Amazon delivery contractors operate with little oversight, report finds

reader comments

106 with 70 posters participating

Share this story

Amazon has seemingly been bringing shipping services in-house as rapidly as it can as the company ramps up efforts to get packages to Prime members in just one day. But although those ubiquitous gray-blue vans and uniformed drivers all have Amazon branding on them, at least 250 subcontracted companies around the country actually do all the heavy lifting—a system that allows Amazon to skirt liability when heavy pressure on drivers means disaster strikes, according to a new report.

The company has actively encouraged employees to quit their jobs and go start local delivery firms it can contract with. Operating under heavy pressure to make as many deliveries as possible, as quickly as possible, and with lax regulatory oversight, drivers delivering items for Amazon have been involved in "hundreds" of crashes and other incidents in the past five years, BuzzFeed News reports. At least six people have been killed in those incidents, including a 10-month-old baby.

Amazon-branded services now deliver about half of all the company's last-mile shipments, bringing goods from the local warehouse to your doorstep. The US Postal Service and UPS

between them handle a large chunk of the other half. Professional commercial delivery businesses, such as UPS and FedEx, are subject to heavy federal regulation, and their commercial vehicles are subject to regular safety inspections. But the same is not true for Amazon.

The “sprinter” style vans Amazon delivery services use fall just under the weight limit that would subject them to Department of Transportation oversight, BuzzFeed notes. Amazon purchased about 20,000 of those vans from Mercedes-Benz last year, which it leases to the companies that deliver its goods. The vans are subject to yearly state safety inspections, as are passenger vehicles in most states, but the vehicles are not held to the same inspection, repair, and maintenance standards as a UPS truck would be.

“We have invested tens of millions of dollars in safety mechanisms across our network, and regularly communicate safety best practices to drivers,” Amazon told BuzzFeed. “We are committed to greater investments and management focus to continuously improve our safety performance.”

Spotty records

Safety training is also much more rigorous at the big delivery firms. Applicants and employees face drug testing and must pass entrance exams before being hired. “Even the most minor fender benders trigger internal investigations that seek to identify who was at fault and how such accidents can be avoided in the future,” BuzzFeed observes.

In some cases, though, it seems like almost anyone with a driver’s license can get a job delivering Amazon packages. Some of the lawsuits filed against the company after crashes have identified drivers who had previous convictions for traffic infractions. One former employee of an Amazon delivery firm told BuzzFeed that in his first week of training, the driver he was shadowing first backed into a light post before

speeding away, then he later blew through several stop signs and ultimately ran a red light before crashing into a motorcyclist going the other way. The driver at the time had been pulled over several times in the previous eight years, BuzzFeed found: twice for going more than 20 miles per hour over the posted speed limit, and once for running a stop sign.

The former employee told BuzzFeed that he quit on his first day of driving solo after completing his training. “I thought, ‘No, this is crazy. I had 160 packages and it was raining, you can’t even see,’” he told BuzzFeed. “I took the truck back and went and told the guy, ‘This is it. I’m done.’”

The companies also face little oversight for their own bad practices, BuzzFeed reports. Amazon contracts with at least a dozen companies that BuzzFeed identified as being “repeatedly sued or cited by regulators for alleged labor violations, including failing to pay overtime, denying workers breaks, discrimination, sexual harassment, and other forms of employee mistreatment.” Two drivers working for an Amazon delivery company in the Los Angeles area told BuzzFeed they were encouraged to skip meals, use bottles instead of taking real bathroom breaks, and not to wear seat belts (which are required in California) in order to move faster.

The outsourcing problem

Amazon has a whole lot of company in relying on a shadowy network of third-party companies to do business under its brand banner. A huge number of “employees” for most tech firms are in fact employees of contracting firms.

“Gig economy” businesses such as Uber and Lyft infamously classify the people doing the work for them as independent contractors, not as employees of the company, but plenty of full-time workers for big-name tech firms are also actually working for staffing firms or smaller intermediaries.

The work of content moderation in particular tends to be outsourced to third-party firms. Several reports in recent years have exposed the poor working environments and lack of support the workers, who try to keep large platforms such as YouTube and Facebook useable, encounter trying to do the job.

More than half, about 54%, of Google's worldwide workforce are in fact not Google employees at all, and these workers do not receive the same levels of pay or extensive benefits. Frustration from that workforce, more than 90,000 strong, bubbled over earlier this year, resulting in Google requiring all the firms it contracts with to offer a $15 minimum wage, paid sick days, health benefits, paid parental leave, and tuition reimbursement benefits. About 90 contract workers for Google in Pittsburgh, actually employees of a company called HCL America, voted just before Labor Day to unionize.

Drivers for one Amazon delivery firm did attempt to unionize in 2017, BuzzFeed reports. Detroit-area workers for Silverstar Delivery voted 22-7 to join the Teamsters. Within weeks of the vote, the drivers reported to the National Labor Relations Board that they had been fired in retaliation for joining the union. (The NLRB dismissed the retaliation charge, but it did ultimately settle with Silverstar for more than $15,000 to settle other claims of anti-union activity.) A few months later, Silverstar shut down its Michigan operation entirely.

Not long after, Amazon held a meeting in Chicago with management from local delivery firms. "The whole purpose of the meeting was to say to you, 'Here's how to not get unionized. Because if you do, we pretty much don't want anything to do with a union," one attendee told BuzzFeed.

https://arstechnica.com/?p=1561557

How the NFL—not the NSA—is impacting data gathering well beyond the gridiron

reader comments

14 with 12 posters participating

Share this story

Video shot and edited by Christopher Schodt.

SANTA CLARA, Calif.—As guards were going so far as to check inside NFL fans' wallets as part of routine security measures before a recent preseason game at Levi's Stadium, a different form of surveillance was taking place on the inside of the San Francisco 49ers' one-year-old, $1.3 billion home here in Silicon Valley.

We're not talking about facial recognition devices, police body cams, or other security measures likely zeroing in on fans. Instead, employees from San Jose-based Zebra Technologies had recently finished scanning the NFL uniforms of the 49ers and of their opponents—the Dallas Cowboys. All of a sudden, an on-the-field *de facto* surveillance society was instantly created when Zebra techies activated nickel-sized Radio Frequency Identification Device (RFID) chips that were fastened inside players' shoulder pads. Every movement of every player now could be monitored within an accuracy level of all but a few inches.

On its surface, this seems pretty innocuous. Cameras already track things like total player movement in sports, allowing teams to better recognize tendencies or gauge the physical toll on players. RFID chips, however, can provide more accurate, more granular information along these lines. The

NFL’s new real-time player tracking data—including things such as player speed and team formations—undoubtedly promises to reformat the game in terms of fan participation, team practicing methods, and potentially game-time strategy.

There’s a larger story playing itself out as well. The league’s RFID initiative may push far beyond the gridiron.

That’s because this so-called geo-fencing technology has a geekier side, and it will likely recast things like fantasy football, the Microsoft’s Xbox One experience, and perhaps even the Madden NFL video game produced by Electronic Arts. What’s more, the technology potentially opens up new proposition gambling bets in Las Vegas sports books or other gambling venues. But its most unexpected impact will have nothing to do with sports at all. Fortune 500 companies are watching the NFL closely, examining how they might incorporate the RFID chip to monitor every move of their onsite employees from the construction site, the office, and beyond.

- This is where the RFID device is hidden on both sides of an NFL player’s shoulder pads.
  Christopher Schodt
- From left to right, the evolution of Zebra Technologies’ RFID device attached to NFL players.
  Christopher Schodt
- Zebra Technologies techies manning in-stadium game day operations.
  Christopher Schodt
- In the bowels of Zebra Technologies’ off-stadium data center in San Jose, California.
  Christopher Schodt
- A close view of one of 20 onsite RFID receivers at Levi’s Stadium that triangulates player movements with the ability to do so from as far as 1,000 feet.
  Christopher Schodt
- A panoramic view of one of 20 onsite RFID receivers that

triangulates player movements.
Christopher Schodt

- Television viewers will be seeing this MPH stat more and more.
  Zebra Technologies
- Television viewers will also often see replay images showing the actual distance and path a player ran.
  Zebra Technologies
- This photo shows the passing routes traveled during a play.
- A big-board computer monitoring screen at Zebra Technologies' control center in San Jose, California.
  Christopher Schodt
- Some live action, pre-season football between the Dallas Cowboys at San Francisco 49ers on August 23, 2015.
  Christopher Schodt

Game day

Starting this week, this is the first NFL season in which all NFL stadiums are outfitted with cigar-box-sized receivers across the venue to triangulate the players' movements. These devices can track the players from up to 1,000 feet away, and at Levi's Stadium, there are 20 of these receivers. Players and the field officials are tracked at least 15 times a second. The technology can even tell which way a player is facing in real time.

For now, the ball isn't being tracked like it was in World Cup soccer matches last year. The NFL test-tracked the pigskin in last year's Pro Bowl (the NFL equivalent of an all-star game), but American football isn't like soccer. If the ball crosses the goal line in soccer, it's a goal. In the NFL, action is dead and spotted wherever the ball is being carried when the ball carrier's knee hits the ground when tackled. So while the NFL has instant replay to help officials, it isn't about to

automate or dehumanize the game's officiating any further.

"We're not looking to replace officials with robots," Matt Swensson, the NFL's senior director of emerging technology, told Ars.

According to Zebra, here's the data being tracked in real time:

- Player participation.
- Player groupings.
- Play formation and route running.
- Player speed.
- Player separation from another player.
- Yards player ran in a game, yards run before and after catch, yards run by quarter. Virtually an unlimited variety of relevant distance data in real time.

And here are all the technical specifications (PDF) of Zebra's player tracking system and servers.

"Basically, we can take all of the specifics that are tracked in a game and automate them," Jill Stelfox, a Zebra general manager, told Ars. So in total, 2 to 3 gigs of data are generated per game under the current operation. However, the NFL for the moment is keeping most of the data under lock and key—and won't even disperse it among the league's own teams.

"Right now we're still working through the proper distribution model of the data. We're not just handing it over to the clubs to go through," the NFL's Swensson said.

Why keep everything centrally? It's a combination of preparedness and competition. If the data is provided in real time to coaches during a game, that could influence the outcome, Swensson said. Coming up with the appropriate distribution channels and security measures for such a setup will require time and energy, and the NFL isn't ready to go to

that stage yet.

“Ultimately, we want the game to be fair and balanced,” Swensson said.

NFL teams can take advantage of this surveillance during practice. Only three teams currently do, according to Zebra’s Stelfox: the 49ers, Detroit Lions, and New Orleans Saints.

Sean Payton, the Saints’ head coach, said it only makes sense to surveil practices via RFID.

“For us it is distance, workload, travel, all of those things. Zebra has been great to work with. We think it is helpful for us to monitor workload,” Payton said on the Saints’ website. He said he is able “to look for the exceptions when you are

studying numbers. You are able to study and see maybe something that is unusual that stands out." For example, Stelfox told us a story about Zebra's technology discovering that running back Reggie Bush, now of the 49ers, was running about 7 to 8 miles per practice.

"Why practice at that level? You can burn out," Stelfox said.

Stelfox showed Ars some of the real-time data generated during last year's Super Bowl on condition that it not be published. Looking through information collected, you could easily determine that when a certain player lined up in a certain spot, he was almost guaranteed to get the ball. So while top-level game film and old-school coaching could catch that, so does the Zebra technology—and it does so instantly.

"It's super valuable data," Stelfox said.

For now, fans watching on television will be some of the primary beneficiaries of the NFL's great data experiment. Broadcasters can instantly get a limited amount of real-time data to provide viewers—like how far and how fast a player ran and the route taken.

But by making even this tiny of a fraction of data *public,* there are grand implications.

Listing image by Zebra Technologies

http://arstechnica.com/?p=735643

Unlicensed signal boosters

get a boost from Amazon

Enlarge / You really can find anything in a stock image library: “Antennas of mobile cellular systems with Wi-Fi hot spot repeater and blue sky.”
Just_One_Pic / Getty Images

reader comments

13 with 13 posters participating

Share this story

Cell phone signal boosters are powerful devices. Installed in a home or office, they can potentially amplify one signal bar into five. In rural areas with poor cell coverage, or in buildings where signals have trouble penetrating, they can be lifesavers, providing reliable access to communication networks and emergency services.

But boosters also have a dark side: If misconfigured or poorly manufactured, they can knock out service for everyone who happens to be nearby. That’s why the Federal Communications Commission began regulating the devices five years ago. Today, all consumer signal boosters sold and marketed in the United States must meet the agency’s strict technical standards. Doing so can get expensive, and many FCC-authorized boosters cost hundreds or even thousands of dollars. Ecommerce sites like Amazon offer cheaper options. The only problem is, they’re not always compliant.

The FCC requires booster manufacturers to get their products certified as safe, and it publishes each valid certification

on its website. WIRED found a number of sellers offering boosters on Amazon that are not listed as certified by the FCC. Their models often cost less than $200, compared to $300 or more for FCC-certified versions. A number of them have been top sellers in the signal booster category, and some are promoted with a badge reading “Amazon’s Choice.”

“We’ve reached out to Amazon multiple times to inform them that these products are not legal for being sold in the US,” says Laine Matthews, the vice president for business at SureCall, an American signal booster manufacturer. “And it hasn’t yielded results.” Amazon removed some listings after WIRED reached out for comment this week.

Uncertified signal boosters are sold on other websites, but Amazon is by far the largest ecommerce platform where US consumers can purchase them. The company still dominates online shopping in the US, and it’s so successful in part because of the millions of independent merchants who also sell goods on its marketplace. But lawmakers, consumer advocates, and other businesses have raised concerns about Amazon’s oversight, and problems like counterfeit items. The company has rolled out some programs designed to police third-party vendors, but they don’t catch everything. A recent *Wall Street Journal* investigation found thousands of items for sale that were unsafe or banned by regulators. FCC-noncompliant signal boosters similarly pose risks. They can be an enormous nuisance to wireless carriers who have to track them down, and when they disrupt service, people might not be able to reach 911 in an emergency.

“Selling partners are required to comply with all relevant laws and regulations when listing items for sale in our stores,” an Amazon spokesperson said in a statement. “Those who do not will be subject to action, including potential removal of their account. The products in question have been removed.” WIRED had sent Amazon a list of the vendors it discovered, rather than individual product listings. As of

publication time, all six sellers could be found on its website selling signal boosters. When asked about this, Amazon responded with another statement: “We use a variety of methods to ensure that the products sold in our stores are compliant with applicable laws and meet our Amazon polices [sic]. We expand these tools every day, and our dedicated teams constantly review and refine our policies.”

The FCC did not return a request for comment.

Amazon’s booster bazaar

Sina Khanifar wasn’t surprised when the booster he ordered on Amazon recently turned out to be unauthorized. He’s the cofounder of RepeaterStore, which also sells boosters online, including on Amazon. The model he says he ordered, a 700MHz booster from a company called Anntlent, came with a certification, but for an entirely different product. Still, the item was labeled “Amazon’s Choice.” (Lawmakers have asked Amazon to explain how it makes this designation.)

If Khanifar tried to register the unauthorized booster with his carrier, it may not have permitted him to use it. The FCC requires everyone register their boosters—including older models purchased before its rules went into effect in 2014 and were grandfathered in. If Khanifar ran the booster anyway and it caused interference, his wireless carrier or the FCC could come to his house and ask him to shut it down. Either way, it would mean he spent nearly $200 on a device he wasn’t permitted to actually use.

Khanifar believes Amazon could be doing more to help consumers. “Amazon should at least require people to list the FCC ID on the page very clearly,” he says.

WIRED found six third-party vendors on Amazon selling signal boosters that when cross-referenced with the FCC’s database appear to be unauthorized, including KKBSTR, SH·W·CELL,

HJCINTL, Phonelex, Subroad, and MingColl. Each one had associated trademarks registered to an individual or company located in China.

Many sellers were appropriating reviews from other Amazon products, a common tactic used by sellers to make their goods appear more popular than they actually are. “This is the second time I purchased these curtains. I love them,” one reviewer supposedly said about a Phonelex booster, for example, that has since been removed. On the Amazon page for a since-deleted HJCINTL device, a number of reviews referenced replacement wheels for rolling suitcases. One five-star review of a SH·W·CELL booster said “I absolutely love my new bling case for my iPhone 7 plus!” The manufacturers themselves are difficult to reach, and don’t appear to have company websites.

In reviews that appeared to actually be about signal boosters, some customers noted the boosters had caused interference issues. “ATT service tech knocked on my door and said this unit screwed up three cell towers in my area,” one review for a MingColl device reads. “He said it was not FCC passed and was a bootleg from China.” In a one-star Amazon review of a booster from the company Phonetone, that has since been removed from Amazon’s site, a man named Scotty Wideman said that a representative from AT&T came to his house and “informed us this booster was interfering with their tower and if we didn’t turn it off the FCC would be contacting us.” AT&T declined to comment.

“Improperly configured signal boosters can affect mobile networks, which is why we encourage customers to contact us for help finding a solution that works, like our free Personal CellSpot with unique software that won’t interfere with the broader network,” a T-Mobile spokesperson said in a statement. Sprint didn’t comment in time for publication.

Legitimate manufacturers say they have tried alerting Amazon to the noncompliant boosters on its marketplace for over a

year. “It creates a bad name for our industry and it takes away sales for companies that are doing the right thing,” SureCall’s Matthews says. He says he has tried contacting Amazon numerous times, including sending a letter to the company’s legal department, but has only received boilerplate responses in return. Khanifar, the other booster seller, says he has also reached out to Amazon and received no response.

The issue isn’t limited just to the US, either. Earlier this year, the Cellular Operators Association of India, a trade group representing the wireless industry, asked Amazon and other ecommerce sites to stop selling illegal signal boosters, according to local news reports. In a letter sent in response, Amazon argued that sellers and buyers were responsible for any legal obligations, and that it was merely functioning as a marketplace. This is a common refrain from the company.

Can you hear me now?

Dennis McColl has been at Verizon for over 20 years. As an associate fellow in its radio frequency systems group, which is responsible for solving issues like network interference, he says he’s seen plenty of noncompliant boosters. They can cause two types of problems. If the two ends of the device aren’t far enough apart, they can get into a feedback loop, like what happens when a microphone gets too close to a speaker, which causes the booster to malfunction.

The bigger issue for carriers is thermal noise, a byproduct the boosters give off. Signal boosters “take this thermal noise and amplify the bejesus out of it,” says McColl. “If it’s really far away, then all of this noise is dissipated before it gets to the cell site.” But if a booster is too close to a cell tower, that excess noise can cause massive interference, since it’s been amplified thousands of times. It makes calls drop, and other people in the area lose service.

The rules enacted by the FCC in 2014 were meant to prevent

this. The new Network Protection Standard it introduced is “a series of technical safeguards designed to minimize potential for Consumer Signal Boosters to cause interference in wireless networks.” It requires boosters to automatically shut down when they get into a feedback loop, as well as when they’re too close to cell towers, among other restrictions.

But outdated signal boosters are still out there, as well as illegal ones purchased on sites like Amazon. That means Verizon and other carriers continue to discover them causing interference, typically when engineers notice an unusual uptick in things like dropped calls in a certain area. Sometimes when Verizon builds new wireless infrastructure, McColl says, it discovers new boosters that until then had been too far away to cause problems. Technicians then have to go into the field and decipher where the problem is coming from. McColl says he’s knocked on hundreds of people’s front doors and asked them politely to please turn off their noncompliant boosters. “I always approach it as if you’re making friends.”

This story first appeared on Wired.com. Is there something about Amazon you think WIRED should know? Contact the author at louise_matsakis@wired.com or via Signal at 347-966-3806.

https://arstechnica.com/?p=1560847

GirlsDoPorn.com faces trial for allegedly filming 22

women under false pretenses

Anca Gabriela Rafan / EyeEm / Getty

reader comments

173 with 84 posters participating, including story author

Share this story

Almost two dozen women say they were tricked into appearing in pornographic videos on the prominent porn site GirlsDoPorn. They sued the owner of the site, Michael Pratt, for fraud in 2016. The trial began in mid-August and is expected to run for more than a month.

One of the victims wrapped up her testimony in a San Diego courtroom on Monday.

“If I had known that they were posting it on the Internet, that my name would be attached to it, that it would be in the United States,” the woman identified as Jane Doe 15 said in court, according to the Daily Beast. “If I had known that it was more than 30 minutes of filming, if I had known any of that, just any one of those, I wouldn’t have done it.”

The victims of the alleged scheme were young women aged 18 to 23 who initially responded to online ads for clothed modeling gigs. But no such opportunities materialized. Instead, they were contacted by men who encouraged them to appear in a pornographic video.

Most of the women were reluctant, but they were offered as much as $5,000 for 30 minutes on camera—an offer that some women found hard to refuse. Women say they were told that the videos would only be distributed on DVDs outside the United

States.

The plaintiffs say that this was all lies. The men planned to post the videos directly to the GirlsDoPorn website—as well as uploading shorter clips to free porn sites like PornHub and YouPorn. After they had traveled to San Diego, the women say they were pressured to sign lengthy contracts before they had time to read them carefully. Women were told they would receive less than the agreed-upon price—in one case, $3,000 rather than $5,000—because the men were "disappointed" with their appearance.

A woman says she was paid to lie to other women

To assuage their fears, prospective women were connected with other women to serve as references and reassure them that the videos wouldn't appear online. Some had shot their own videos so recently that they hadn't yet been posted online. But others were women who had never shot their own videos, but they were instead paid to say otherwise.

In a court declaration, one of the women said that Andre Garcia—the male talent in a number of the videos and a central figure in Pratt's operation—"coached me on how to correspond with the prospective women to gain their trust, even if that included telling lies and hiding information."

She said Garcia encouraged her to "tell the prospective women that I too had previously filmed a video for them, even though I had never done so." She was also coached "to tell the women that I come from a small town, shot a video for them, that no one has found out, and that the women had nothing to worry about, and to tell prospective women the videos they filmed would never be released in the United States or on the Internet."

She said she was paid $50 to $200 for each call she took from women, depending on the attractiveness and age of the women.

“This ruined my life”

The women’s videos generally appeared on the GirlsDoPorn site under a pseudonym, but this provided little protection. Inevitably, someone who knew the woman would notice the video and share it. It then circulated rapidly among the woman’s real-life friends and acquaintances.

After this happened to Jane Doe 15, she texted a woman who had helped convince her to do the video.

“Hey, you lied to me, and they lied to me,” she wrote in a text message. “It’s on a website now and my whole town back home knows. This ruined my life.”

This didn’t just lead to embarrassment with friends and family—it could also lead to harassment by strangers, the plaintiffs point out.

“Since being launched in 2009, GirlsDoPorn has grown in popularity and generated a cult-like following of hobbyists/stalkers who obsess over the amateur women featured in the videos,” the plaintiffs wrote in a legal filing. “Dozens of websites, forums, and message boards exist dedicated solely to publishing victims’ real names, hometowns, social media accounts, photographs, and other personal information.”

Indeed, the plaintiffs say Pratt and his associates directly contributed to this stalker-like behavior. In July 2015, personal information about numerous GirlsDoPorn victims was published on a website called pornwikileaks.com, a site that specializes in publishing personal information about pornographic actresses.

Later the same year, the plaintiffs say, “administrative

control of pornwikileaks.com was transferred to a person using the email address mike@bll-media.com—a known email used by Pratt." Afterwards, "none of the information regarding defendants' victims was taken down, and in January 2016, advertisements for GirlsDoPorn with hyperlinks began appearing in posts on PornWikileaks.com." According to the lawsuit, personal information about women appearing in GirlsDoPorn videos was only removed in mid-2016—after women filed their lawsuit.

On Thursday, porn site Bang Bros purchased control of PornWikileaks and shut it down—promising that it would never again host personal information about porn actresses. It's not clear who Bang Bros paid for the domain or how much money changed hands.

Lawyers for the plaintiffs say they have personally talked to well over 100 women who have complaints similar to the 22 women who filed lawsuits. However, they say many other women are afraid that defendants will do everything they can to embarrass women who come forward—asking intrusive questions about their personal lives, seeking to strip them of anonymity, and even seeking permission to show the women's pornographic videos in open court. This week, a judge rejected a request by defendants to play one of the women's GirlsDoPorn videos during the trial.

https://arstechnica.com/?p=1560683

President Trump tweets

picture of sensitive satellite photo of Iranian launch site

Enlarge / I guess it’s not classified anymore.
National Reconnaissance Office?

reader comments

363 with 163 posters participating

Share this story

President Donald Trump posted a photo today via Twitter of Iran’s Imam Khomeini Space Center in northern Iran, showing the damage done to the facility by the explosion of what appears to have been a Safir rocket during launch. The rocket was apparently being used in the attempted launch of Iran’s Nahid-1 satellite.

Commercial satellite imagery from Planet Labs made available this morning showed a plume of smoke rising from the space center’s launch pad. But the photo posted by President Trump was a much higher-resolution, black and white photo—a resolution that suggested it came from a National Reconnaissance Office satellite.

> *The United States of America was not involved in the catastrophic accident during final launch preparations for the Safir SLV Launch at Semnan Launch Site One in Iran. I wish Iran best wishes and good luck in determining what happened at Site One.* ***pic.twitter.com/z0iDj2L0Y3***
>
> *— Donald J. Trump (@realDonaldTrump)* ***August 30, 2019***

While the posted photo was obviously not at full resolution—and was partially obscured by the reflection from the flash for the phone camera used to capture it—it showed details clearly at well below a meter's resolution. NRO satellites are known to have a resolution in approximately the tenth of a meter range, like the imagery shared in the Twitter post.

This afternoon, CNN's Barbara Starr reported that a US official had confirmed the photo came from a National Reconnaissance Office satellite.

This is not the first time President Trump has instantly declassified intelligence information that reveals capabilities or sources. In May of 2017, President Trump shared sensitive intelligence from a foreign partner on ISIS with Russia's ambassador and Foreign Minister in an Oval Office visit. As President, Trump is the ultimate classification authority, so he can declassify anything he feels is necessary

https://arstechnica.com/?p=1560787

Ring reportedly shared video sharing data, detailed maps with police in 2018

Enlarge / A map showing the approximate location of the 405 police departments working with Ring as of August 30, 2019

reader comments

13 with 11 posters participating

Share this story

Ring, Amazon’s home security camera and surveillance company, has since 2018 rapidly expanded its business by partnering with more than 400 police and sheriff departments nationwide. Amid a growing chorus of privacy complaints and media reports about these partnerships, Ring has repeatedly promised explicitly that police have no way of knowing details of who has the cameras installed and what residents are—or aren’t—willing to share their footage. New reports, however, indicate that police departments may be receiving more data about Ring users in their jurisdictions than previously disclosed.

Gizmodo reports today that documents it obtained from a Florida police department included emails from Ring “about the number of times residents had refused police access to their cameras or ignored their requests altogether.”

Owners of Ring devices can connect them to an app called Neighbors, which is also available for the general public to use. The app collects “crime reports” from participants, who can also choose to upload images and video either directly from their Ring devices or uploaded from other sources.

Police who partner with Ring have access to a sort of companion portal, which among other things, allows them to send out an email blast to all Neighbors members in a specific area asking them to share footage captured during a window of time as part of an investigation. “Law enforcement agencies who participate in the Neighbors app must go through the Ring team when making a video request to customers,” a Ring representative told Ars earlier this week. “Customers can choose to opt out or decline any request, and law enforcement

agencies have no visibility into which customers have received a request and which have opted out or declined."

Ring representatives have been pushing "engagement" hard on the police departments they work with, and the data obtained by Gizmodo makes it easy to see why. The police department in question issued 22 requests for footage between May and September 2018, Gizmodo found, leading to 319 distinct emails being sent to residents asking them to hand over footage. They received permission to access a total of 11 files, a 3.5% success rate.

Gizmodo notes that customers seemed intuitively to understand that the "do not share" option in the emails they received was not worth the effort: exactly zero recipients of the email clicked the button, instead simply ignoring or deleting the email 308 times.

In one email, a Ring manager admitted more granular data could be helpful. "Did one person share 11 videos or did 11 people share one video each," the manager wrote. "We will have a better idea after we collect more data."

Ring now keeps statistical data of this type to itself, the company told Gizmodo. "This is not representative of our current policies or the current video request process," the company said. "Ring does not provide video request data to law enforcement agencies."

Now you see it…

Ring doesn't like for its law enforcement partners to share information about the portal back-end with the public. Cnet last week published a roundup of those features Ring might wish to keep quiet, including a "heat map" showing where police could find active Ring devices in their area. Ring told Ars on Wednesday that it "recently updated the steps law enforcement partners take" to request video during an

investigation, and, “as a result, there is no device density heat map” available any longer.

While heat maps may no longer be available, however, at one time Ring did indeed provided detailed maps to its partners. The Guardian obtained documents it published today showing the evolution of the agreement between Ring and Gwinnett County, Georgia, just outside of Atlanta.

Ring approached the Gwinnett police in August 2018, The Guardian found, and the agreement was approved by the police in May of this year. The records show that Ring heavily edited the press release Gwinnett authorities used to discuss the deal, as seems to be standard for these arrangements.

During those months, Ring also provided the Gwinnett police with a map showing the locations of “hundreds” of Ring devices within the county borders

The Electronic Frontier Foundation calls Ring “a perfect storm of privacy threats.”

“The rapid proliferation of this partnership between police departments and the Ring surveillance system—without any oversight, transparency, or restrictions—poses a grave threat to the privacy of all people in the community,” the EFF said. “The growing partnerships between Amazon and police departments corrodes trust in an important civic institution by turning public servants into salespeople for Amazon products.”

https://arstechnica.com/?p=1560667

Comcast, beware: New city-run broadband offers 1Gbps for $60 a month

You can check out any time you'd like, but you can never… well, you know the song.
Aurich Lawson

reader comments

102 with 77 posters participating

Share this story

A municipal broadband service in Fort Collins, Colorado went live for new customers today, less than two years after the city's voters approved the network despite a cable industry-led campaign against it.

"Finally, a broadband provider you can trust," the city-run broadband service's website says in a pointed message about the Comcast cable and CenturyLink DSL services that are the city's primary broadband networks.

Fort Collins Connexion, the new fiber-to-the-home municipal option, costs $59.95 a month for 1Gbps download and 1Gbps upload speeds, with no data caps, contracts, or installation fees. There's a $15 monthly add-on fee to cover Wi-Fi, but customers can avoid that fee by purchasing their own router. Fort Collins Connexion also offers home phone service, and it plans to add TV service later on.

Connexion is only available in a small portion of the city right now.

“The initial number of homes we’re targeting this week is 20-30. We will notify new homes weekly, slowly ramping up in volume,” Connexion spokesperson Erin Shanley told Ars. While Connexion’s fiber lines currently pass just a small percentage of the city’s homes and businesses, Shanley said the city’s plan is to build out to the city limits within two or three years.

“Ideally we will capture more than 50% of the market share, similar to Longmont,” another Colorado city that built its own network, Shanley said. Beta testers at seven homes are already using the Fort Collins service, and the plan is to start notifying potential customers about service availability today.

The city reportedly issued $143 million in bonds to finance the city-wide network. Fort Collins has a population of 165,000.

Ballot question

In November 2017, voters in Fort Collins approved a ballot question that authorized the city to build the broadband network.

The Colorado Cable Telecommunications Association (CCTA), of which Comcast is a member, donated $815,000 toward a campaign against the ballot initiative. The Chamber of Commerce also opposed the plan. Comcast didn’t participate in the campaign publicly, but the company would have been the main beneficiary of a vote against the municipal option.

In all, the industry-led opposition spent more than $900,000 fighting the ballot question, while the pro-broadband group led by residents spent about $15,000.

Before the election, a study by a pro-municipal broadband group estimated that “Competition in Fort Collins would cost

Comcast between $5.4 million and $22.8 million per year.”

Net neutrality, competitive prices

Fort Collins Connexion promises to follow net neutrality principles, saying it will not “intentionally block, slow down, or charge money for specific websites and online content.”

The municipal ISP’s privacy pledge says that it does not “share, distribute, or sell a User’s specific Internet usage history, call history, voicemail, or other electronic data generated from a User’s Internet and phone Service to any external third party.”

Connexion’s website is advertising only two residential Internet packages, the $59.95 gigabit plan and a 10Gbps plan for $299.95 a month. Shanley told Ars that “there are no taxes and fees on Internet service,” aside from the optional $15 charge to use city-provided Wi-Fi hardware instead of a customer-purchase router.

Connexion offers a gigabit Internet and phone service bundle for $74.90 a month. Phone service on its own starts at $19.95 a month. When TV service is available, there will be an Internet and TV bundle for $119.90 a month, and a bundle of all three services starts at $144.85.

Connexion’s prices are competitive. Looking at Comcast’s website for offers in Fort Collins today, we found a $60 monthly price for download speeds of up to 400Mbps, and $70 a month for 1Gbps. But those Comcast prices are only good for two years and would automatically rise after the promotional period. Comcast charges early termination fees, and the company says that equipment fees, taxes, other fees, and “applicable charges” may be added to the advertised price. Comcast’s modem/router gateway costs $13 a month.

Besides that, Comcast’s cable upload speeds are a fraction of download speeds, and Comcast enforces a 1TB monthly data cap in Colorado and many other states. Comcast charges $10 for each additional block of 50GB used after a customer hits 1TB, or $50 extra per month for unlimited data.

Comcast potentially offers lower prices than Connexion for lower-speed plans, but even then it’s hard to do better than the city-run option. We found an offer in Fort Collins of 60Mbps download speeds for $29.99 a month from Comcast, but the price rises to at least $59.95 after a year. Another offer for 15Mbps download speeds has the same $29.99 monthly price for the first year and rises to 51.95 afterward.

But again, these advertised prices don’t include extra taxes and fees, data cap charges, and the mental cost of dealing with Comcast’s customer service. Comcast may also charge installation fees of up to $90 depending on which package you buy.

Although Connexion is only available to a small portion of Fort Collins so far, residents who advocated for the network are excited that it’s now a reality.

“All in all, it’s remarkably neat to see this all come to fruition after our four-year journey with all of its ups and downs,” Colin Garfield of the Fort Collins Citizens Broadband Committee told Ars. “It’s my hope that other communities across the country will be inspired by the muni fiber hotbed that is now northern Colorado (Fort Collins, Loveland, Estes Park, Longmont). I’m excited to use my newfound gig speed to cancel Comcast.”

https://arstechnica.com/?p=1560555

Rash of ransomware continues with 13 new victims—most of them schools

reader comments

53 with 40 posters participating, including story author

Share this story

As investigations into a massive, coordinated ransomware attack against local governments in Texas continues, 13 new victims of ransomware attacks have been publicly identified. Most of them are school districts, thought the victims also include an Indiana county, a hospice in California, and a newspaper in Watertown, New York.

The ransomware involved in the Texas attacks, which hit 22 local-level government entities, has not yet been identified. Multiple sources have suggested that the Texas attacker gained access through a managed service provider that the local governments all had in common, but that has not been confirmed by state officials.

In the case of this latest batch of attacks, Ryuk ransomware has been identified as the malware used on at least three occasions. The victims, based on data collected by the threat research group at cloud security firm Armor, include:

- Lake County, Indiana
- Rockville Center School District in Rockville Center, New York
- Moses Lake School District in Moses Lake, Washington

(the attack apparently occured in July but was only reported as ransomware this month
- Mineola Public Schools in Mineola, New York
- The Stevens Institute of Technology in Hoboken, New Jersey
- New Kent County Public Schools in New Kent, Virginia
- Nampa Idaho School District, Nampa, Idaho
- Middletown School District, Middletown, Connecticut
- Wolcott Public Schools, Wolcott, Connecticut
- Wallingford School District, Wallingford, Connecticut
- New Haven Public Schools, New Haven, Connecticut
- The Watertown Daily Times in Watertown, New York
- Hospice of San Joaquin, San Joaquin, California

Pay after pay

According to a report in Newsday, the Rockville Center School District initially received a ransom demand of $176,000. The district's insurance company negotiated with the ransomware operator, reducing the payout to $88,000. The school district paid a deductible of $10,000.

There's no word on whether other victims have paid the ransom yet.

As new attacks become public, it's worth remembering the fallout from such attacks can add up quickly in terms of dollars and require a lengthy recovery period. The leadership of Baltimore City—hit by a ransomware attack in May—recently announced that $6 million of the money needed to cover the city's more than $10 million ransomware cleanup operation would be pulled from funds earmarked for upkeep of city parks and public facilities. So far, the RobbinHood ransomware cost the city over $8 million in lost revenue and interest on deferred revenue.

Baltimore is also now considering a contract for a $20 million "cyber liability" insurance plan. A vote on the proposed

$835,000 contract was deferred until next week.

Add it up

Enlarge / A map of reported US ransomware attacks this year provided by Armor,
This brings the total known, *publicly reported* ransomware attacks this year alone to 149, 30 of which have involved educational institutions. As Ars reported in May, school districts are a particularly easy target for ransomware operators because of their low budget for information technology and limited security resources. According to Armor's data, schools have become the second-largest pool of ransomware victims—slightly behind local governments and closely followed by healthcare organizations.

But these numbers only include publicly reported incidents. Just this week, for instance, CNN reported Percsoft and Digital Dental Record, two companies that handle online services in the dental industry, told roughly 400 customers

that the software they use to connect to individual offices had been infected with ransomware earlier in the week. Dental administrators told CNN they couldn’t access basic information such as patient charts, X-ray data, or payment services. Digital Dental provided a statement saying 100 of the affected practices had been restored this week.

As this incident emphasizes, many ransomware attacks initially go unreported, particularly those against small and mid-sized companies who largely turn to insurers to help them pay off attackers quietly. That distinction may help explain why, in its 2018 Internet crime report, the FBI reported a total of 1,493 ransomware cases last year.

“Just like municipalities, which rely on critical systems to manage records and revenue in a community, school districts host data and systems critical to their community and its students,” said Chris Hinkley, head of Armor’s Threat Resistance Unit security team. “Thus, hackers know that schools cannot afford to shut down, that budgets are typically stretched thin, and that they often have few security protections in place, all aspects which make them a viable target.”

Again, outside of Rockville, there is no word yet whether any of the other new public organizations targeted have cyber insurance or plans to pay ransoms. The payouts ransomware operators have recently received from similar targets—such as Rockville Center School District’s $88,000 payment, Riviera City, Florida’s $600,000 ransom and Lake City, Florida’s $500,000 ransom—”have signaled to the hackers that impacting entire communities can be very lucrative,” Hinkley noted.

https://arstechnica.com/?p=1560491

Trump admin. announces plan to kill 2016 methane emissions limits

Enlarge / In some cases, stray methane is burned to limit how much escapes into the atmosphere.

reader comments

4 with 4 posters participating

Share this story

The Trump administration today announced a new proposal to reverse Obama-era regulations that limit how much methane, a potent greenhouse gas, the oil and natural gas industries are allowed to emit.

The Environmental Protection Agency's proposed amendments would "remove unnecessary regulatory duplication" put into place in 2016, according to a press release. The proposals made today are separate from and in addition to a 2018 proposed rule that eased methane reporting and monitoring requirements for oil- and gas-extraction businesses.

The proposed plan (PDF) would "rescind emissions limits for methane from the production and processing segments of the industry," the EPA says. The proposal would also remove parts of the transmission and storage segments of the oil and gas industry—generally called the midstream business—from being subject to regulation, by claiming the agency was out of line when it added sources such as transmission compressor stations, pneumatic controllers, and underground storage vessels to the rule.

The agency estimates an additional 370,000 short tons of methane would be released into the atmosphere by 2025, as compared to leaving the 2016 rule in place, as well as 10,000 short tons of volatile organic compounds and 300 short tons of "hazardous air pollutants."

The increased emissions would also result in a loss to "total present value of climate benefits" between $2.3 million and $8.1 million per year, the EPA says. The removal of methane emissions caps would, however, save the oil and natural gas sector $17-$19 million per year ($97-$123 million by 2025), the EPA estimates, or about 0.07% of the US industry's $28 billion net income for 2018.

The proposal "delivers on President Trump's executive order and removes unnecessary and duplicative regulatory burdens from the oil and gas industry," EPA head Andrew Wheeler said in a statement. "The Trump administration recognizes that methane is valuable, and the industry has an incentive to minimize leaks and maximize its use."

But what is "clean air," really?

Methane is an incredibly potent greenhouse gas, with roughly 30 times more heat-trapping potential than carbon dioxide. At least one study has found that the EPA likely dramatically underestimates how much methane is released in the production of oil and natural gas.

In addition to seeking to roll back methane emissions limits, the agency is asking for "alternative interpretations of EPA's legal authority to regulate pollutants" under the terms of the Clean Air Act.

The EPA says that its predecessors in 2016 took the position that the agency was not required first to make a "separate, pollutant-specific determination" that methane and other greenhouse gases produced by the oil and natural gas industry

“cause, or significantly contribute to, air pollution that may endanger public health or welfare.” In the current proposal, the EPA seeks comment on whether it was right to do so in 2016 and—if it should have made a separate, pollutant-specific determination—if methane would qualify.

The proposal also seeks comment on the “appropriate criteria to use” in the future when trying to determine if a specific pollutant from a particular source—like methane produced by the extraction industry—could be “reasonably anticipated” to endanger public health and the environment.

The proposed amendments will face a 60-day public comment period from the time they are published in the Federal Register, after which the EPA will make any revisions it deems necessary and then can issue a final rule. The agency also said it will hold a public hearing on the proposal at a time and in a place yet to be announced.

https://arstechnica.com/?p=1559821

Court: Girl broke child porn law by texting explicit video of herself

Erikona / iStock / Getty

reader comments

56 with 42 posters participating

Share this story

Maryland’s law against distributing child pornography applies even when the person distributing a pornographic video is the video’s minor subject, Maryland’s highest court ruled on Wednesday in a 6-1 vote.

The girl, identified only as “S.K.” in court documents, was 16 years old when she performed oral sex on an unidentified male. The act was captured on video—he appears to have been holding the camera—and S.K. shared the video with two friends via a text message. She eventually became estranged from one of the friends, a 17-year-old boy, and he showed the video to a police officer at the school.

The government charged the girl as a juvenile for distributing child pornography and displaying an obscene item to a minor. She was ultimately found to be involved in delinquent acts on both charges—the juvenile equivalent of a criminal conviction.

Because she was a minor, the girl didn’t face prison time. But she was placed on a year’s probation.

The girl appealed the decision, arguing that the state’s child pornography law was designed to protect minors from sexual exploitation. S.K. argued that she wasn’t exploited—and that it was nonsensical to prosecute someone for exploiting herself.

But the majority of the Maryland Court of Appeals—the state’s highest court—was unconvinced. The court ruled that the statute banned all distribution of child pornography, with no exception for cases where the pornographer and the victim was the same person. The majority admitted that the outcome was unfortunate, but they argued that it was up to the legislature—not the courts—to change the law.

One judge dissented

One of the court's judges, Michele Hotten, dissented, arguing that the judges were misreading the law. The law says that "a person may not cause, induce, solicit, or knowingly allow a minor to engage as a subject in the production of obscene matter." It also says that a person may not "photograph or film a minor engaging" in "sexual conduct."

Hotten argued that it makes sense to read "a person" and "a minor" as different people because someone can't "induce" or "solicit" herself to do something. In her view, that means a minor can't break the law by filming herself engaged in sexual acts—because if she's the "minor" in the statute then the "person" must be someone else.

She argues that this interpretation of the law is more consistent with the intent of the Maryland legislature, which was aiming to protect minors from sexual exploitation during the production of child pornography. But the girl in this case doesn't seem to have been sexually exploited, and she certainly didn't sexually exploit herself.

It's not clear if anyone else will be charged in the case. By the time S.K. was charged, the video of her performing oral sex had begun to circulate more widely around her high school. She says she only shared the video with her two friends, which implies one of them shared the video with others. That itself could be a violation of laws against the distribution of child pornography.

This week's ruling also doesn't mention whether authorities have identified the boy receiving oral sex in the video who reportedly was holding the camera. It's not clear if he was an adult or a juvenile at the time of their sexual encounter.

Officials have been struggling with this kind of issue across the country. On Thursday, the Chicago suburb of Naperville

agreed to pay a $250,000 settlement to the parents of a 16-year-old boy who killed himself shortly after harsh interrogation about reports that he had shown sexually explicit material to other students on his iPhone.

According to the *Chicago Tribune*, “police later determined his recording contained audio of a consensual sexual encounter, and there were no illegal images on the boy’s phone.” But by then it was too late—the boy had already thrown himself off the top of a parking structure and fallen to his death.

https://arstechnica.com/?p=1559899