Some junk for sale on Amazon is very literally garbage, report finds

Enlarge / The Amazon logo at the entrance of a logistics center in France, July 2019.

reader comments

182 with 118 posters participating

Share this story

Some days it seems like searching for an item on Amazon just brings up endless pages of junk with no clear pattern. There's a reason for that, it turns out: dumpster divers are, in fact, literally reselling discarded junk.

Resellers hunt through trash to find and repair treasures, the Wall Street Journal reported today. Those sellers, for understandable reasons, mostly didn't want to talk to the WSJ, so reporters for the paper tried it themselves.

Writers went digging through the trash in New Jersey and came up with dozens of items to sell, such as "a stencil set, scrapbook paper, and a sealed jar of Trader Joe's lemon curd." Setting up a storefront and listing the items for sale was "easy," the WSJ said.

Amazon's screening process seemed to be haphazard, the paper added:

> *After a later dumpster dive, the Journal was able to go through almost all of the listing process with salvaged*

> *breath mints, sunflower seeds, marmalade, crispbread, fig fruit butter, olives, a headband and a Halloween mask—stopping just short of shipping them to the Amazon warehouse, which is required for an item to appear for purchase on the site.*
>
> *To list a sunscreen lotion, Amazon asked for a safety-data sheet. Attempts to list a protein powder, a pea-powder dietary supplement and a face sheet mask—all from the dive—elicited a request from Amazon for proof of purchase.*

Nothing in Amazon's rules prevented "salvaged" items from being resold, at the time. The policies do require that most goods be new, but the rules also allow for certain product categories to be sold used, including books and electronics, as long as those listings are clear about those items being used.

Amazon updated its seller policies after the WSJ contacted the company about this story to include a prohibition on items "intended for destruction or disposal or otherwise designated as unsellable by the manufacturer or a supplier, vendor, or retailer."

"Sellers are responsible for meeting Amazon's high bar for product quality," a company spokesperson told the WSJ, adding that the company was investigating and such stores were "isolated incidents."

Not so high a bar

The Amazon sellers who find and repair or clean and sell usable goods from the trash are not a new phenomenon. Any flea market, secondhand shop, or closeout store features "found" items, some of which genuinely are surprisingly high-quality, like-new finds. These sellers are just taking the business model online.

But consumer expectations at a flea market are very different from consumer expectations at Amazon. Most shoppers are going to expect that an item “fulfilled by Amazon” (as many third-party items are) is delivered by an Amazon Prime-branded van, dispatched from an Amazon warehouse, and actually new—especially when it’s described that way on a product page.

Amazon consumers, though, are increasingly having to get used to shopping at their own risk. Counterfeit items, especially imported ones, are rampant on the site, as are listings for recalled, unsafe, or defective goods.

The WSJ analyzed about 45,000 shopper comments left on product listings in 2018 and 2019 and found 8,400 comments on 4,300 food, makeup, and over-the-counter drug items making reference to “unsealed, expired, moldy, unnaturally sticky, or problematic” goods. Of those 4,300 products, 544 had “Amazon’s Choice” flags promoting them to consumers in search results.

Update: Amazon contacted Ars to repeat the statements it issued to the WSJ. The company also added that any “negligent and potentially illegal activity” by some seller is “unfair to the vast majority” of sellers on the site. Additionally, the company says it has “expanded the scope of our existing supply-chain verification efforts including increased spot checks of source documentation to ensure seller compliance with our policies.”

Amazon also said, “sourcing items from the trash has always been inconsistent with Amazon’s high expectations of its sellers and prohibited by the Seller Code of Conduct on Amazon, which requires that sellers act fairly and honestly to ensure a safe buying and selling experience.”

https://arstechnica.com/?p=1633799

Russian media group Rambler attempting to hold Nginx hostage

Enlarge / This listing image is slightly hyperbolic—Nginx co-founders Sosoev and Konovalov didn't do time in jail, they were "just" detained and interrogated at gunpoint in their homes at 7am local time.

reader comments

86 with 63 posters participating, including story author

Share this story

Maxim Konovalov and Igor Sysoev—founders and creators of the popular Web server software Nginx—were arrested, detained, and interrogated last Thursday. Sysoev's former employer, Rambler—Russia's third-largest Internet company, which occupies a roughly similar position in Russian-language Internet to Yahoo or AOL at their height in the English-speaking world—alleged that it owned the rights to Nginx's source code, due to Sysoev having originally developed it while an employee at Rambler.

In an interview with Meduza.io—a news site focusing on Russian and former Soviet Union reporting—founder Konovalov decried Rambler's move as "a typical racket, simple as that," and he went on to state that no attempt had been made to negotiate with or even notify him or Sysoev before the raid happened. Their first indication of a problem came with the police raids

which detained the two, seized IT equipment from them, and interrogated them early that morning. Konovalov described the raid as “professional and polite, if you exclude the fact that special forces agents were standing around with automatic weapons… then there were interrogations. Generally speaking, the questions weren’t particularly interesting or pleasant.”

Konovalov characterized the move as a money-grabbing shakedown from the current leadership at Rambler, inspired by Nginx’s $670 million acquisition by American tech giant F5 Networks approximately six months earlier.

He told Meduza:

> *Nginx was officially registered in 2011, and it’s now 2019, and in all this time Rambler never raised any issues… there was the deal with F5, the big money became palpable, and then we see the desire to grab a piece of it for themselves. It’s a typical racket. Simple as that.*

Konovalov and Sysoev were not even certain what criminal charges were filed against them. But earlier today, Rambler requested the Russian courts to drop the criminal charges and instead turned to civil litigation. This follows Konovalov’s earlier prediction that the criminal charges were merely being used as an excuse to go on a fishing expedition for leverage to use in a civil case. Rambler further claimed it was cutting ties with the “Lynwood” law firm which had filed criminal charges; but this seems likely to be a move for show only, since Lynwood Investments is tied to Alexander Mamut—a Russian billionaire who is co-owner of Rambler itself.

A simple cash grab?

Although Nginx co-founder Konovalov characterizes the move by Rambler as a simple cash grab inspired by Nginx’s $670 million acquisition, the potential ramifications are far wider-

reaching than ~42 billion rubles in cold hard cash. A successful, retroactive acquisition of the rights to Nginx would not just give Rambler access to that cash—it would also provide the ability to declare the entire open source license of the Nginx platform invalid.

This would, in turn, open up effectively the entire developed world's tech industry to shakedowns for licensing fees—both for continued operation, and in theory, retroactively for more than a decade of "unlicensed" usage.

Since the Nginx license was a weak, permissive license—largely akin to the BSD license, requiring nothing but acknowledgement of the original copyright notice in source code and documentation—Nginx has not just proliferated directly as a Web server used on general purpose computers but also as a key embedded component of many other solutions. For instance, Symantec's Blue Coat appliances, Sophos' Email Appliances, and Netflix's Open Connect Appliances all depend on Nginx.

Moving back to "simple" software deployments, UK Internet services company Netcraft lists Nginx as the single-most common Internet-facing Web server on the planet in its Q3 2019 Web server survey, with more than 31 percent of all sites surveyed detected as Nginx. Filtering to only "active" sites seemingly reduces Nginx to the second-most common server, with Apache at 30 percent and Nginx at 20 percent. But this conveniently ignores a whopping 37 percent of "other" results, representing Web servers locked down in production too tightly to be easily classified. Many of those "other" servers will also be Nginx or Nginx derivatives.

Enlarge / As of December 2019, Nginx is even more popular than Apache. Netcraft confirms it.

If Russian courts were to grant a civil victory to Rambler and award it ownership of the rights to Nginx, the sweeping impact on the entire global technical industry is difficult even to estimate. A simple self-hosted blog might be able to swap out Nginx for Apache in a few hours. A more complex and heavily optimized site, designed to field a lot of traffic, might get back on its feet nearly as quickly but operate at reduced capacity for a week.

Meanwhile, the industry giants which depend on Nginx include Facebook, Netflix, and WordPress. Add in Cloudflare‘s Content Distribution Network and DDoS protection service, and it becomes easier to discuss what portion of the Internet *wouldn’t* stop working without Nginx than which ones would.

It seems difficult to believe that this fact is lost on the Rambler executives who initiated this grab. But it also seems difficult to believe that the rest of the world would tolerate it and honor a Russian-court decision with such far-ranging effects. Adding to the already ham-handed obviousness of the grab—which comes more than a decade after Nginx established itself as both a service company and a significant part of the global Internet infrastructure—Igor Ashmanov, a Rambler chief

executive from the time Sysoev worked at the company, declared on Facebook that “developing software wasn’t part of [Sysoev’s] job description at all,” and “Rambler [probably can’t] come up with a single piece of paper, never mind a non-existent task to develop a web server.”

This author believes that it would be difficult to find a court outside Russia’s direct control that would issue injunctions based on such a decision which would necessarily bind the entire visible Internet from operation. As dark as politics has become, I believe sanctioning corruption this immediately and obviously visible and damaging to both tech industry giants and everyday citizens—No cat memes today? No pictures of each others’ lunches? Sacrilege!—would represent immediate political suicide no elected official would likely believe they could ignore.

https://cms.arstechnica.com/?p=1633471

Amazon bans third-party merchants from shipping with FedEx

Enlarge / Amazon’s going to need some bigger boxes to ship those Outpost racks next year.

reader comments

135 with 107 posters participating

Share this story

If you’re cramming last-minute Christmas or Hanukkah shopping online ahead of next week’s holidays, and it absolutely, positively has to be there overnight, don’t count on FedEx being the service to get it there for you. Not only is Amazon no longer working with the carrier, but now third-party merchants are banned from using the service, too.

The Wall Street Journal obtained a copy of a message Amazon sent to its third-party vendors Sunday night explaining the prohibition. Starting this week, marketplace vendors offering Prime shipments will not be allowed to use FedEx Ground or Home services. This ban will persist “until the delivery performance of these ship methods improves.”

Third-party retailers accounted for about 58% of Amazon’s retail activity in 2018, company CEO Jeff Bezos said earlier this year, and sold a cumulative $160 billion worth of goods. The vendor marketplace is on track to be at least as large a share of Amazon’s retail business in 2019.

FedEx ended its last domestic contract with Amazon in August in part due to that in-house business. “High-volume shippers such as Amazon “are developing and implementing in-house delivery capabilities and utilizing independent contractors for deliveries, and may be considered competitors,” FedEx wrote in an investor document earlier this year. The company added that Amazon in particular is “investing significant capital to establish a network of hubs, aircraft, and vehicles.”

A FedEx representative told the WSJ that the impact to the shipping firm is “minuscule,” while admitting that Amazon’s directive “limits the options for those small businesses on some of the highest shipping days in history.”

Marketplace sellers selling items marked for Amazon Prime delivery can use UPS services, FedEx’s Express service (which

is pricey), or Amazon’s own in-house logistics business (which the company heavily encourages vendors to use). That encouragement is so heavy, in fact, that at least one merchant has complained to Congress that the shipping business should be considered one of Amazon’s many potential antitrust violations.

https://cms.arstechnica.com/?p=1633491

Controversial sale of .org domain manager faces review at ICANN

reader comments

73 with 55 posters participating

Share this story

ICANN is reviewing the pending sale of the .org domain manager from a nonprofit to a private equity firm and says it could try to block the transfer.

The .org domain is managed by the Public Internet Registry (PIR), which is a subsidiary of the Internet Society, a nonprofit. The Internet Society is trying to sell PIR to private equity firm Ethos Capital.

ICANN (Internet Corporation for Assigned Names and Numbers)

said last week that it sent requests for information to PIR in order to determine whether the transfer should be allowed. “ICANN will thoroughly evaluate the responses, and then ICANN has 30 additional days to provide or withhold its consent to the request,” the organization said.

ICANN, which is also a nonprofit, previously told the Financial Times that it “does not have authority over the proposed acquisition,” making it seem like the sale was practically a done deal. But even that earlier statement gave ICANN some wiggle room. ICANN “said its job was simply to ‘assure the continued operation of the .org domain’—implying that it could only stop the sale if the stability and security of the domain-name infrastructure were at risk,” the Financial Times wrote on November 28.

In its newer statement last week, ICANN noted that the .org registry agreement between PIR and ICANN requires PIR to “obtain ICANN’s prior approval before any transaction that would result in a change of control of the registry operator.”

ICANN can raise “reasonable” objection

The registry agreement lets ICANN request transaction details “including information about the party acquiring control, its ultimate parent entity, and whether they meet the ICANN-adopted registry operator criteria (as well as financial resources, and operational and technical capabilities),” ICANN noted. ICANN’s 30-day review period begins after PIR provides those details.

Per the registry agreement, ICANN said it will apply “a standard of reasonableness” when determining whether to allow the change in control over the .org domain. As Domain Name Wire noted in a news story, whether ICANN can block the transfer using that standard “might ultimately have to be

determined by the courts."

The agreement between PIR and ICANN designates PIR as the registry operator for the .org top-level domain. It says that "neither party may assign any of its rights and obligations under this Agreement without the prior written approval of the other party, which approval will not be unreasonably withheld."

Concern about price hikes, transparency

The pending sale comes a few months after ICANN approved a contract change that eliminates price caps on .org domain names. The sale has raised concerns that Ethos Capital could impose large price hikes.

ICANN says it wants to make the transaction-review process more transparent. But ICANN apparently needs PIR's permission to publish the request for information and PIR's responses, and so far PIR has refused a request to make documents public. In last week's letter to PIR and the Internet Society, ICANN General Counsel and Secretary John Jeffrey urged PIR to make the information public:

> *As you are well aware, transparency is a cornerstone of ICANN and how ICANN acts to protect the public interest while performing its role. In light of the level of interest in the recently announced acquisition of PIR, both within the ICANN community and more generally, we continue to believe that it is critical that your Request, and the questions and answers in follow up to the Request, and any other related materials, be made public.*
>
> *While PIR has previously declined our request to publish the Request, we urge you to reconsider. We also think there would be great value for us to publish the questions that you are*

> *asked and your answers to those questions. We will of course provide you with the opportunity to redact portions of the documents that you believe contain personally identifiable information before posting and renew that offer here.*
>
> *As you, [ISOC CEO] Andrew [Sullivan], stated publicly during a webcast meeting in which you participated on 5 December 2019, you are uncomfortable with the lack of transparency. Many of us watching the communications on this transaction are also uncomfortable.*
>
> *In sum, we again reiterate our belief that it is imperative that you commit to completing this process in an open and transparent manner, starting with publishing the Request and related material, and allowing us to publish our questions to you, and your full responses.*

We contacted PIR today and the organization said it isn't able to comply with the request to make documents public because of confidentiality agreements. PIR told Ars:

> *PIR is committed to being transparent with ICANN and the Internet community, and PIR is working to answer ICANN's questions and address why this acquisition will be good for the .org community. But like any company in the middle of an acquisition, and consistent with other changes of control that have been reviewed by ICANN, we are limited in what we can release publicly due to confidential[it]y agreements with other parties and proprietary information involving the transaction.*

PIR defends sale

PIR CEO Jon Nevett defended the pending sale in a blog post last week, calling it "the best path for .org's future."

"[A] diversified portfolio is much better, and less risky,

than relying on one company like Public Interest Registry—in one industry—for nearly all of its funding," Nevett wrote.

Under the Internet Society's ownership, PIR has "been in perpetual 'harvest' mode, where PIR sends the fruits of our labor to support the amazing work they do," Nevett continued. "A relationship with Ethos will allow us to invest in .org, enabling us to deliver more to the .org community, and the Internet at-large."

But critics of the sale want guarantees in writing that the new owner won't impose big price increases. ICANN's Noncommercial Stakeholders Group (NCSG) has called on the ICANN board to require public-interest protections in the sale. For example, the NCSG said that before any wholesale price increases, .org domain registrants should be given "six months to renew their domains for periods of up to 20 years at the pre-existing annual rate."

Ethos Capital should also have to commit to content neutrality with a pledge that it "will not suspend or take away domains based on their publication of political, cultural, social, ethnic, religious, and personal content, even untrue, offensive, indecent, or unethical material, like that protected under the US First Amendment," the NCSG said.

If Ethos Capital refuses to make those commitments, ICANN should "exercise its right" from the registry agreement to withhold its approval, the NCSG said.

When contacted by Ars, PIR said that its existing agreement with ICANN "requires that PIR provide notification six months in advance of any price increase" and that "PIR under new ownership will honor the terms of that contract." However, PIR did not commit to accepting the NCSG proposals.

https://cms.arstechnica.com/?p=1633441

This alleged Bitcoin scam looked a lot like a pyramid scheme

reader comments

86 with 62 posters participating

Share this story

The world of cryptocurrency has no shortage of imaginary investment products. Fake coins. Fake blockchain services. Fake cryptocurrency exchanges. Now five men behind a company called BitClub Network are accused of a $722 million scam that allegedly preyed on victims who thought they were investing in a pool of bitcoin mining equipment.

Federal prosecutors call the case a “high-tech” plot in the “complex world of cryptocurrency.” But it has all the hallmarks of a classic pyramid scheme, albeit with a crypto-centric conceit. Investors were invited to send BitClub Network cash, which would allow the company to buy mining equipment—machines that produce bitcoin through a process called hashing. When those machines were turned on, all would (in theory) enjoy the spoils. The company also allegedly gave rewards to existing investors in exchange for recruiting others to join. According to the complaint, the scheme began in April 2014 and continued until earlier this month.

Matthew Brent Goettsche, Jobadiah Sinclair Weeks, and Silviu Catalin Balaci are accused of conspiracy to commit wire fraud and conspiracy to offer and sell unregistered securities. A fourth defendant, Joseph Frank Abel, faces only the latter charge. Another unnamed defendant remains at large. Balaci's name was redacted from one public version of the indictment, but appeared on another.

The scheme appears to have started as a relatively modest scam and spiraled dramatically in ambition. Internal messages between the conspirators give the impression of growing glee at the ease of taking advantage of investors, referring to "building this whole model on the backs of idiots." The men allegedly described their victims as "dumb" investors and "sheep."

"They were not wrong," Emin Gun Sirer, the CEO of blockchain startup Ava Labs, quipped on Twitter.

In October 2014, a few months after BitClub Network was founded, Goettsche allegedly posted about the need to "fak[e] it for the first 30 days while we get going," instructing a co-conspirator to do some "magic" on the company's revenue numbers. They allegedly agreed on a method of cooking the numbers that would include inconsistencies to make sure they appeared real. The tricks swiftly became more daring. Later, Goettsche allegedly suggested the company "bump up the daily mining earnings starting today by 60%."

https://arstechnica.com/?p=1632539

Feds reap data from 1,500 phones in largest reported reverse-location warrant

Enlarge / You’re not the only one looking at your phone’s location history.

reader comments

78 with 58 posters participating

Share this story

Federal investigators trying to solve arson cases in Wisconsin have scooped up location history data for about 1,500 phones that happened to be in the area, enhancing concerns about privacy in the mobile Internet era.

Four Milwaukee-area arsons since 2018, as yet unsolved, have resulted in more than $50,000 of property damage as well as the deaths of two dogs, Forbes explains. In an attempt to find the person or persons responsible, officers from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) obtained search warrants to gather data about all the devices in the area at the time.

The two warrants Forbes obtained together covered about nine hours’ worth of activity within 29,400 square meters—an area a smidge larger than an average Milwaukee city block. Google found records for 1,494 devices matching the ATF’s parameters and sent the data along.

While this is far from the first search to demand a wide swath of data in a given geographic location, Forbes notes, this is

the highest number of results such a geofenced search has so far produced. Not only is that a whole lot of potentially unrelated data for investigators to sort through, but it's also possible that the search will prove entirely fruitless, as whoever committed the crimes may not have a phone, may not have brought it with them, or may have brought it with them in airplane mode or powered off.

The big net

The concept behind such a request is straightforward: you can't track the phone of a suspect you don't have, but you can start with the time and place the crimes were committed and look to see who was there. With that information in hand, they can drill down, as Forbes explains:

> *[T]he police give Google a timeframe and an area on Google Maps within which to find every Google user within. Google then looks through its SensorVault database of user locations, taken from devices running the tech giant's services like Google Maps or anything that requires the "location history" feature be turned on. The police then look through the list, decide which devices are of interest to the investigation and ask for subscriber information that includes more detailed data such as name, email address, when they signed up to Google services and which ones they used.*

While the ability to go through data that way might be handy for law enforcement, some privacy experts are not on board. Such a request "shows the unconstitutional nature of reverse location search warrants because they inherently invade the privacy of numerous people, who everyone agrees are unconnected to the crime being investigated, for the mere possibility that it may help identify a suspect," Jerome Greco, a public defender in the Digital Forensics Unit of the Legal Aid Society, told Forbes.

Google told Forbes it tries to protect individual users' privacy when it receives such a request, saying, "We only produce information that identifies specific users when we are legally required to do so." The company does have a history of trying to push back on overly broad reverse-location requests, Forbes notes. For example, when federal investigators wanted information on devices in a 400-meter radius around a bank robbery earlier this year, the company convinced them to drop that to a 50-meter radius.

Users who disable Google's location history features should, in theory, not have data in Google's SensorVault for the company to pass along to investigators. That said, Google is facing multiple lawsuits, including a potential class-action in the US and a suit by consumer protection regulators in Australia, alleging the company misled users and retained location data even if the setting was turned off.

https://arstechnica.com/?p=1632383

FCC's "illogical" claim that broadband isn't telecommunications faces appeal

Enlarge / The Federal Communications Commission seal hangs inside a meeting room at the headquarters ahead of an open commission meeting in Washington, DC, on Thursday, December 14, 2017.

Getty Images | Bloomberg

reader comments

56 with 49 posters participating

Share this story

Mozilla and other organizations today appealed the court ruling that upheld the Federal Communications Commission's repeal of net neutrality rules, arguing that the FCC's claim that broadband isn't telecommunications should not have been accepted by judges.

The FCC repeal was upheld in October by a three-judge panel at the US Court of Appeals for the District of Columbia Circuit. The court had some good news for net neutrality supporters because it vacated the FCC's attempt to preempt all current and future state net neutrality laws. But Mozilla and others aren't giving up hope on reinstating the FCC rules nationwide.

The Mozilla petition filed today asks for an *en banc* rehearing of the case involving all of the DC Circuit judges. Mozilla is probably facing an uphill battle because the three-judge panel unanimously agreed that the FCC can repeal its own net neutrality rules.

Joining Mozilla in the appeal were online companies Etsy and Vimeo, industry lobby group Incompas, and the Ad Hoc Telecom Users Committee, which represents business users of communications services. The case is known as *Mozilla v. FCC*.

Another appeal was filed today by several advocacy groups, namely New America's Open Technology Institute, Free Press, Public Knowledge, the Center for Democracy & Technology, the Benton Institute for Broadband & Society, the Computer & Communications Industry Association, and the National Association of State Utility Consumer Advocates. Another appeal was filed by the National Hispanic Media Coalition,

and another by Santa Clara County, San Francisco, the California Public Utilities Commission, and the National Association of Regulatory Utilities Commissioners.

Mozilla wrote in a blog post today:

> *Mozilla's petition focuses on the FCC's reclassification of broadband as an information service and on the FCC's failure to properly address competition and market harm. We explain why we believe the court can in fact overturn the FCC's new treatment of broadband service despite some of the deciding judges' belief that Supreme court precedent prevents rejection of what they consider a nonsensical outcome. In addition, we point out that the court should have done more than simply criticize the FCC's assertion that existing antitrust and consumer protection laws are sufficient to address concerns about market harm without engaging in further analysis. We also note inconsistencies in how the FCC handled evidence of market harm, and the court's upholding of the FCC's approach nonetheless.*

Judge blasted FCC but upheld repeal

Circuit Judge Patricia Millett, one of the three judges who decided the case, wrote that the FCC's justification for classifying broadband as an information service instead of a telecommunications service "is unhinged from the realities of modern broadband service." But the FCC has broad authority to classify offerings as either information services or telecommunications, as long as it provides a reasonable justification for its decision, and judges said they had to leave the net neutrality repeal in place based on US law and Supreme Court precedent.

Obviously, consumer advocacy groups are arguing that judges didn't have to give the FCC so much deference.

“Although the court came to the right conclusion on some key issues, such as the FCC’s lack of authority to preempt state net neutrality rules, in other ways it gave the FCC the benefit of the doubt too many times,” Public Knowledge Legal Director John Bergmayer wrote today. “While agencies should be given deference where appropriate, they do not have the authority to rewrite the law or come to illogical, results-driven conclusions.”

The FCC argued that broadband isn’t telecommunications because Internet providers also offer DNS (Domain Name System) services and caching as part of the broadband package. Millett wrote that this interpretation “confuse[s] the leash for the dog,” but ruled in the FCC’s favor because of the Supreme Court’s 2005 decision in the *Brand X* case, which let the FCC classify cable broadband as an information service. *Brand X* “compels us to affirm as a reasonable option the agency’s reclassification of broadband as an information service based on its provision of Domain Name System (‘DNS’) and caching,” Millett wrote.

Circuit Judge Robert Wilkins agreed with Millett’s assessment. Senior Circuit Judge Stephen Williams didn’t join Millett and Wilkins in this line of criticism, but he joined them in upholding the repeal. Williams wanted to uphold the other big portion of the FCC order, too, as he dissented from a 2-1 decision to vacate the FCC’s preemption of state laws.

The advocacy groups’ petition argued that judges “misconstrued *Brand X* as precluding any judicial review of the reasonableness of classifying a service that overwhelmingly offers telecommunications as an information service simply because it includes DNS and caching.”

If the court decides not to grant the request for a re-hearing of the case, petitioners could appeal to the Supreme Court.

The FCC could also appeal, since judges ruled against the

commission on its attempt to preempt state laws. Today is the deadline for filing appeals at the DC Circuit court, and we'll update this story if the FCC submits one.

https://arstechnica.com/?p=1632575

AT&T doesn't want you to see its slow Internet speed-test results

Getty Images | Steven Puetzer

reader comments

121 with 83 posters participating

Share this story

AT&T doesn't want its home Internet speeds to be measured by the Federal Communications Commission anymore, and it already convinced the FCC to exclude its worst speed-test results from an annual government report.

"AT&T this year told the commission it will no longer cooperate with the FCC's SamKnows speed test," The Wall Street Journal wrote in an investigative report titled "Your Internet provider likely juiced its official speed scores."

AT&T already convinced the FCC to exclude certain DSL test results from last year's Measuring Broadband America report.

The reports are based on the SamKnows testing equipment installed in thousands of homes across the US.

“AT&T was dismayed at its report card from a government test measuring Internet speeds” and thus “pushed the Federal Communications Commission to omit unflattering data on its DSL Internet service from the report,” the Journal wrote.

“In the end, the DSL data was left out of the report released late last year, to the chagrin of some agency officials,” the Journal wrote. “AT&T’s remaining speed tiers notched high marks.”

Pai’s FCC gives less attention to speed tests

The Obama-era FCC began the Measuring Broadband America program in 2011 to compare the actual speeds customers receive to the advertised speeds customers are promised. The FCC released reports annually through 2016, but the testing program has gotten less attention since Ajit Pai became chairman in January 2017.

As we wrote in November 2018, the FCC hadn’t yet released any new Measuring Broadband America reports since Pai became chair. Pai’s FCC in December 2018 finally released both the 2017 and 2018 reports, tucking them into the final appendices of a larger “Communications Marketplace Report.” You can see all the Measuring Broadband America results from over the years at this page.

The 2017 report includes two categories for AT&T, one for its oldest DSL technology and another for its DSL-based IP broadband with speeds of up to 45Mbps. While AT&T’s oldest DSL service only provided 82 percent of advertised download speeds, AT&T IP broadband was over 100 percent. The 2018 report only includes AT&T’s IP broadband category, leaving out

the company’s worst results.

Satellite Internet provider ViaSat also “left the FCC’s program” last year, the Journal wrote. ViaSat results were included in the 2018 report, which covers tests from September 2017.

We asked the FCC yesterday if it will include any AT&T and ViaSat test results in future reports, since SamKnows testing equipment could still be in AT&T and ViaSat customer homes, and we asked when the next Measuring Broadband America report will come out. We’ll update this article if we get any answers.

AT&T says its own speed test is better

AT&T defended its decision to drop out of FCC testing when contacted by Ars. “AT&T developed a best-in-class tool to measure its consumer broadband services,” the company said in a statement provided to Ars. “This tool measures performance on all AT&T IP broadband technologies and is more accurate, versatile, and transparent. For these and other reasons, our tool provides better and more useful information to our customers.”

But consumers have less reason to trust a speed-test tool created by AT&T than one created by the FCC. Even with the FCC’s speed tests, AT&T was able to exclude unflattering results. It would be even easier to dump slow speed-test results when AT&T is the one determining which numbers to show the public.

AT&T and the mobile industry’s top lobby group have also argued that carriers shouldn’t have to submit detailed 5G maps to the FCC. Separately, the FCC said this month that Verizon, T-Mobile, and US Cellular exaggerated their 4G coverage in

official government filings.

Back in 2011, AT&T touted the FCC’s in-home speed tests as being far more accurate than previous testing methodologies. But the company’s opinion then seems to have been influenced by early test results that AT&T said showed “consumers are getting high-quality broadband services from their ISPs.”

https://arstechnica.com/?p=1632455

Wave of Ring surveillance camera hacks tied to podcast, report finds

Enlarge / An Amazon Ring security camera on display during an unveiling event on Thursday, Sept. 20, 2018.

reader comments

58 with 45 posters participating

Share this story

A series of creepy Ring camera intrusions, including one where a stranger sang to an 8-year-old child and said he was Santa Claus, may be linked through a forum and associated livestream podcast, a new report finds.

The cluster of hacks, first reported by local media outlets, have become national news in the past few days. In all the

cases, some bad actor accessed indoor Ring cameras (not doorbells) and used them to harass, intimidate, or attempt to extort the residents.

One family in Florida suddenly heard racist commentary about their teenage son coming from their Ring camera on Sunday night. On Monday, someone yelled at a couple in Georgia to "wake up." Another family, in Tennessee, heard a voice taunting their daughter through a camera in their kids' room on Tuesday. And in Texas yesterday, someone tried to demand a ransom to exit the household camera system, telling the homeowners to pay 50 bitcoin (roughly $360,000).

In all the cases, the residents stopped the intrusions by unplugging or removing the batteries from their devices, successfully cutting off access to them.

In response to the incidents, Ring said it had not suffered any kind of breach or intrusion and urged subscribers not to use account credentials that could have been stolen in one of the thousands of other data breaches that happen in any given year. That's excellent advice for all services, as far as it goes, as is enabling two-factor authentication on any service that supports it (which Ring does), particularly as cameras have been easy targets for years. In at least one instance, however, the camera owner said her Ring account used a specific passphrase she has not associated with any previous accounts.

Nulled

Cheap tools for accessing Ring illicitly are plentiful and easy to get, reporters for Vice Motherboard found yesterday. The reporters also found a reason so many incidents using those tools are popping up all at once: the NulledCast.

The NulledCast is livestreamed on Discord, Motherboard explains, and it's connected to the forum (also called Nulled)

where the tools for accessing Ring cameras are sold and traded. Motherboard continues:

> *"Sit back and relax to over 45 minutes of entertainment," an advertisement for the podcast posted to a hacking forum called Nulled reads. "Join us as we go on completely random tangents such as; Ring & Nest Trolling, telling shelter owners we killed a kitten, Nulled drama, and more ridiculous topics. Be sure to join our Discord to watch the shows live."*

Motherboard was able to see a message from a now-deleted thread saying, in part, "Hello everyone. As you probably have heard, I was featured on the news for a stunt I pulled," apparently linked to one of the media reports. The national spotlight is, however, more attention than the Ring hackers apparently wanted to draw. Motherboard found that, since yesterday, posts in the forum relating to Ring hacking have apparently been deleted, as has some content from the Discord server.

As of Wednesday, members of the server insisted that the livestream would be continuing with another installment on Friday. Earlier this afternoon, however, Motherboard reporter Joseph Cox (no relation) said on Twitter that Discord banned the server and all its users. That said, the Internet being what it is, they are likely to pop up somewhere else before long.

https://arstechnica.com/?p=1632059

---

988 will be the new 911 for suicide prevention—by sometime in 2021

reader comments

49 with 42 posters participating

Share this story

The Federal Communications Commission plans to designate 988 as the short dialing code for the United States' suicide-prevention hotline. Much like 911 for general emergencies, 988 could be dialed by anyone undergoing a mental health crisis and/or considering suicide.

The National Suicide Prevention Lifeline can already be reached at 1-800-273-8255 (or 1-800-273-TALK), but the FCC today gave preliminary approval to a plan that would make 988 redirect to that hotline. The commission's unanimous vote approved a Notice of Proposed Rulemaking (NPRM) that seeks public comment on the plan.

Once the NPRM is published in the Federal Register, there will be a 60-day period for taking public comments, and the FCC would finalize the plan after considering the public input. It could take another 18 months after that to implement 988 nationwide, depending on what requirements the FCC imposes on phone providers.

The 1-800-273-8255 hotline "provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week," its website

says. Callers are connected to one of "163 crisis centers funded by the Department of Health and Human Services' Substance Abuse and Mental Health Services Administration," the FCC said. "In 2018, trained Lifeline counselors answered over 2.2 million calls and over 100,000 online chats."

The 988 proposal was spurred by Congress, which last year passed a law directing the FCC to examine the technical feasibility of designating "a simple, easy-to-remember, 3-digit dialing code" for the hotline.

Before today's vote, FCC Chairman Ajit Pai said that "988 has an echo of the 911 number we all know as an emergency number, and we believe that this 3-digit number, dedicated for this purpose, will help ease access to crisis services. It'll reduce the stigma surrounding suicide and mental health conditions. And it'll ultimately save lives."

18-month deadline up for debate

The proposal would require all telecommunications carriers and interconnected VoIP providers to support 988 on their networks within 18 months, the FCC said. But the FCC noted that it is "seek[ing] comment on all aspects of implementation, including whether a longer or shorter timeframe would be needed to make 988 a reality." Based on the comment-period length and proposed implementation time frame, 988 would be implemented nationwide sometime in late 2021.

The FCC's NPRM explained:

> *We believe this time frame would provide sufficient time for providers to make any necessary changes to equipment and software and to institute new dialing requirements, if necessary. To begin with, we understand that modern IP switches can already accommodate 988 today or do so with minor software updates. In this regard, we observe that most providers are already actively upgrading their equipment to*

> *IP technology given the technological advances in the marketplace and the advanced services that consumers are demanding. Moreover, we believe that 18 months is sufficient time to upgrade the approximately 12 percent of legacy switches that will need such upgrades and we anticipate that the majority of technical upgrades necessary to switches and systems can be done in parallel with other work to implement 988.*

FCC Commissioner Jessica Rosenworcel said the public comment period will help the FCC fine-tune details of the plan. “How we implement this matters. So we ask for input on the details to get this done, including just how calls will be routed and how to implement the three-digit code in areas where it is already used at the start of a seven-digit telephone number,” she said.

https://arstechnica.com/?p=1632027