NASA's Juno spacecraft prepares for rendezvous with Jupiter

NASA`s solar-powered Juno spacecraft, set to arrive at Jupiter this year, successfully executed a maneuver to adjust its flight path on Wednesday.

The maneuver refined the spacecraft’s trajectory, helping set the stage for Juno’s arrival at the solar system’s largest planetary inhabitant five months and a day from now.

“This is the first of two trajectory adjustments that fine tune Juno`s orbit around the Sun, perfecting our rendezvous with Jupiter on July 4,” said Scott Bolton, Juno principal investigator at the Southwest Research Institute in San Antonio.

The Juno spacecraft`s thrusters consumed about 0.6 kg of fuel during the burn and changed the spacecraft`s speed by 0.31 metres per second.

At the time of the maneuver, Juno was about 82 million kms from Jupiter and approximately 684 million kms from Earth.

Launched on August 5, 2011, thee spacecraft will orbit the Jovian world 33 times, skimming to within 5,000 kms above the planet`s cloud tops every 14 days.

During the flybys, Juno will probe beneath the obscuring cloud cover of Jupiter and study its aurorae to learn more about the planet`s origins, structure, atmosphere and magnetosphere.

The next trajectory correction maneuver is scheduled on May 31.

According to NASA, the name Juno comes from Greek and Roman mythology. The god Jupiter drew a veil of clouds around himself to hide his mischief, and his wife – the goddess Juno – was able to peer through the clouds and reveal Jupiter’s true nature.

Netflix cracks down on proxy streaming

Video-streaming giant Netflix has said it is going to stop subscribers from using internet proxies to view content not available in their home countries.

Due to licensing agreements, Netflix content varies between countries – many users have a virtual private network (VPN) or other proxy to get round this.

The firm said it would increase efforts in the next few weeks to block the use of such proxies.

Netflix expanded streaming services to more than 130 countries last week.

But some countries have more content than others – for example, the Australian Netflix catalogue has only about 10% of the content available to its US subscribers.

David Fullagar, vice president of content delivery architecture, said in a blog post on Thursday that the US firm was in the process of licensing content around the world.

But he said it had a long way to go before it could offer viewers the same films and shows everywhere.

“If all of our content were globally available, there wouldn’t be a reason for members to use

proxies or ‘unblockers’ to fool our systems into thinking they’re in a different country than they’re actually in,” he said.

“In the meantime, we will continue to respect and enforce content licensing by geographic location.”

Subscribers that currently use proxies to view content outside their countries will only be able to access the service in their own countries in the coming week, the company said.

Those members that do not use VPNs will not be impacted by the crackdown, it added.

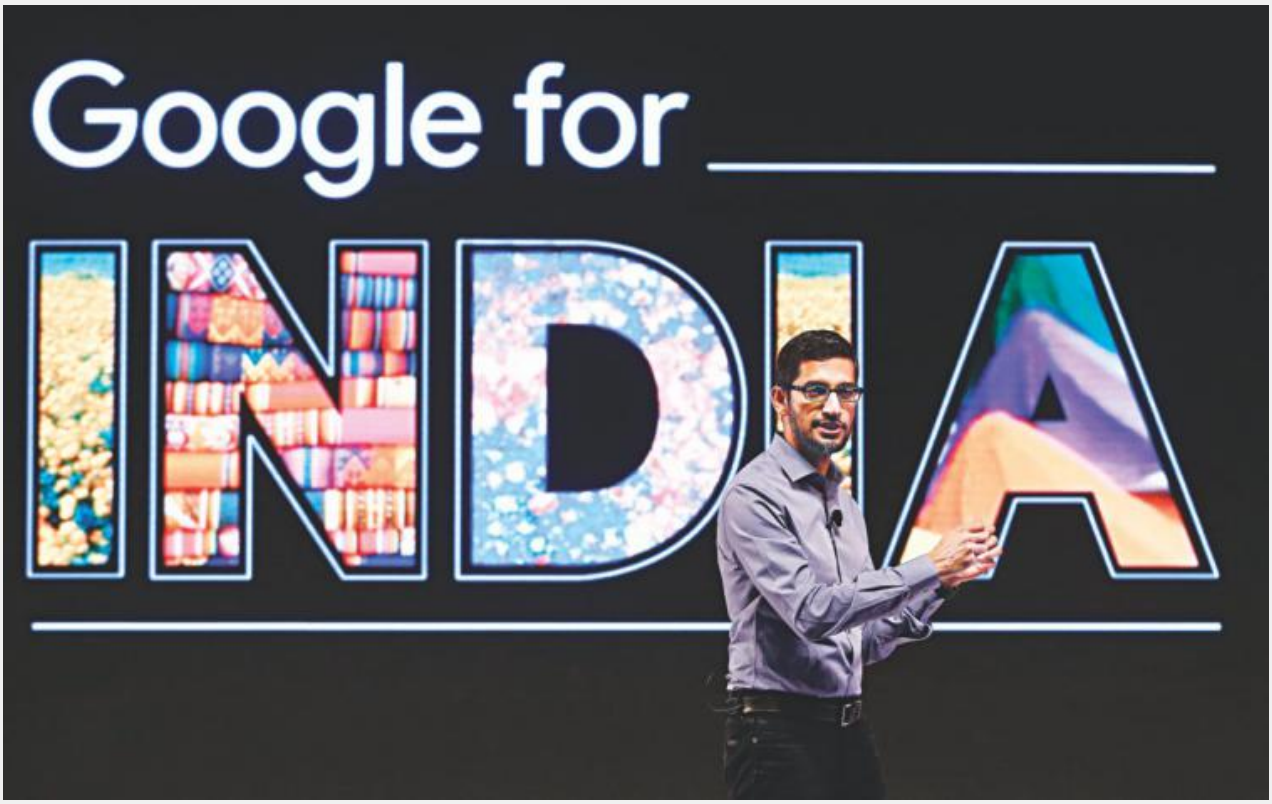
The move is a reversal of Netflix’s denial last week after reports had surfaced that they would be restricting VPN access to their content.

Google CEO Pichai touts India as key testing ground for new products

New Google leader Sundar Pichai pledged on Wednesday to use India as a testing ground for its products as the US tech giant targets hundreds of millions of consumers in the developing world set to move online in the next few years.

“We think that what we build in India will apply to many global places,” Indian-born Pichai, appointed chief executive officer in August, told reporters at an event in New Delhi.

With internet penetration already topping more than 90 percent in many developed markets, Google is increasingly betting on large developing countries like India as a future source of growth. The company does not disclose how much it has invested in India.



Google CEO Sundar Pichai gestures as he addresses a news conference in New Delhi, India yesterday. Photo: Reuters

Google expects more than 500 million Indians to be online by 2018, up from around 300 million today. But Pichai said that with most new users accessing the internet via cheap smartphones instead of desktops, poor mobile connectivity is forcing the company to adapt how it structures and sells its software.

Google's CEO said the company would train two million Indian developers for its Android operating system by 2019, promote internet use among rural women in thousands of villages, and expand its campus in Hyderabad to get more people online.

"It's about making sure that as the next one billion come online, they have access," he said during a visit to the Indian capital, where he is also scheduled to meet Prime Minister Narendra Modi. There are likely to be more users of Google's Android software in India than in the United States next year, Google said in a statement.

Pichai cited user-generated maps, as well as a version of YouTube that allows consumers with limited internet access to store videos offline, as two recent examples of products developed in India that have since been rolled out to other countries.

Google is also working with Indian Railways to bring wireless internet service to 100 train stations, with Mumbai Central the first to go online in January. It's also working on increasing the number of local languages available on its virtual keyboard to target non-English speakers.

Facebook amends 'real name' policy after protests

After passionate and at times angry pleas from various vulnerable communities, Facebook has announced it is to amend its controversial "real name" policy.

On Tuesday the site said it was to test new tools that allowed people to share any special circumstances they felt meant they could not use their real name.

The tool is intended to help people who may have suffered domestic abuse, or in cases where their sexuality could put them in danger.

However, Facebook stood firm on insisting people use "real names" in all but the most unusual situations.

"We require people to use the name their friends and family know them by," the company said.

"When people use the names they are known by, their actions and words carry more weight because they are more accountable for what they say.

"We're firmly committed to this policy, and it is not changing.

"However, after hearing feedback from our community, we recognise that it's also important that this policy works for everyone, especially for communities who are marginalised or face discrimination."

Intense pressure

The company is also adding a new tool for reporting fake names, requiring anyone who is reporting another user to provide more context for their complaint.

Facebook said it received hundreds of thousands of reports of fake names every week.

“In the past, people were able to simply report a ‘fake name’ but now they will be required to go through several new steps that provide us more specifics about the report,” the company said.

“This additional context will help our review teams better understand why someone is reporting a name, giving them more information about a specific situation.”

The social network had faced intense pressure from rights groups over its hard-line stance on real names.

Founder Mark Zuckerberg was heavily criticised after he suggested that people that use two names, or have an alias, showed a “lack of integrity”.

Drag queens

Last year, prominent drag queens in San Francisco had their Facebook accounts deleted as they were deemed to be violating the real name policy.

After considerable uproar, including a planned protest outside Facebook’s headquarters, the company acknowledged that it had been a mistake to delete the accounts, but said it faced a challenge in verifying people on the network.

It argued that insisting on real names played a role in preventing bad actors on the site has it made people more accountable for what they posted.

“The stories of mass impersonation, trolling, domestic abuse, and higher rates of bullying and intolerance are oftentimes the result of people hiding behind fake names, and it’s both terrifying and sad,” the site said.

“Our ability to successfully protect against them with this policy has borne out the reality that this policy, on balance, and when applied carefully, is a very powerful force for good.”

A group of civil liberties organisations and rights groups formed the Nameless Coalition which has been leaning on Facebook to change its policies.

The new tools announced on Tuesday fall short of the group’s complete suggestions, but representatives from Facebook are met members of the Nameless Coalition at a public event in San Francisco.

News Source

US hobbyists 'must register drones' from 21 December

Drones in the US, and the people who fly them, must be registered on a government database starting from 21 December.

Any drones purchased from that date onwards must be logged before the first outdoor flight, the country's Federal Aviation Administration (FAA) has said.

Existing drone owners have until 19 February 2016 to register their drones, but a $5 (£3.30) fee will be waived to encourage registration within the first 30 days.

FAA spokesman Les Dorr told the BBC that it would seek to educate, rather than punish, those found to have no registered their drones.

But he added: "For people who simply refuse to register, we do have enforcement tools available."

Those punishments could be civil penalties of up to $27,500, but in severe cases, criminal prosecutions could result in a $250,000 fine and a maximum of three years in prison.

The rule affects drones weighing in at half a pound to 55lb (228g to 22.7kg). Users older than 13 must register themselves, but parents can register on behalf of younger children.

Each drone will be given a unique identification number to be displayed on the device.

'Great responsibility'

On Monday, the FAA promised the process would be "streamlined and user-friendly".

"Make no mistake: unmanned aircraft enthusiast are aviators and with that title comes a great deal of responsibility," US transportation secretary Anthony Foxx said in a statement.

"Registration gives us an opportunity to work with these users to operate their unmanned aircraft safely.

"I'm excited to welcome these new aviators into the culture of safety and responsibility that defines American innovation."

In depth: Drone discipline

Hobby drones. Unmanned aerial vehicles. Remote-controlled copters.

Call them what you will, they're becoming a nuisance.

A minority of irresponsible users has been flying them too close to aeroplanes and helicopters, wandering into restricted military airspace, spying on neighbours; disrupting sporting events and even injuring people.

It was only a matter of time before some trigger-happy vigilante shot one of the pesky privacy invaders out of the sky.

Regulators and law enforcers are struggling to cope with the growth in their popularity,

increasing the likelihood that heavy-handed legislation could stifle innovation in a sector that has great commercial potential for businesses large and small.

Read more: Can technology keep our skies safe from nuisance drones?

Regulators had been under pressure to clamp down on what many people, particularly those in the emergency services, consider to be a growing menace – hobbyist drone users flying in unwanted places.

Firefighters in California said drones had disrupted efforts to contain wildfires.

‘Stupidity’

However, some believe the drone database will be ineffective.

“The fact is that for the most part, when there are sightings, they don’t actually get to recover the drone itself,” Mickey Osterreicher, from the National Press Photographers’ Association, told BBC News when consultations began in October.

Image copyright US Forest Service
Image caption Warnings about flying drones near fires were issued by the US Forest Service
“So, what would registering the drone accomplish?”

He added that further rules would not prevent bad drone use, drawing comparisons to people who drive cars without a licence or insurance, saying: “You really can’t legislate against stupidity.”

But other bodies, including the Association for Unmanned Vehicle Systems International (AUVSI), have backed the idea and taken an active role in consultations.

The regulations fall some way short of calls to make it legal for emergency services to forcibly disable drones by using electronic jamming.

Follow Dave Lee on Twitter @DaveLeeBBC

The computer virus that blackmails you

Out of media player. Press enter to return or tab to continue.
Media captionWhat is ransomware?
Ransomware is the fastest growing form of computer malware, experts warn.

It’s a malicious virus that locks the user out of their computer and demands a fee to return their files.

A report published by the Australian government claims 72% of businesses surveyed experienced ransomware incidents in 2015.

The figure was just 17% in 2013 .

It’s also a growing threat for mobile devices as it can be hidden in an app, says Gert-Jan

Schenk, vice-president at internet security company Lookout.

“For the most part, we’ve seen ransomware delivered through drive-by downloads – it pretends to be a popular app, increasing the chances that you’ll click on it,” he explains.

“To avoid these threats, users should be very careful about what apps they install, and where they come from – read the reviews on Google Play, and avoid side-loading from untrusted sources.”

How does it work?

Like most computer viruses, ransomware often arrives in the form of a phishing email, or spam, or a fake software update – and the recipient clicks a link or opens an attachment.

The virus then sets to work encrypting the user’s files.

Once the computer is effectively locked down, it demands a fee – often in bitcoins because it is less easy to trace – for the return of the files.

The fee is generally one or two bitcoins – the equivalent of about $500 (£330).

It is less common now, but in the earlier days of the malware – about five years ago – the ransom note could take the form of a law enforcement notice.

The user was directed to a web page that appeared to be from, for example, the FBI, falsely claiming illegal images of children had been been found on the machine and a fine was payable.

There is generally a time limit to comply, after which the ransom increases.

Is there any way to get round it?

Sometimes it is just a threat, but mostly the virus really does encrypt files.

The only way to retrieve your files without paying the ransom is to go to a backed-up version.

Neil Douglas, from Edinburgh-based IT company Network Roi, has just helped a small business client whose server was hit by ransomware.

“We had to recover everything from back-up. We’d had a back-up two minutes before the infection, so the timing couldn’t have been any better – but it did result in quite a bit of downtime,” he says.

“You could risk paying them – but it’s a bit like paying a blackmailer. We would only recommend it as a last resort.

“You don’t know whether they’ll come back for more, you don’t know that they’ll clear the infection.”

Cybersecurity expert Prof Alan Woodward says paying also leaves you vulnerable to further cybercrime.

“As soon as you pay up, you get on a suckers’ list and you’ll probably get contacted again,” he says.

“It’s low-hanging fruit for the criminals.”

Do many people pay?

While all the expert advice is, of course, not to pay, plenty of people do – even those you would least expect to.

Tewksbury Police, in the US, admitted they had paid up when their main server had been attacked and locked down at the end of last year.

“Nobody wants to negotiate with terrorists. Nobody wants to pay terrorists,” Police Chief Timothy Sheehan told the town’s local paper.

“We did everything we possibly could.

“It was an eye-opening experience, I can tell you right now. It made you feel that you lost control of everything.

“Paying the bitcoin ransom was the last resort.”

Ransomware is lucrative for criminals because so many victims pay rather than face the shame of false accusations – or like the police department, they just desperately need their files.

“Some companies have set up bitcoin accounts in case it happens to them,” says Prof Woodward.

“I would recommend that nobody ever pays up.

“The only way to deal with it is to be sure you have a virus checker and back up.”

Who is behind it?

“It tends to be organised crime,” says Prof Woodward.

“They do make millions out of it. It’s opportunistic… they just try it on everybody. You keep third parties out of it – the bank isn’t involved.”

Recent research by Palo Alto Networks and industry partners suggested one family of ransomware known as Crypto Wall had generated about $325m (£215m) for the gang behind it.

“In the volume cybercrime space, ransomware is one of the most prolific problems we face,” Greg Day, chief security officer for Europe at Palo Alto Networks, told the BBC last month.

“Credit card theft is getting to the point where the value of each card is very low. As a result, ransomware has stepped into that gap and gives a higher value for each victim.”

News Source

Moonfruit takes websites offline after cyber-attack threat

Thousands of business and personal websites have been taken offline by web host Moonfruit, after it was threatened with a cyber-attack.

The Moonfruit service lets customers easily build templated websites.

But the company said it had been threatened with a cyber-attack and had decided to make its customers' websites unavailable for "up to 12 hours" to make infrastructure changes.

One business owner told the BBC it was "very bad timing".

On Thursday, 10 December, the company said it had been hit by a distributed denial of service (DDoS) attack.

Attackers bombarded the company's computers to overwhelm them with traffic, so they could not serve its legitimate users.

The company consequently told customers it had decided to take websites offline for "up to 12 hours" starting at 10:00 GMT on Monday.

Film-maker Reece de Ville said: "They have been slow to communicate via their website what is going on.

"I'm going to have hundreds of people finding my site today but not being able to access it.

"I could be losing out on a lot of money from potential clients, and they may not come back if they think the company has gone.

"It's incredibly bad timing, especially for businesses selling Christmas cards and gifts on their website."

Short notice

In an email to its customers, the company apologised for giving them "short notice" that their websites would be offline.

"We have been working with law enforcement agencies regarding this matter and have spared no time or expense in ensuring we complete the work as quickly as possible," the company's director, Matt Casey, said in a statement.

The BBC has invited Moonfruit to comment.

News Source