Russia’s only carrier, damaged in shipyard accident, now on fire

Enlarge / MURMANSK, RUSSIA – DECEMBER 12, 2019: A fire has broken out aboard the Project 11435 aircraft carrier Admiral Kuznetsov of the Russian Northern Fleet. Admiral Kuznetsov is the only aircraft carrier of the Russian Navy. Lev Fedoseyev/TASS
TASS / Lev Fedosev

reader comments

344 with 182 posters participating

Share this story

The Admiral Kuznetsov, Russia’s only aircraft carrier, caught fire today during repairs in Murmansk. While officials of the shipyard said that no shipyard workers were injured, Russia’s TASS news service reports that at least 12 people (likely Kuznetsov sailors) were injured, some critically. In addition, three people, possibly including the third-rank captain in charge of the ship’s repairs, are unaccounted for.

The Kuznetsov has had a long string of bad luck, experiencing fires at sea, oil spills, and landing deck accidents—including a snapped arresting wire that caused a landing Sukhoi Su-33 fighter to roll off the end of the deck and into the ocean. Its boilers belched black smoke during the ship’s transit to Syria in 2016, and it had to be towed back home after breaking down during its return in 2017. Then last year, as it was undergoing repairs in a floating drydock in Murmansk’s Shipyard 82, the drydock sank and a crane on the drydock

slammed into the Kuznetsov, leaving a gash in the ship's hull. It looked like completion of repairs might be put off indefinitely because repair of the drydock would take over a year, and the budget for repairs had been slashed.

The fire was caused when sparks from welding work near one of the ship's electrical distribution compartments set a cable on fire. The fire spread through the wiring throughout compartments of the lower deck of the ship, eventually involving 120 square meters (1,300 square feet) of the ship's spaces.

In total, 12 victims were delivered to hospitals, 10 of them were saved during the fire. One is assessed as serious, and one suffered a head injury. Most received poisoning from combustion products, according to a report from TASS.

Shipboard firefighting, even in port, is a grim and hellish undertaking. Lack of ventilation, darkness, and the toxic smoke released by burning electrical wiring, oil, paint, and equipment make fighting fires aboard a ship particularly difficult, requiring frequent relief of those fighting the fires due to the stress and limits on breathing apparatuses. Those who have served in any navy afloat can attest to how terrifying even the thought of a mass conflagration aboard a ship is, even when pier-side.

https://arstechnica.com/?p=1631867

Senate Judiciary committee

interrogates Apple, Facebook about crypto

Enlarge / Lindsay Graham doesn’t want people reading his texts. But he’ll make darned sure there are backdoors for law enforcement into encrypted texts and devices, and he will pass a law if he needs to.

reader comments

88 with 78 posters participating

Share this story

In a hearing of the Senate Judiciary Committee yesterday, while their counterparts in the House were busy with articles of impeachment, senators questioned New York District Attorney Cyrus Vance, University of Texas Professor Matt Tait, and experts from Apple and Facebook over the issue of gaining legal access to data in encrypted devices and messages. And committee chairman Sen. Lindsay Graham (R-S.C.) warned the representatives of the tech companies, “You’re gonna find a way to do this or we’re going to do it for you.”

The hearing, entitled “Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy,” was very heavy on the public safety with a few passing words about privacy. Graham said that he appreciated “the fact that people cannot hack into my phone, listen to my phone calls, follow the messages, the texts that I receive. I think all of us want devices that protect our privacy.” However, he said, “no American should want a device that is a safe haven for criminality,” citing “encrypted apps that child molesters use” as an example.

“When they get a warrant or court order, I want the government to be able to look and find all relevant information,” Graham declared. “In American law there is no place that’s immune from inquiry if criminality is involved… I’m not about to create a safe haven for criminals where they can plan their misdeeds and store information in a place that law enforcement can never access it.”

Graham and ranking member Sen. Diane Feinstein (D-Calif.)—who referenced throughout the hearing the 2015 San Bernardino mass shooting and the confrontation between Apple and the Federal Bureau of Investigation that resulted from mishandling of the shooter’s county-owned iCloud account by administrators directed by the FBI—closed ranks on the issue.

“Everyone agrees that having the ability to safeguard our personal data is important,” Feinstein said. “At the same time, we’ve seen criminals increasingly use technology, including encryption, in an effort to evade prosecution. We cannot let that happen. It is important that all criminals, whether foreign or domestic, be brought to justice.”

Vance, for his part, called Apple’s and Google’s introduction of device encryption “the single most important challenge to law enforcement over the last 10 years… Apple and Google upended centuries of American jurisprudence.” He cited a human trafficking case he could not get evidence for because of encryption, recounting how the suspect in jail told a cellmate that Apple’s encryption was “a gift from God” to him.

That isn’t how any of this works

Vance has been a frequent and long advocate for federal legislation to ensure legal, extraordinary access to data. “I’m not sure state and local law enforcement are going to be able to bridge the gap with technology without congressional intervention,” Vance told the committee in a response to a question from Sen. Feinstein. Explaining that his office’s lab

gets about 1,600 devices a year as part of case evidence, Vance said, “About 82 percent are locked—it was 60 percent four years ago,” he said. “About half of those are Apple devices. Using technology, we’re able to unlock about half of the devices—so there are about 300 to 400 phones [a year] that we can’t access with the technology we have. There are many, many serious cases where we can’t access the device in the time period where it is most important.”

Feinstein then told the other witnesses, “You heard a very prominent district attorney from New York explain what the situation is… I’d like to have your response on what you’re going to do about it. That will determine the degree to which we do something about it.”

Apple Manager of User Privacy Erik Neuenschwander responded that Apple will continue to work with law enforcement, citing the 127,000 requests from law enforcement for assistance Apple’s team—which includes former law enforcement officials—has responded to over the past seven years, in addition to thousands of emergency requests that Apple has responded to usually within 20 minutes. “We’re going to continue to work with law enforcement as we have to find ways through this,” Neuenschwander said. “We have a team of dedicated professionals that is working on a daily basis with law enforcement.”

Feinstein interrupted Neuenschwander: “My understanding is that even a court order won’t convince you to open the device.”

Neuenschwander replied, “I don’t think it’s a matter of convincing or a court order. It’s the fact that we don’t have the capability today to give the data off the device to law enforcement.” There had been conversations about making changes to fix that, Neuenschwander said, “But ultimately we believe strong encryption makes us all safer, and we haven’t found a way to provide access to users’ devices that wouldn’t

weaken security for everyone.”

Vance said in response that Apple should re-engineer its phones to allow access. “What they created, they can fix,” he said.

https://arstechnica.com/?p=1631711

Lawsuit forces CenturyLink to stop charging “Internet Cost Recovery Fee”

Enlarge / A CenturyLink repair truck in Estes Park, Colorado, in 2018.

reader comments

58 with 46 posters participating

Share this story

CenturyLink has agreed to pay a $6.1 million penalty after Washington state regulators found that the company failed to disclose fees that raised actual prices well above the advertised rates. CenturyLink must also stop charging a so-called “Internet Cost Recovery Fee” in the state, although customers may end up paying the fee until their contracts expire unless they take action to switch plans.

“CenturyLink deceived consumers by telling them they would pay

one price and then charging them more," Washington Attorney General Bob Ferguson said in an announcement yesterday. "Companies must clearly disclose all added fees and charges to Washingtonians."

Ferguson encouraged Washington residents "who believe they have received bills that include undisclosed fees to file a complaint" with the state.

Ferguson's office said it began investigating CenturyLink in 2016 "after receiving complaints from consumers that their actual bills were more than the advertised price, or the price that they were promised by sales representatives."

Here's what Ferguson's office found:

> *There were three main fees CenturyLink did not disclose: a broadcast fee of $2.49 per month, a sports fee of $2.49 per month, and CenturyLink's "Internet Cost Recovery Fee," ranging from $0.99 to $1.99 per month.*
>
> *CenturyLink charged its Internet Cost Recovery Fee to 650,000 Washingtonians. Of those, another 60,000 were also charged the broadcast and sports fees. These fees alone added up to $7 per month to a television subscriber's bill—$84 per year.*
>
> *The investigation found that CenturyLink did not adequately disclose additional taxes and fees for its cable, Internet and telephone services.*

CenturyLink admitted no wrongdoing but agreed to a financial settlement and changes in business practices as part of a consent decree filed in King County Superior Court on Monday. The attorney general's office detailed its allegations in a lawsuit filed the same day.

Internet Cost Recovery Fee

The attorney general's office said that "CenturyLink is required to… stop charging its Internet Cost Recovery Fee" in Washington state. CenturyLink says the fee "helps defray costs associated with building and maintaining CenturyLink's High-Speed Internet broadband network, as well as the costs of expanding network capacity to support the continued increase in customers' average broadband consumption." In other words, the fee covers the company's normal costs of doing business but is excluded from advertised rates in order to make CenturyLink's service sound cheaper than it really is. CenturyLink has been charging $1.99 for the Internet Cost Recovery Fee in Washington and continues to charge an Internet Cost Recovery Fee of $3.99 per Internet connection in other states.

There are circumstances in which CenturyLink can continue charging the fee in the Evergreen State until the end of customers' contracts, but the company must give everyone a chance to opt out of the fee. It would be easier for customers if CenturyLink simply had to eliminate the fee immediately for everyone, regardless of their contract status, but the settlement between Washington and CenturyLink isn't that simple.

"Within 90 days of the effective date of this consent decree, CenturyLink shall not charge any new Washington consumers for any Internet Cost Recovery Fee or Broadband Cost Recovery Fee," the consent decree said. Also within 90 days, CenturyLink must notify current Washington customers that they can cancel service without paying an early termination fee or switch to another plan that doesn't include the Internet Cost Recovery Fee.

If customers who are under contract do not cancel service or switch plans within 30 days of receiving that notice, "these

consumers will continue to be charged the Internet or Broadband Cost Recovery Fee through the expiration of their Internet service plans," the consent decree said.

To settle the case, CenturyLink must also "disclose the actual price of its services, including charges and fees" in sales materials and advertising, provide order confirmations with complete bill summaries to customers "within three days after consumers order services from CenturyLink," and "honor any and all incentives and discounts promised to consumers." Like the promise to stop charging the Internet Cost Recovery Fee, these requirements only apply in Washington state.

To ensure that CenturyLink lives up to its commitment, the company must retain all sales call recordings and correspondence related to sales calls and submit compliance reports to the attorney general's office after one year and again after three years.

https://arstechnica.com/?p=1631587

New YouTube policy tries to ban "implied" threats, "malicious" insults

Enlarge / Photoshopped image of YouTube logo behind a barbed-wire fence.

reader comments

142 with 67 posters participating

Share this story

YouTube has for a long time been used as a platform for bad actors to launch massive campaigns of targeted harassment against individuals. After years of professing an inability to act and reduce such behavior, YouTube is finally updating its policies to reflect the ways bad actors actually tend to behave, and the site is promising to increase consequences against harassers.

Content that “maliciously insults” someone based on their membership in a legally protected class, such as race, gender, or sexual orientation, is now against the rules, YouTube said in a blog post today. “Veiled or implied” threats, of the sort that tend to rile up an online mob to go harass someone, are also now prohibited.

“Something we’ve heard from our creators is that harassment sometimes takes the shape of a pattern of repeated behavior across multiple videos or comments,” YouTube added, catching up to what targets of coordinated online abuse campaigns have been saying for the better part of a decade. As such, the pattern of behavior will now be something the platform takes into account.

Accounts that repeatedly “brush up against” YouTube’s new and improved harassment policy may face financial harm for doing so, the company now says:

> *We’re tightening our policies for the YouTube Partner Program (YPP) to get even tougher on those who engage in harassing behavior and to ensure we reward only trusted creators. Channels that repeatedly brush up against our harassment policy will be suspended from YPP, eliminating their ability to make money on YouTube. We may also remove content from*

channels if they repeatedly harass someone.

Why now?

The change was spurred in part by pushback to YouTube's handling of a harassment campaign against journalist Carlos Maza earlier this year. Maza, who is Latino and openly gay, became a target of conservative personality Steven Crowder, who repeatedly hurled homophobic and racist invectives against Maza in the videos shared with his millions of subscribers.

YouTube investigated the reports against Crowder. On June 4, the company told Maza in a series of tweets that while Crowder's behavior was "hurtful," it did not violate YouTube's policies. One day later, after widespread negative reactions to that statement, YouTube amended its stance and demonetized Crowder, prohibiting him from selling ads on his YouTube videos.

At the same time, YouTube updated its hate speech policy to ban neo-Nazi material and similar white supremacist content. That policy update also prohibited "truther"-style denialist content, such as videos claiming the Holocaust or the 2012 mass shooting at Sandy Hook Elementary School never happened.

That update, however, had an extremely rocky rollout. As soon as the policy launched, a journalist who makes documentary films chronicling hate movements had content removed from YouTube, and his channel was demonetized.

Equally applied?

YouTube said in its statement that the new rules apply to everyone, "from private individuals, to YouTube creators, to public officials." Whether that actually translates into practice, however, is anyone's guess.

Historically speaking, YouTube has not been great about applying its already existing policies evenly across the board. Content moderators working on behalf of YouTube have reported the company deliberately exempts certain high-profile creators from enforcement. But the problem goes well beyond high-profile YouTube "influencers." If anything trips the company up, it's likely to be that claim that "public officials" are also subject to its policies.

Other social media platforms, including Facebook and Twitter, are having a hard time enforcing rules against inflammatory, racist, threatening, or otherwise policy-breaking content on their sites when it comes from politicians, especially but not exclusively US President Donald Trump.

Trump's political rallies, during which he often makes disparaging remarks about a person or group of people, are livestreamed on YouTube, as are other videos in which he does something that would theoretically break YouTube's new terms of service—such as mocking a reporter with a disability. One wonders what, if anything, YouTube will do about videos of this type, which Facebook's and Twitter's policies would leave in place.

https://arstechnica.com/?p=1631401

Maze ransomware was behind Pensacola "cyber event," Florida officials say

Enlarge / Pensacola was hit by Maze ransomware, which has apparently stolen data before encrypting it in other cases.
Paul Harris / Getty Images

reader comments

14 with 13 posters participating

Share this story

An email sent by the Florida Department of Law Enforcement to all Florida county commissioners indicated that the ransomware that struck the city of Pensacola on December 7 was the same malware used in an attack against the private security firm Allied Universal, according to a report by the Pensacola News Journal. That malware has been identified elsewhere as Maze, a form of ransomware that has also been distributed via spam email campaigns in Italy.

Bleeping Computer's Lawrence Abrams reported in November that the Maze operators had contacted him after the Allied Universal attack, claiming to have stolen files from the company before encrypting them on the victims' computers. After Allied apparently missed the deadline for payment of the ransom on the files, the ransomware operators published 700 megabytes of files from Allied and demanded 300 Bitcoins (approximately $2.3 million) to decrypt the network. The Maze operators told Abrams that they always steal victims' files to use as further leverage to get them to pay:

> *It is just a logic. If we disclose it who will believe us? It is not in our interest, it will be silly to disclose as we gain nothing from it. We also delete data because it is not really interesting. We are neither espionage group nor any other type of APT, the data is not interesting for us.*

Stealing data as proof of compromise—and to therefore encourage payment by ransomware victims—is rare but not new. The RobbinHood ransomware operator that attacked Baltimore City in May also stole files as part of the attack and posted screenshots of some files—faxed documents sent to Baltimore City Hall's fax server—on a Twitter account to encourage city officials to pay. Baltimore did not pay the ransom.

Theft of data opens up another problem for targets of ransomware who in the past would pay quietly to decrypt their data, as it introduces the possibility that they will have to report the breach to customers and government regulators. So in some cases, it may ironically remove some of the motivation for victims to pay, since their data may be sold off by the attackers whether they pay or not.

The use of the data to blackmail the victim, and in Allied's case, the threat to use Allied's certificates and domain name to spam customers with additional ransomware attacks, is something new."This is fhe first time this has ever happened, as far as we know," said Brett Callow, a spokesperson for the antivirus software vendor Emisoft." Ransomware groups usually encrypt, not steal. We expect data exfiltration to become more and more commonplace. Whether Pensacola's data was exfiltrated, I obviously can't say."

"Broad targeted" attacks

Maze, Ryuk, and other ransomware attacks against government agencies and companies have moved increasingly toward what Raytheon Cyber Services Senior Manager Dylan Owen referred to as a "broad targeted" attack—while they rely on spam for the initial breach, the attackers "are poking around figuring out who they breached" before they launch the attack.

"They don't necessarily target a specific agency," Owen told Ars. "The attackers have often either gotten a list of emails from another source, or they "have programs that randomly try

emails, or combinations of username, first name/last name, middle initial, all different kinds of combinations," he explained. "They might do a little bit of research if they were going for a particular type of organization, but usually they're very broad-based… then once they get a beacon back saying, 'Hey, somebody clicked on my link', they go and figure out who it was." And if the click came from a larger organization rich in targets, Owen said, they go forward.

State and local agencies have been particularly vulnerable to these sorts of attacks because of the economics of their IT operations. "They're dependent on the funding through taxes or whatever, and that money can only go so far," Owen noted. "They also have a preponderance of older IT systems because of the lack of funding over the years. So it's something that's built upon itself. A lot of them also have proprietary software, so it's not commercial, off the shelf—they hired somebody to create some special code, and that code may not run on newer operating systems. So now they have older operating systems that are harder to patch."

On top of that, many state and local agencies haven't done the work of segregating those vulnerable systems and putting additional defenses around them to reduce the risk posed by legacy systems, Owen explained. But he said that's starting to change. "I know with Louisiana particularly, the governor had said that cyber security is going to be a really big focus for 2020," he said. "They put a lot of money in it in 2019." And while Louisiana had to take the drastic step of cutting off many services during the recent Ryuk attack, it was effective in stopping the spread of the attack.

https://arstechnica.com/?p=1631441

Failed plot to steal domain name at gunpoint brings 14-year prison term

reader comments

116 with 88 posters participating

Share this story

An Iowa man who plotted to steal an Internet domain name at gunpoint was sentenced to 14 years in federal prison yesterday.

Rossi Lorathio Adams II, a former Iowa State University student who ran a social-media platform featuring “images and videos of young adults engaged in crude behavior, drunkenness, and nudity,” repeatedly tried to buy the “doitforstate.com” domain name from a resident of Cedar Rapids. But Adams refused to pay the domain-name owner’s $20,000 asking price—and then things got weird.

“In June 2017, Adams enlisted his cousin, Sherman Hopkins Jr., to break into the domain owner’s home and force him at gunpoint to transfer doitforstate.com to Adams,” a Department of Justice press release said. Hopkins was previously sentenced to 20 years in prison as part of a plea agreement. More details are in the government’s trial brief.

Adams’ social-media venture was called “State Snaps” and had more than 1 million followers on Snapchat, Instagram, and Twitter, the DOJ press release said. The phrase “Do It For State!” was commonly used on the State Snaps platform, which

explains why Adams wanted the doitforstate.com domain name.

The DOJ described Adams as a "social media influencer." Adams told law enforcement that "he used to own the doitforstate.com domain name" before the victim did, according to the trial brief. The victim registered the domain name on GoDaddy sometime after Adams lost control of it. Adams allegedly began pressuring the victim to sell the domain name to him in June 2015.

Robbery ends in gunshots

In June 2017, Adams drove Hopkins to the domain-name owner's house "and provided Hopkins with a demand note, which contained instructions for transferring the domain to Adams' GoDaddy account," the DOJ said. The heist didn't go as planned, and both the domain-name owner and Hopkins ended up suffering gunshot wounds.

Here's how the DOJ described the incident:

> *When Hopkins entered the victim's home in Cedar Rapids, he was carrying a cellular telephone, a stolen gun, [and] a taser, and he was wearing a hat, pantyhose on his head, and dark sunglasses on his face.*
>
> *The victim was upstairs and heard Hopkins enter the home. From the top of a staircase, the victim saw Hopkins with the gun on the first floor. Hopkins shouted at the victim, who then ran into an upstairs bedroom and shut the door, leaning up against the door to stop Hopkins from entering.*
>
> *Hopkins went upstairs, kicked the door open, grabbed the victim by the arm and demanded to know where he kept his computer. When the victim told Hopkins that he kept his computer in his home office, Hopkins forcibly moved the victim to the office. Hopkins ordered the victim to turn on his computer and connect to the Internet. Hopkins pulled out*

> *Adams' demand note, which contained a series of directions on how to change an Internet domain name from the domain owner's GoDaddy account to one of Adams' GoDaddy accounts.*
>
> *Hopkins put the firearm against the victim's head and ordered him to follow the directions on the demand note. Hopkins then pistol whipped the victim several times in the head. Fearing for his life, the victim quickly turned to move the gun away from his head. The victim then managed to gain control of the gun, but during the struggle, he was shot in the leg. The victim shot Hopkins multiple times in the chest. He then contacted law enforcement.*

Hopkins also tased the victim in the "left arm, back, and neck," the trial brief said. Even as the victim was trying to finish the domain-name transfer on the GoDaddy website, Hopkins "cocked the firearm and stated, 'If this isn't right I'm going to blow your fucking head off!'" the trial brief said. That's when the victim fought back and wrestled the gun away from Hopkins. The domain-name transfer apparently wasn't completed.

Adams was convicted in April by a jury in US District Court for the Northern District of Iowa. In addition to his 14-year sentence, Adams was "ordered to make nearly $9,000 in restitution" and pay for court costs of nearly $26,000. "Adams had court-appointed counsel during trial, but the court later discovered Adams was earning significant amounts of money while the case was pending," the press release said.

https://arstechnica.com/?p=1631063

Pensacola confirms ransomware attack but provides few details

Enlarge / Pensacola, home of the Navy's flight school and a cyberwarfare training center, was still reeling from a mass shooting at the Naval Air Station when ransomware hit the city's network.

reader comments

8 with 8 posters participating

Share this story

On December 7—less than a day after a mass shooting at Naval Air Station Pensacola—the city of Pensacola, Florida, was hit by what was originally described as a generic "cyber incident." A city spokesperson has since confirmed that ransomware had struck a number of the city's servers, taking down phones, email, electronic "311" service requests, and electronic payment systems.

With a population of 52,500 people, Pensacola is in Florida's Gulf Coast "panhandle." In addition to being the home of the US Navy's pilot training center, Pensacola is also, perhaps ironically, home of one of the training centers for the Navy's Information Warfare Training Command.

Pensacola public information spokesperson Kacee Lagarde said in a statement that the Pearl Harbor Day ransomware attack began in the early morning. Lagarde said:

> *As a result of the incident, Technology Resources staff*

> *disconnected computers from the city's network until the issue can be resolved… The City of Pensacola has remained operational throughout the incident, but some services have been impacted while the network is disconnected, including City emails, some city landlines, 311 customer service (311 can receive calls, but online services are not available) [and] online bill payments including Pensacola Energy and City of Pensacola Sanitation Services. Emergency dispatch services and 911 were not impacted and continue to operate normally.*

The attack's timing appears to be coincidental and not related to the killing of three sailors by a Saudi Air Force officer on December 6. And it follows the pattern of a number of recent Ryuk-based ransomware attacks on other state and local agencies.

Ars reached out to Pensacola officials for more details on the attack but received no response—possibly because the city has just begun to restore email service to city workers with mobile devices.

Enlarge / A Pensacola city-government Facebook update on the ransomware attack.

Backup on the bayou

Meanwhile, Louisiana officials claim to have largely shrugged off last month’s Ryuk ransomware attack. In a statement to Ars, Jacques Berry, director of policy and communication for Louisiana’s Division of Administration, characterized the ransomware as an “abject failure” because there was no “major data loss or compromised information or irrecoverable applications—none of these happened.” Berry insisted that sources who spoke to Ars “have incorrect, misleading, or conflicting information. I would strongly caution you against trusting information that doesn’t come from me or an interview arranged by me.”

The staff of Louisiana's Office of Technology Services spent the week after the attack "laboring 24/7," Berry said, "and scaling back only somewhat since then… They implemented a plan with a specific order of priority and continue their efforts as final service restorations are completed in the most urgent but accurate manner possible."

Medicaid records affected were limited to "program files from the Medicaid office," Berry said, and the state's new LaMEDS (Louisiana Medicaid Enrollment System) was not affected. Additionally, he said, no Medicaid recipient's personal information was in the affected data. Other reported data outages were due to network shutdowns and not data loss, Berry explained.

https://arstechnica.com/?p=1631115

Uploaded Ring footage reportedly provides location to the square inch

Enlarge / A Ring camera doorbell.

reader comments

141 with 75 posters participating, including story author

Share this story

Amazon's aggressive push to grow its surveillance-camera

company Ring is working, and adoption has skyrocketed in the past two years thanks to deals with hundreds of police departments. A new set of reports highlights the ways Amazon convinces police to join those partnerships—and the amount of data that users can inadvertently reveal.

Integral to the Ring system is an app called Neighbors, kind of like an over-eager NextDoor with everything except the crime stripped out. Neighbors generates a map of your local area, based on your address, and then populates it with crime reports. Those reports include comments from other Neighbors users, as well as reports of burglaries, vehicle break-ins or theft, shots fired or shootings, stabbings, hostages taken, and arson imported from real-time 911 dispatcher data.

Anyone can install the app and create an account, but owners of Ring devices can also upload video snippets to the service, either when they have something they want to share or when police request it using the companion portal for law enforcement. Gizmodo this week published a new report delving into video data available on Neighbors to identify precisely how many Ring cameras are deployed, and where.

Too many to count

Gizmodo conducted its analysis in November, using videos posted to Neighbors in the previous 500 days—since right around July 1, 2018, give or take. The report managed to grab the precise locations of about 20,000 Ring cameras in nine-square-mile zones of 15 different US cities. Gizmodo adds that the reporters don't actually know how many camera locations they *could* have obtained, because they stopped collecting the data once they had enough information to generate their report.

In a location selected at random in Washington, DC, for example, Gizmodo was able to identify at least 1,863 unique Ring cameras that had uploaded video to Neighbors during the

500-day window. In their 9-square-mile sample of Los Angeles, they found at least 5,016 Ring cameras; in Denver, 1,788.

Gizmodo writes:

> *Examining the network traffic of the Neighbors app produced unexpected data, including hidden geographic coordinates that are connected to each post—latitude and longitude with up to six decimal points of precision, accurate enough to pinpoint roughly a square inch of ground.*

Many of those coordinates were indeed right in front of someone's house, a few feet away from the location of the camera. Some were near intersections; the farthest Gizmodo identified was about 260 feet. However, they note, backtracking to find the camera that captured footage is "trivial" in person, when armed with the video and the coordinates, and reporters basically drove or walked up to people's houses to prove it.

Ring did not refute Gizmodo's location findings, the site reports. Instead, the company said, "Only content that a Neighbors user chooses to share on the Neighbors App is publicly accessible through the Neighbors App or by your local law enforcement."

Gizmodo also spoke with a researcher at the Massachusetts Institute of Technology who has used several years' worth of video posted to Neighbors to make a similar map. He has so far pinpointed the locations of about 440,000 Ring cameras.

Ring did not refute that it was possible for anyone, armed with the data Gizmodo acquired, to pinpoint the exact locations of users' homes. Instead, the company reiterated that "Only content that a Neighbors user chooses to share on the Neighbors App is publicly accessible through the Neighbors App or by your local law enforcement."

What privacy?

When neighborhoods are blanketed with surveillance cameras, the privacy implications are profound. And because these cameras belong to individuals, there are few if any restrictions on what footage can be captured or used.

In Washington, DC, for example, Gizmodo notes that at least 13 active Ring cameras line the path between one public charter school for grades 6-12 and the soccer field its students use. Gizmodo also found several dozen instances of DC residents using Neighbors to share videos of children. Some of the kids in question were reportedly doing such activities as riding bicycles and taking selfies. Not exactly striking threats to public safety—but in a densely urban environment such as the District of Columbia, perhaps the homeowners simply did not have lawns to tell the kids to get off of.

Security and surveillance experts voiced concerns to Gizmodo that such a web of cameras could easily track individuals going into or out of “sensitive buildings.” So the reporters looked and did indeed find at least one health clinic that provides abortion services within “unnerving proximity” to some Ring cameras, as well as a legal office handling immigration and refugee cases. Having footage showing individuals going to those sorts of facilities uploaded to a platform like Neighbors and becoming widespread could actually put individuals’ lives in danger.

https://arstechnica.com/?p=1630675

Amazon: Trump used “improper pressure” to block AWS from DOD cloud contract

Enlarge / The JEDI contract is central to DOD’s efforts to rapidly adopt cloud technology. But the winner-take-all contract offer has been controversial from the start—and now Amazon claims President Trump put a whole lot more than a finger on the scales to ensure AWS lost.
Department of Defense

reader comments

143 with 90 posters participating

Share this story

In a redacted filing released today by the US Federal Court of Claims, attorneys for Amazon asserted that Amazon Web Service’s loss of the Department of Defense Joint Enterprise Defense Infrastructure (JEDI) cloud computing contract to Microsoft’s Azure was the result of “improper pressure from President Donald J. Trump, who launched repeated public and behind-the-scenes attacks to steer the JEDI Contract away from AWS to harm his perceived political enemy—Jeffrey P. Bezos, founder and CEO of AWS’ parent company, Amazon.com, Inc. (“Amazon”), and owner of the Washington Post.”

The suit cites Trump’s instructions to former Secretary of Defense James Mattis to “screw Amazon” out of the contract, as recounted by Mattis’ former chief speechwriter, and numerous other incidents of direct interference by Trump in the contract competition, including ordering an “independent” review of the contract by Defense Secretary Mark Esper in

August of 2019.

JEDI was awarded to Microsoft in October. The $10 billion contract is for a DOD-wide enterprise Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service(PaaS) program providing compute and storage services—including delivering them to the "tactical edge," giving troops in the field access to critical data. The initial expenditure, scheduled for the first year of the contract, would be just $1 million—but it would be followed by a base two-year ordering period and up to eight years of optional extensions out to 2029, with a capped value of $10 billion.

- The before (left) and (hopefully) after (right) architecture designs of DOD cloud.
- All sorts of services are supposed to be part of JEDI, at classifications up to Top Secret.
- Only $1 million is guaranteed—so that $10 billion could be a pipe dream if the winner can't deliver.

Because of the scale of the contract, AWS was long assumed to be the front-runner—AWS already provides the DOD with cloud services and other government agencies that meet most of the security requirements set out by the JEDI contract. But Microsoft's Azure was also a strong contender, and the DOD's internal cloud capabilities (provided by the Defense Information Systems Agency) have relied heavily on Microsoft technology. And Amazon's attorneys claim that after Trump injected himself into the procurement discussion, the DOD "took numerous actions to systematically remove the advantages of AWS' technological and experiential superiority and artificially level the playing field between AWS and its competitors, including Microsoft."

The filing cites as an example the DOD's decision in mid-2018 to not evaluate past performance as part of the competition in violation of Federal Acquisition Regulation (FAR)

requirements—when “only AWS possessed [past performance] with regard to a contract remotely comparable to the size and complexity of JEDI.”

“These errors, however, were not merely the result of arbitrary and capricious decision making,” the filing states. “DoD’s substantial and pervasive errors are hard to understand and impossible to assess separate and apart from the President’s repeatedly expressed determination to, in the words of the President himself, ‘screw Amazon.'” As a result, Amazon’s attorneys asserted, “Basic justice requires reevaluation of proposals and a new award decision,” and the court should decide “whether the President of the United States should be allowed to use the budget of DoD to pursue his own personal and political ends.”

https://arstechnica.com/?p=1630099

Bernie Sanders vows to break up huge ISPs and regulate broadband prices

Enlarge / Bernie Sanders speaks to the Organic Farmers Association on December 05, 2019 in Story City, Iowa.
Getty Images | Win McNamee

reader comments

129 with 82 posters participating

Share this story

Presidential candidate and Vermont Senator Bernie Sanders yesterday released a plan to overhaul the US broadband market by breaking up giant providers, outlawing data caps, regulating broadband prices, and providing $150 billion to build publicly owned networks.

“The Internet as we know it was developed by taxpayer-funded research, using taxpayer-funded grants in taxpayer-funded labs,” the Sanders plan said. “Our tax dollars built the Internet, and access to it should be a public good for all, not another price-gouging profit machine for Comcast, AT&T, and Verizon.”

If enacted, Sanders’ “High-Speed Internet for All” plan would be the polar opposite of the Trump administration’s treatment of broadband companies and far more aggressive than the regulatory approach of the Obama administration. Sanders pledged to “use existing antitrust authority to break up Internet service provider and cable monopolies,” specifically by “bar[ring] service providers from also providing content and unwind anticompetitive vertical conglomerates.”

Perhaps most notably, this could force Comcast to divest NBCUniversal and force AT&T to divest Time Warner. Of course, a US president can’t simply issue an order to break up these companies. But if Sanders is elected, he could nominate Department of Justice officials who are likely to file antitrust lawsuits against the companies that dominate the broadband industry.

Bring back Title II regulation

Sanders also pledged to regulate broadband providers as common carriers under Title II of the Communications Act, reinstate net neutrality rules, and impose other pro-consumer rules. This could be achieved via legislation, appointments of

aggressive regulators to the Federal Communications Commission, or a combination of both.

Sanders said he would “eliminate data caps and ban throttling” and “instruct the FCC to regulate broadband Internet rates so households and small businesses are connected affordably.” This would include a requirement “that all Internet service providers offer a Basic Internet Plan that provides quality broadband speeds at an affordable price.”

The FCC is an independent agency, so it wouldn’t have to do what Sanders says. But if Sanders was president, he could nominate commissioners and appoint a chairperson who is likely to carry out his wishes.

$150 billion

Sanders also proposed investing heavily in infrastructure, particularly in government-run networks. He pledged to “provide $150 billion through the Green New Deal in infrastructure grants and technical assistance for municipalities and/or states to build publicly owned and democratically controlled, co-operative, or open-access broadband networks.”

Sanders vowed to preempt 19 state laws that limit the spread of municipal broadband. That could require help from Congress, as the Obama-era FCC’s attempt to preempt such laws was overturned in court.

Presidential candidate Elizabeth Warren has proposed an $85 billion broadband plan, while candidate Joe Biden has proposed $20 billion for rural broadband.

Many US residents lack fast Internet service today because broadband monopolies “don’t provide service to anyone who can’t afford it, or install it in areas where it won’t make them as much money as their shareholders demand,” the Sanders

plan said. Meanwhile, broadband monopolies “exploit their dominant market power to gouge consumers and lobby government at all levels to keep out competition.”

Sanders compared his plan to President Franklin D. Roosevelt’s “promise to deliver electricity to every home in America in 1935, a time when 90 percent of rural households lacked it.”

Sanders’ $150 billion proposal includes a Department of Agriculture Rural Utility Service program “to provide capital funding to connect all remote rural households and businesses and upgrade outdated technology and infrastructure, prioritizing funding for existing co-ops and small rural utilities.” Sanders said that $7.5 billion should be set aside for tribal areas and that all public housing should provide free broadband to residents.

Sanders said the $150 billion investment will “ensure that communities stay connected during natural disasters.” Sanders also proposed a full review of broadband networks to make sure they are “resilient to the effects of climate change.”

Sanders aims to lower prices

US government plans for broadband often focus on network access without talking much about lowering prices. Sanders wants to do both. His plan said:

> *Large Internet service providers have enjoyed government funding, protection from competition, and light regulation while gouging customers with some of the highest prices for service in the world. Bernie will regulate these providers like a utility. The FCC will review prices and regulate rates where necessary, ensuring areas without competition aren’t able to run up prices.*

Moreover, Sanders proposed eliminating the hidden fees broadband providers use to make the actual cost higher than

their advertised rates. ISPs would have to “clearly state the cost of service” and not impose “unexpected rate increases” or “service termination fees.”

Sanders also wants the FCC to define broadband as a minimum of 100Mbps download speeds and 10Mbps uploads, instead of the current 25Mbps down and 3Mbps up. Sanders would also “reinstate and expand privacy protection rules,” reversing the Trump-era decision to eliminate broadband-privacy rules.

https://arstechnica.com/?p=1629483