China’s plan to dominate legacy chips globally sparks US probe

Under Joe Biden’s direction, the US Trade Representative (USTR) launched a probe Monday into China’s plans to globally dominate markets for legacy chips—alleging that China’s unfair trade practices threaten US national security and could thwart US efforts to build up a domestic semiconductor supply chain.

Unlike the most advanced chips used to power artificial intelligence that are currently in short supply, these legacy chips rely on older manufacturing processes and are more ubiquitous in mass-market products. They’re used in tech for cars, military vehicles, medical devices, smartphones, home appliances, space projects, and much more.

China apparently “plans to build more than 60 percent of the world’s new legacy chip capacity over the next decade,” and Commerce Secretary Gina Raimondo said evidence showed this was “discouraging investment elsewhere and constituted unfair competition,” Reuters reported.

Most people purchasing common goods don’t even realize they’re using Chinese chips, including government agencies, and the probe is meant to fix that by flagging everywhere Chinese chips are found in the US. Raimondo said she was “fairly alarmed” that research showed “two-thirds of US products using chips had Chinese legacy chips in them, and half of US companies did not know the origin of their chips including some in the defense industry.”

To deter harms from any of China’s alleged anticompetitive

behavior, the USTR plans to spend a year investigating all of China’s acts, policies, and practices that could be helping China achieve global dominance in the foundational semiconductor market.

The agency will start by probing “China’s manufacturing of foundational semiconductors (also known as legacy or mature node semiconductors),” the press release said, “including to the extent that they are incorporated as components into downstream products for critical industries like defense, automotive, medical devices, aerospace, telecommunications, and power generation and the electrical grid.”

Additionally, the probe will assess China’s potential impact on “silicon carbide substrates (or other wafers used as inputs into semiconductor fabrication)” to ensure China isn’t burdening or restricting US commerce.

Some officials were frustrated that Biden didn’t launch the probe sooner, the Financial Times reported. It will ultimately be up to Donald Trump’s administration to complete the investigation, but Biden and Trump have long been aligned on US-China trade strategies, so Trump is not necessarily expected to meddle with the probe. Reuters noted that the probe could set Trump up to pursue his campaign promise of imposing a 60 percent tariff on all goods from China, but FT pointed out that Trump could also plan to use tariffs as a “bargaining chip” in his own trade negotiations.

https://arstechnica.com/tech-policy/2024/12/chinas-plan-to-dominate-legacy-chips-globally-sparks-us-probe/

Man who claims he invented bitcoin faces prison after filing $1.1 trillion suit

Wright's lawsuit names a defendant he calls "BTC Core," which apparently doesn't exist. Wright alleges that BTC Core "partners" include 122 corporate entities and 22 individuals who contributed to bitcoin development and research. Wright also named BTC Core as a defendant in a 2022 lawsuit.

This week's court ruling said that "COPA (and others) say there is no such entity and it is an invention of Dr. Wright's in his attempt to designate those who are or who have been involved in the development of the software used in various manifestations of Bitcoin as a partnership. They deny there is any such partnership, as Dr. Wright seems to allege. It is not necessary to resolve that issue."

Corporations and individuals that Wright claims are part of BTC Core "were defendants to various of the previous actions brought by Dr. Wright (and his companies)," Mellor wrote.

Wright suit "repeat[s] his dishonest claim to be Satoshi"

Wright contended that his lawsuit falls outside the bounds of the previous order because his new claims "do not involve him claiming to be Satoshi Nakamoto and do not depend on him having invented the Bitcoin system," Mellor wrote. Mellor rejected Wright's arguments.

For one thing, Mellor said the earlier order "is not limited

to prohibiting claims dependent on Dr. Wright asserting that he is Satoshi Nakamoto." For another, Mellor pointed out that Wright's latest lawsuit "does include pleaded contentions that he is Satoshi Nakamoto," and thus "Dr. Wright is wrong to say that his New Claim does not repeat his dishonest claim to be Satoshi."

Further, COPA contended "that each of the principal claims in the New Claim can only be maintained by Dr. Wright asserting intellectual property rights which the Order precludes him from asserting in legal proceedings."

Addressing Wright's copyright claim, Mellor wrote that "Dr. Wright does not claim a license or any assignment from some other person alleged to be owner of copyright in the relevant works. Therefore Dr. Wright cannot bring this claim for copyright infringement without claiming ownership of the rights which he alleges to have been infringed. That is to say, Dr. Wright cannot bring an infringement claim in relation to the works in question, however it is worded, without breaching the Order."

https://arstechnica.com/tech-policy/2024/12/judge-rejects-craig-wrights-1-1-trillion-lawsuit-claiming-rights-to-bitcoin/

Automakers excoriated by Senators for fighting right-to-repair

Yesterday, US Senators Jeff Merkley (D-OR), Elizabeth Warren (D-MA), and Joshua Hawley (R-MO) sent letters to the heads of Ford, General Motors, and Tesla, as well as the US heads of Honda, Hyundai, Nissan, Stellantis, Subaru, Toyota, and Volkswagen, excoriating them over their opposition to the right-to-repair movement.

“We need to hit the brakes on automakers stealing your data and undermining your right-to-repair,” said Senator Merkley in a statement to Ars. “Time and again, these billionaire corporations have a double standard when it comes to your privacy and security: claiming that sharing vehicle data with repair shops poses cybersecurity risks while selling consumer data themselves. Oregon has one of the strongest right-to-repair laws in the nation, and that’s why I’m working across the aisle to advance efforts nationwide that protect consumer rights.”

Most repairs aren’t at dealerships

The Senators point out that 70 percent of car parts and services currently come from independent outlets, which are seen as trustworthy and providing good value for money, “while nearly all dealerships receive the worst possible rating for price.”

OEMs and their tier-one suppliers restricting the supply of car parts to within their franchised dealership networks also slows down the entire repair process for owners as well as increasing the cost of getting one’s car fixed, the letter states.

As Ars noted recently, more than one in five automotive recalls are now fixed with software patches, and increasingly the right-to-repair fight has centered on things digital—access to diagnostics, firmware, and connected services. The percentage of non-hardware recall fixes will surely grow in the coming years as more and more automakers

replace older models with software-defined vehicles.

https://arstechnica.com/cars/2024/12/senators-blast-carmakers-over-right-to-repair-opposition/

Crypto scammers posing as real brands on X are easily hacking YouTubers

“I’m fighting with Google now,” Townsend told Ars. “I don’t expect any real answers from them.”

How YouTubers can avoid being targeted

As YouTube appears evasive, Townsend has been grateful for long-time subscribers commenting to show support, which may help get his videos amplified more by the algorithm. On YouTube, he also said that because “the outpouring of support was beyond anything” he could’ve expected, it kept him “sane” through sometimes 24-hour periods of silence without any updates on when his account would be restored.

Townsend told Ars that he rarely does sponsorships, but like many in the fighting game community, his inbox gets spammed with offers constantly, much of which he assumes are scams.

“If you are a YouTuber of any size,” Townsend explained in his YouTube video, “you are inundated with this stuff constantly,”

so “my BS detector is like, okay, fake, fake, fake, fake, fake, fake, fake. But this one just, it looked real enough, like they had their own social media presence, lots of followers. Everything looked real.”

Brian_F echoed that in his video, which breaks down how the latest scam evolved from more obvious scams, tricking even skeptical YouTubers who have years of experience dodging phishing scams in their inboxes.

“The game has changed,” Brian_F said.

Townsend told Ars that sponsorships are rare in the fighting game community. YouTubers are used to carefully scanning supposed offers to weed out the real ones from the fakes. But Brian_F’s video pointed out that scammers copy/paste legitimate offer letters, so it’s already hard to distinguish between potential sources of income and cleverly masked phishing attacks using sponsorships as lures.

Part of the vetting process includes verifying links without clicking through and verifying identities of people submitting supposed offers. But if YouTubers are provided with legitimate links early on, receiving offers from brands they really like, and see that contacts match detailed LinkedIn profiles of authentic employees who market the brand, it’s much harder to detect a fake sponsorship offer without as many obvious red flags.

https://arstechnica.com/tech-policy/2024/12/crypto-scammers-posing-as-real-brands-on-x-are-easily-hacking-youtubers/

US temporarily bans drones in parts of NJ, may use “deadly force” against aircraft

The Federal Aviation Administration temporarily banned drones over parts of New Jersey yesterday and said “the United States government may use deadly force against” airborne aircraft “if it is determined that the aircraft poses an imminent security threat.”

The FAA issued 22 orders imposing “temporary flight restrictions for special security reasons” until January 17, 2025. “At the request of federal security partners, the FAA published 22 Temporary Flight Restrictions (TFRs) prohibiting drone flights over critical New Jersey infrastructure,” an FAA statement said.

Each NOTAM (Notice to Air Missions) affects a specific area. “No UAS [Unmanned Aircraft System] operations are authorized in the areas covered by this NOTAM” unless they have clearance for specific operations, the FAA said. Allowed operations include support for national defense, law enforcement, firefighting, and commercial operations “with a valid statement of work.”

“Pilots who do not adhere to the following proc[edure] may be intercepted, detained and interviewed by law enforcement/security personnel,” the FAA said. Violating the order could result in “civil penalties and the suspension or revocation of airmen certificates,” and criminal charges, the FAA said.

The New Jersey orders affect areas in Evesham, Hamilton,

Bridgewater, Cedar Grove, Metuchen, North Brunswick Township, Camden, Gloucester City, Westampton, South Brunswick, Edison, Branchburg, Sewaren, Jersey City, Harrison, Elizabeth, Bayonne, Winslow, Burlington, Clifton, Hancocks Bridge, and Kearny.

5,000 tips to FBI, but nothing "anomalous"

The latest notices follow numerous sightings of objects that appeared to be drones, which worried New Jersey residents and prompted state and federal officials to investigate and issue several public statements. The FAA last month imposed temporary flight restrictions at the Picatinny Arsenal, an Army research and manufacturing facility, and a Bedminster golf course owned by President-elect Donald Trump.

On December 16, a joint statement was issued by the US Department of Homeland Security, the FBI, the FAA, and Department of Defense. The "FBI has received tips of more than 5,000 reported drone sightings in the last few weeks with approximately 100 leads generated," but evidence so far suggests "the sightings to date include a combination of lawful commercial drones, hobbyist drones, and law enforcement drones, as well as manned fixed-wing aircraft, helicopters, and stars mistakenly reported as drones," the statement said. "We have not identified anything anomalous and do not assess the activity to date to present a national security or public safety risk over the civilian airspace in New Jersey or other states in the northeast."

https://arstechnica.com/tech-policy/2024/12/us-temporarily-bans-drones-in-parts-of-nj-may-use-deadly-force-against-aircraft/

Amazon’s RTO delays exemplify why workers get so mad about mandates

Concern about RTO planning is underscored by Amazon reportedly lacking enough space for its current in-office policy. Bloomberg said that “in recent interviews, employees complained of working from shared desks, crowded corporate canteens, and a lack of conference rooms for confidential calls or team meetings.”

The publication also pointed to employee displeasure with having to work in an office full-time when other tech firms have more lax policies. This could result in Amazon losing some of its best talent. Per the study from the University of Pittsburgh, Baylor University, The Chinese University of Hong Kong, and Cheung Kong Graduate School of Business researchers, senior, skilled workers are more likely to depart a company over an RTO mandate because they have “more connections with other companies.”

Employees eyeing greener pastures could put Amazon at risk of losing some of its most experienced employees. That also reportedly happened to Apple, Microsoft, and SpaceX following their RTO mandates, per a May study from University of Chicago and University of Michigan researchers (PDF). Following Amazon’s RTO announcement, 73 percent of 2,285 workers that Blind surveyed said they were “considering looking for another job” due to the rule change.

Finally, banning remote work while giving workers a few months to figure out how to adjust resulted in a lot of negative discourse, including Garman reportedly telling workers that if

they don’t work well in offices, “that’s okay; there are other companies around.” As the November RTO study put it:

“An RTO announcement can be a big and sudden event that is distasteful to most employees, especially when the decision has not been well communicated, potentially triggering an immediate response of employees searching for and switching to new jobs.”

If Amazon had communicated RTO dates with greater accuracy once office plans were finalized, it could have alleviated some of the drama that followed the announcement and the negative impact that had on employee morale.

For its part, Amazon has instituted a tool for reserving conference rooms, which requires workers to commit to using the space so it’s not wasted, Bloomberg reported.

But with companies now having had years to plot their RTO approaches, employees are expecting more accurate communication and smooth transitions that align with their respective department’s culture. Amazon’s approach missed those marks.

https://arstechnica.com/tech-policy/2024/12/amazons-rto-delays-highlight-why-workers-get-so-mad-about-mandates/

$2 per megabyte: AT&T mistakenly charged customer $6,223 for 3.1GB of data

An AT&T customer who switched to the company's FirstNet service for first responders got quite the shock when his bill came in at $6,223.60, instead of the roughly $260 that his four-line plan previously cost each month.

The Texas man described his experience in a now-deleted Reddit post three days ago, saying he hadn't been able to get the obviously incorrect bill reversed despite calling AT&T and going to an AT&T store in Dallas. The case drew plenty of attention and the bill was finally wiped out several days after the customer contacted the AT&T president's office.

The customer said he received the billing email on December 11. An automatic payment was scheduled for December 15, but he canceled the autopay before the money was charged. The whole mess took a week to straighten out.

"I have been with AT&T for over a decade and I have always had unlimited plans so I knew this was a mistake," he wrote. "The only change I have made to my account is last month I moved my line over to FirstNet. I am a first responder and I was told my price per month would actually go down a few dollars a month."

"We have apologized for the inconvenience"

AT&T confirmed to Ars today that it "straightened out the customer's bill."

"We understand how frustrating this must have been for [the customer] and we have apologized for the inconvenience. We have resolved his concerns about his bill and are investigating to determine what caused this system error," an AT&T spokesperson told Ars.

The customer posted screenshots of his bill, which helpfully pointed out, “Your bill increased $5,956.92” since the previous month. It included a $5.73 “discount for first responder appreciation,” but that wasn’t enough to wipe out a $6,194 line item listed as “Data Pay Per use 3,097MB at $2.00 per MB.”

https://arstechnica.com/tech-policy/2024/12/2-per-megabyte-att-mistakenly-charged-customer-6223-for-3-1gb-of-data/

Supreme Court to decide if TikTok should be banned or sold

While the controversial US law doesn’t necessarily ban TikTok, it does seem designed to make TikTok “go away,” Greene said, and such a move to interfere with a widely used communications platform seems “unprecedented.”

“The TikTok ban itself and the DC Circuit’s approval of it should be of great concern even to those who find TikTok undesirable or scary,” Greene said in a statement. “Shutting down communications platforms or forcing their reorganization based on concerns of foreign propaganda and anti-national manipulation is an eminently anti-democratic tactic, one that the US has previously condemned globally.”

Greene further warned that the US “cutting off a tool used by 170 million Americans to receive information and communicate

with the world, without proving with evidence that the tools are presently seriously harmful" would "greatly" lower "well-established standards for restricting freedom of speech in the US."

TikTok partly appears to be hoping that President-elect Donald Trump will disrupt enforcement of the law, but Greene said it remains unclear if Trump's plan to "save TikTok" might just be a plan to support a sale to a US buyer. At least one former Trump ally, Steven Mnuchin, has reportedly expressed interest in buying the app.

For TikTok, putting pressure on Trump will likely be the next step, "if the Supreme Court ever says, 'we agree the law is valid,'" Greene suggested.

"Then that's it," Greene said. "There's no other legal recourse. You only have political recourses."

Like other civil rights groups, the EFF plans to remain on TikTok's side as the SCOTUS battle starts.

"We are pleased that the Supreme Court will take the case and will urge the justices to apply the appropriately demanding First Amendment scrutiny," Greene said.

https://arstechnica.com/tech-policy/2024/12/supreme-court-to-decide-if-tiktok-should-be-banned-or-sold/

TP-Link faces possible US ban as hijacked routers fuel

Chinese attacks

Chinese hackers use botnet of TP-Link routers

Microsoft warned on October 31 that hackers working for the Chinese government are using a botnet of thousands of routers, cameras, and other Internet-connected devices for attacks on users of Microsoft's Azure cloud service. Microsoft said that "SOHO routers manufactured by TP-Link make up most of this network," referring to routers for small offices and home offices.

The WSJ said its sources allege that "TP-Link routers are routinely shipped to customers with security flaws, which the company often fails to address" and that "TP-Link doesn't engage with security researchers concerned about them." The article notes that "US officials haven't disclosed any evidence that TP-Link is a witting conduit for Chinese state-sponsored cyberattacks."

We contacted TP-Link today and will update this article if it provides a response. A TP-Link spokesperson told the WSJ that the company "welcome[s] any opportunities to engage with the US government to demonstrate that our security practices are fully in line with industry security standards, and to demonstrate our ongoing commitment to the US market, US consumers, and addressing US national security risks."

A March 2024 Hudson Institute policy memo by Michael O'Rielly, a former Federal Communications Commission member, said it remained "unclear how prevalent TP-Link's vulnerabilities are compared to other wireless routers—from China or elsewhere—as

there is no definitive comparison or ranking of routers based on security." O'Rielly urged federal agencies to "keep track of TP-Link and other manufacturers' cybersecurity practices and ownership structure, including any ties to the Chinese government," but said "there is no evidence to suggest negligence or maliciousness with regard to past vulnerabilities or weaknesses in TP-Link's security."

New push against Chinese tech

TP-Link routers don't seem to be tied to an ongoing Chinese hack of US telecom networks, dubbed Salt Typhoon. But that attack increased government officials' urgency for taking action against Chinese technology companies. For example, the Biden administration is "moving to ban the few remaining operations of China Telecom," a telco that was mostly kicked out of the US in 2021, The New York Times reported on Monday.

https://arstechnica.com/tech-policy/2024/12/report-us-considers-banning-tp-link-routers-over-security-flaws-ties-to-china/

Companies issuing RTO mandates "lose their best talent": Study

Still, the study provides insight into how employees respond to RTO mandates and the effect it has on corporations and available talent at a time when entities like Dell, Amazon, and the US government are getting stricter about in-office

work.

Higher turnover rates

The researchers concluded that the average turnover rates for firms increased by 14 percent after issuing return-to-office policies.

“We expect the effect of RTO mandates on employee turnover to be even higher for other firms” the paper says.

The researchers included testing to ensure that the results stemmed from RTO mandates “rather than time trends.” For example, the researchers found that “there were no significant increases in turnover rates during any of the five quarters prior to the RTO announcement quarter.”

Potentially alarming for employers is the study finding that senior and skilled employees were more likely to leave following RTO mandates. This aligns with a study from University of Chicago and University of Michigan researchers published in May that found that Apple and Microsoft saw senior-level employee bases decrease by 5 percentage points and SpaceX a decrease of 5 percentage points. (For its part, Microsoft told Ars that the report did not align with internal data.)

Senior employees are expected to be more likely to leave, the new report argues, because such workers have “more connections with other companies” and have easier times finding new jobs. Further, senior, skilled employees are “dissatisfied” when management blames remote work for low productivity.

Similarly, the report supports concerns from some RTO-resistant employees that back-to-office mandates have a disproportionate impact on certain groups, like women, which the researchers said show “more pronounced” attrition rates following RTO mandates:

> *Importantly, the effect on female employee turnover is almost three times as high as that on male employees … One possible reason for these results is that female employees are more affected by RTO mandates due to their greater family responsibilities, which increases their demand for workplace flexibility and work-life balance.*

Trouble finding talent

RTO mandates also have a negative impact on companies' ability to find new employees, the study found. After examining over 2 million job postings, the researchers concluded that companies with RTO mandates take longer to fill job vacancies than before:

https://arstechnica.com/tech-policy/2024/12/companies-issuing-rto-mandates-lose-their-best-talent-study/