, avoiding its use would reduce unnecessary antibiotic consumption.
“Overuse of antibiotics during Covid-19 pandemic may lead to increased selection for antimicrobial resistance. Widespread use of azithromycin for Covid 19 in the absence of a clear bacterial indication may contribute to resistance selection,” Oldenburg and others have written.

Source: The Indian Express

4. The laws for surveillance in India, and the concerns over privacy

Relevant for GS Prelims & Mains Paper II; Polity & Governance

In response to the finding by a global collaborative investigative project that Israeli spyware Pegasus was used to target at least 300 individuals in India, the government has claimed that all interception in India takes place lawfully. So, what are the laws covering surveillance in India?

Communication surveillance in India takes place primarily under two laws — the Telegraph Act, 1885 and the Information Technology Act, 2000. While the Telegraph Act deals with interception of calls, the IT Act was enacted to deal with surveillance of all electronic communication, following the Supreme Court's intervention in 1996. A comprehensive data protection law to address the gaps in existing frameworks for surveillance is yet to enacted.

Telegraph Act, 1885

Section 5(2) of the Telegraph Act reads: "On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order…"

Under this law, the government can intercept calls only in certain situations — the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order, or for preventing incitement to the commission of an offence. These are the same restrictions imposed on free speech under Article 19(2) of the Constitution.

Significantly, even these restrictions can be imposed only when there is a condition precedent — the occurrence of any public emergency, or in the interest of public safety.

Additionally, a proviso in Section 5(2) states that even 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 shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

Supreme Court intervention

In Public Union for Civil Liberties v Union of India (1996), the Supreme Court pointed out lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions. A public interest litigation was filed in the wake of the report on "Tapping of politicians phones" by the CBI.

The court noted that authorities engaging in interception were not even maintaining adequate records and logs on interception. Among the guidelines issued by the court were setting up a review committee that can look into authorisations made under Section 5(2) of the Telegraph Act.

"Tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to sold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of subrosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by she authorities of the day," the court said. The Supreme Court's guidelines formed the basis of introducing Rule 419A in the Telegraph Rules in 2007 and later in the rules prescribed under the IT Act in 2009.

Rule 419A states that a Secretary to the Government of India in the Ministry of Home Affairs can pass orders of interception in the case of Centre, and a secretary-level officer who is in-charge of the Home Department can issue such directives in the case of a state government. In unavoidable circumstances, Rule 419A adds, such orders may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary or the state Home Secretary.

IT Act, 2000

Section 69 of the Information Technology Act and the Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were enacted to further the legal framework for electronic surveillance. Under the IT Act, all electronic transmission of data can be intercepted. So, for a Pegasus-like spyware to be used lawfully, the government would have to invoke both the IT Act and the Telegraph Act. Apart from the restrictions provided in Section 5(2) of the Telegraph Act and Article 19(2) of the Constitution, Section 69 the IT Act adds another aspect that makes it broader — interception, monitoring and decryption of digital information "for the investigation of an offence".

Significantly, it dispenses with the condition precedent set under the Telegraph Act that requires "the occurrence of public emergency of the interest of public safety" which widens the ambit of powers under the law.

Identifying the gaps

In 2012, the Planning Commission and the Group of Experts on Privacy Issues headed by former Delhi High Court Chief Justice A P Shah were tasked with identifying the gaps in laws affecting privacy.

On surveillance, the committee pointed out divergence in laws on permitted grounds, "type of interception", "granularity of information that can be intercepted", the degree of assistance from service providers, and the "destruction and retention" of intercepted material, according to a report by the Centre for Internet & Society.

Although the grounds of selecting a person for surveillance and extent of information gathering has to be recorded in writing, the wide reach of these laws has not been tested in court against the cornerstone of fundamental rights.

Source: The Indian Express

PrepMate - Cengage UPSC Book Series

CLICK HERE TO ORDER

KEY FEATURES OF THE BOOK SERIES

- Complete subject in a single book
- Use of Flow Charts, Maps & Diagrams to explain the concepts
- Chapter-wise Practice Questions
- Chapter-wise Past Prelims Questions
- A thorough & Practical Approach to write Mains answers
- Solutions for UPSC Mains from authors
- Repository of Videos along with Books