Evacuation of village near explosion of nuclear cruise-missile engine called off

reader comments

49 with 32 posters participating, including story author

Share this story

In the wake of an apparent explosion of the nuclear-powered engine of an experimental cruise missile, the Russian government has reportedly evacuated residents of a nearby village. According to local media, residents of Nyonoska, the site of a Russian missile testing facility, were told to evacuate and that a “special” passenger train would move residents to a safe distance during some sort of military operation—possibly an effort to retrieve the nuclear reactor involved in the accident. But just hours before that evacuation was to take place, the Russian government cancelled the operation.

On August 13, Russian news outlet TV 29 reported that residents of Nyonoska were saying that they had been told they would be evacuated from 5am to 7am local time today, in what TV 29 jokingly referred to as “a new stage in the development of Arctic tourism.” Authorities in Severodvinsk told Interfax that the movement of civilians was because of “planned activities” at the Nyonoska testing range. But that evening, acting head of Severodvinsk, Irina Sakharova, said that the activities were called off and that “everything is to be carried out in a regular, planned mode.”

After the accident on August 8, radiation levels in the village were reported to be three times the normal background levels (to borrow a phrase, this is not great but not terrible). A similar spike was seen in the nearby city of Severodvinsk.

Another local news outlet (News Nord) reported that some of the victims of the explosion had been brought to Arkhangelsk Regional Clinical Hospital and that "everything that was connected with their admission and assistance was sealed." Doctors had to sign non-disclosure papers, according to the report, and were not warned that the patients may have had radioactive debris on them.

"After the operation, the surgeon's apron squeaked when checking on the radiation diagnostic apparatus," News Nord reported. "Now everyone who somehow contacted the victims was taken to Moscow for examination."

https://arstechnica.com/?p=1551465

Warren: FTC's $125 cash option in Equifax settlement "misled" customers

Enlarge / Elizabeth Warren speaking to a crowd on February 18, 2019 in Glendale, California.
Getty Images | Mario Tama

reader comments

154 with 95 posters participating

Share this story

Equifax’s massive 2017 data breach screwed over more than 140 million people, so it was not terribly surprising when tens of millions of people jumped at the opportunity to claim cash money in compensation. The Federal Trade Commission, however, apparently *was* surprised. A few days after the settlement claims page went public, the option for affected consumers to claim cash vanished, with the agency citing “overwhelming” and “unexpected” public response.

Sen. Elizabeth Warren (D-Mass.) is now among the many who were frustrated by the FTC’s apparently questionable description of the settlement, and she’s calling on the agency to investigate its own claims about available consumer compensation.

“The FTC has the authority to investigate and protect the public from unfair or deceptive acts or practices, including deceptive advertising,” Warren says in a letter (PDF) to the commission’s inspector general. “Unfortunately, it appears as though the agency itself may have misled the American public about the terms of the Equifax settlement and their ability to obtain the full reimbursement to which they are entitled.”

The page on which consumers could file claims, as well as all the FTC’s public statements about the settlement, originally said breach victims could sign up for “free credit monitoring OR $125” if you already have credit monitoring services and declined to enroll. The “alternative compensation fund” from which that $125 would come, however, was capped at $31 million—only enough for 248,000 people, or about 0.2% of affected consumers, to receive the full amount.

That cap was not mentioned in the FTC’s initial press release, nor was it made clear in the claim form, Warren points out.

“These pages did not inform consumers that the cash payment was subject to—and in fact was very likely to be—severely reduced.” It took about a week after the settlement was announced for the commission to change its tune, warning consumers in an almost passive-aggressive way that claimants would get “nowhere near the $125 they could have gotten if there hadn’t been such an enormous number of claims filed.”

Warren asks the inspector general to “determine how the FTC made a series of decisions that will result in millions of Americans receiving only a small amount of the $125 they believe they are owed as remuneration for Equifax’s failures” and provides a list of questions the IG can tackle, starting with why the FTC notified the public about the $125 in the first place and who made that decision.

Why was the cash option so popular?

An FTC spokesman told Ars last month that the settlement “was designed with the 10-year credit monitoring product as the primary source of relief for affected consumers because it was viewed as the best source of future protection from identity theft.”

Aside from the allure of “free” money simply sounding great to millions of people, however, consumers have good reason to opt for the lump sum instead of the credit monitoring: they’ve probably already got more free credit monitoring than they can ever use and will keep being offered more.

It’s now standard practice for a company on the wrong end of a data breach to offer at least a year of free credit monitoring services to affected customers—and that list of “affected customers” basically includes everyone at this point. Data compiled by the Identity Theft Resource Center finds that while almost 198 million total records were exposed in hacks, breaches, and leaks in 2017, that number more than doubled to more than 446 million in 2018. Simply having an email address,

going shopping, applying for a job, having health insurance, or basically existing at all as a modern consumer, as in the case of Equifax, leaves your data vulnerable.

https://arstechnica.com/?p=1551419

FAA tells airlines MacBook Pros with defective batteries can’t fly

The 2015 15-inch Retina MacBook Pro.

reader comments

61 with 40 posters participating

Share this story

The Federal Aviation Administration has banned certain 15-inch MacBook Pros with potentially defective batteries from US flights. The move, which follows Apple’s June recall announcement, is part of a general FAA policy on devices with defective batteries.

“The FAA is aware of the recalled batteries that are used in some Apple MacBook Pro laptops,” FAA spokespeople said in emails to Ars Technica. Under FAA policy, affected MacBook Pros are banned from the passenger cabin and from checked luggage.

The FAA says it alerted airlines about the recall in early July. The agency also says it informed the public on social media around the same time, though it didn’t get much attention at the time.

Regulators in the European Union have also restricted the recalled MacBooks from use on European flights.

Apple isn’t the only manufacturer to have devices restricted from US flights. Samsung recalled the Galaxy Note 7 in 2016 after several exploding battery incidents. After one unit exploded onboard a Southwest Airlines flight (thankfully it hadn’t yet taken off), the FAA banned the devices from US airlines.

Which laptops are affected?

Affected laptops were mostly sold between September 2015 and February 2017.

“In a limited number of older generation 15-inch MacBook Pro units, the battery may overheat and pose a fire safety risk,” says a statement on Apple’s website. If you have a 15-inch MacBook Pro, you can visit Apple’s recall page and enter its serial number to determine whether your machine is affected. Apple says it will replace the batteries at no charge, though replacement could take up to two weeks.

https://arstechnica.com/?p=1551437

Verizon sues city to avoid

paying 5G fees, says the FCC has its back

Enlarge / A monitor seen on the floor of the New York Stock Exchange on Tuesday, Sept. 4, 2018.

reader comments

44 with 39 posters participating

Share this story

Verizon has sued the City of Rochester, New York, in order to avoid paying fees for deploying 5G equipment and fiber lines.

Verizon's lawsuit, filed in US District Court for the Western District of New York on Thursday, claims that the fees are higher than those allowed by federal law. As proof, Verizon points to a Federal Communications Commission preemption order from last year that attempts to limit the fees and aesthetic requirements cities and towns impose on carrier deployments. Rochester imposed its new fees in February of this year.

Verizon may have a good chance of winning its lawsuit if that FCC preemption order stands. But the FCC is being sued by cities from Washington, Oregon, California, and Arizona, which claim that the preemption is illegal. (Cities from Florida, Colorado, Nevada, and New York also intervened in the lawsuit to support the case against the FCC.) The outcome of that case could affect the Verizon suit against Rochester and any similar lawsuits filed against cities in the future.

Rochester vowed to fight Verizon's lawsuit and called it "frivolous." The city told WROC and other news outlets that "Other communications providers are complying with the law

while building out their networks and paying the necessary fees. These fees are comparable to what other cities required."

FCC preempted fees nationwide

Led by Chairman Ajit Pai, the FCC said it aimed to eliminate $2 billion worth of fees over five years, less than 1% of the estimated $275 billion that carriers would have to spend to deploy 5G small cells throughout the United States. Pai, a former Verizon lawyer, criticized cities and towns for "extracting as much money as possible in fees from the private sector" and claimed that lowering the fees would boost broadband deployment. But even Verizon previously said the FCC decision wouldn't change the pace of its 5G rollout.

In Rochester, the fees Verizon complained about include $1,500 per year for attaching a small cell to a city-owned pole. "These rates stand in sharp contrast with the FCC Ruling/Order," Verizon's lawsuit said.

As Verizon noted, the FCC determined that small cell fees of up to $270 a year "are presumptively consistent" with federal law. That doesn't mean cities can't charge more, but the FCC says they have to prove that the fees are a reasonable approximation of all costs and are "non-discriminatory."

"[W]hen Verizon Wireless requested that the City provide cost justification for these rates, the City did not provide any substantiation based on costs," Verizon's complaint said.

Rochester's letter to Verizon, included in an exhibit, said the following:

> *[W]e have concluded that our permit fees and recurring fees for use of the City's rights of way, including those for pole attachments related to the deployment of small wireless facilities, comply with all federal law requirements and*

> *limitations. You understand that requesting justifiable reimbursement from our telecom providers appropriately shifts that burden away from the City's taxpayers who would otherwise incur those costs irrespective of whether or not they are also a Verizon customer. It would be an unfair burden to place solely on our taxpayers.*

Verizon also objected to other Rochester fees, including $10,000 up front for deploying up to 2,500 linear feet of underground fiber, plus $5,000 annually in subsequent years. The per-foot charges decrease progressively for larger deployments, going as low as $0.50 per foot each year. But that first $10,000 charge applies even for deployments smaller than 2,500 feet, Verizon said.

"The Code imposes the same $10,000 first-year and $5,000 subsequent-year fees for 'underground' open-trenching use of either one linear foot or 2,500 linear feet, which inherently cannot accurately reflect Defendant's cost in each case," Verizon wrote. "These fees are thus not cost-based, are unreasonable, and are not objectively determined."

The different per-foot fees for longer fiber deployments "inherently cannot accurately reflect Defendant's cost and is thus unreasonable," Verizon also said. Rochester required the same fees for fiber lines that are hung on poles instead of buried, and Verizon raised the same objections to those fees.

While Verizon mostly stopped expanding its fiber-to-the-home service years ago, it still needs to deploy plenty of fiber to provide bandwidth for its 5G wireless network.

https://arstechnica.com/?p=1551025

Senators demand Amazon explain how junk winds up in “Choice” listings

Enlarge / Why is this particular product Amazon’s “Choice” when you search for a can opener, instead of an alternate item? Outside of Amazon, nobody actually knows.

reader comments

87 with 68 posters participating

Share this story

Amazon is a gigantic international marketplace filled with all sorts of goods from countless manufacturers and vendors—a selection so broad, it can easily overwhelm shoppers. Though the company doesn’t really curate what’s sold on its platform, it does do the equivalent of showing off certain products in the window with its “Amazon’s Choice” label. The problem is that nobody outside Amazon knows how those choices get chosen… and some of those “choice” products are basically crap.

Several media outlets have tried and failed to learn how it all works, but this week members of the Senate have come knocking on Amazon’s metaphorical door with some pointed questions. Democrats Bob Menendez of New Jersey and Richard Blumenthal of Connecticut are calling on Amazon to explain why certain products get that coveted Amazon’s Choice badge to determine if the moniker “deceives consumers into purchasing products of inferior quality.”

A search for a product like dish detergent returns more than 20,000 results, Blumenthal and Menendez write in a letter

(PDF) addressed to Amazon CEO Jeff Bezos. Given that volume, consumers “look for distinctive product features to help narrow the extensive search results,” and those shoppers “reasonably rely” on the Amazon’s Choice label “to guide their final purchasing decisions.”

The label does indeed seem to guide purchasing decisions, the senators note in their press release. A research study showed that products granted Amazon’s Choice status can see a threefold sales increase—but products that have the badge and then lose it see sales slump by 30%.

Amazon introduced the “Choice” feature in 2015 as a way to create a default for shoppers talking to their Alexa-enabled devices to buy goods. “Alexa, buy dish soap” is one thing if you buy the same kind of dish soap every month, but what if you have no purchase history? You can’t easily browse 20,000 items—or even 20 items—when you’re talking to a speaker. So Amazon’s Choice product became what Alexa would suggest for you up front.

These “choice” products can be of dubious quality, as highlighted by a BuzzFeed News report from June. BuzzFeed found dozens of instances of consumers complaining, both in Amazon reviews and elsewhere on social media, about Amazon’s Choice products that broke down or just plain didn’t work—including a thermometer where the product description itself said the item was “widely inaccurate.”

“I took the Amazon’s Choice label as an endorsement by Amazon, although I later found out that’s more of an algorithmic term,” one Amazon shopper told BuzzFeed at the time. “I find that to be confusing at best, misleading at worst.”

Pay to place?

The letter gives Amazon until September 16 to respond to a whole host of questions about how the Amazon’s Choice label

gets assigned, starting with a request for a detailed description of the process and whether it’s purely algorithmic or if human hands are ever involved. It also asks if all Amazon shoppers see the same “choice” products or if the label varies between shoppers based on individual purchase and browsing histories.

The senators also want to know what metrics Amazon uses to make the call. As part of that, the letter also asks Amazon to define what “highly rated” means, in context, especially given the challenges the company has faced in the past with fraudulent, paid-for reviews and review recycling, in which a lesser product is swapped into the listing of a different product that already has a positive rating.

The Amazon’s Choice moniker may mean Amazon is “actively promoting products with fraudulent reviews” and exacerbating the problem, the senators write. The company may also be unfairly disadvantaging competitors in the marketplace by promoting its own private-label brands (which are not always marked as Amazon brands) over others.

“Amazon bears the responsibility of providing its customers with accurate information” so shoppers can make informed decisions, the senators write. “Unfortunately, Amazon has failed to fulfill this responsibility.”

https://arstechnica.com/?p=1550849

YouTube should stop

recommending garbage videos to users

Enlarge / YouTube headquarters in San Bruno, California.

reader comments

25 with 19 posters participating

Share this story

In The New York Times, reporters Max Fisher and Amanda Taub explain how YouTube propelled the career of controversial Brazilian politician Jair Bolsonaro. Before his election as Brazil's president, they write, Bolsonaro "had long used the platform to post hoaxes and conspiracies."

Ostensibly, YouTube's recommendation algorithms are politically neutral. However, they're optimized to boost "engagement," and in practice that means promoting videos with extremist and conspiratorial points of view. In Brazil, that has meant bringing a cadre of far-right social media stars to prominence, ultimately helping them gain power in national politics.

According to the Times, Brazilians are also increasingly turning to "Dr. YouTube"—relying on YouTube videos rather than conventional professionals for medical advice.

"Harvard researchers found that YouTube's systems frequently directed users who searched for information on Zika, or even those who watched a reputable video on health issues, toward conspiracy channels," the reporters write.

We've seen similar developments here in the United States,

where social media has boosted the profile of anti-vaccine activists.

YouTube's auto-play recommendations aren't great for kids, either. Two years ago, writer James Bridle penned a widely read essay about the increasingly bizarre and disturbing children's videos that have been appearing on YouTube as publishers generate automated videos to game YouTube's recommendation algorithm.

YouTube's recommendation engine "isn't built to help you get what you want—it's built to get you addicted to YouTube," argued Guillaume Chaslot, an engineer who used to work on YouTube's recommendation algorithm, in a June interview with TNW.

There's a simple way to solve these problems: YouTube should stop making algorithmic video recommendations. When a video finishes playing, YouTube should show the next video in the same channel. Or maybe it could show users a video selected from a list of high-quality videos curated by human YouTube employees. But the current approach—in which an algorithm tries to recommend the most engaging videos without worrying about whether they're any good—has got to go.

YouTube isn't using its vast power responsibly

In recent years, YouTube, Facebook, and other major platforms have been embroiled in debates about whether to ban extreme and controversial content. It's a bit of a no-win situation for them. If they leave a video up, many people see it as endorsing the video's odious views. If they take videos down, they get attacked for political bias and censorship.

But the situation isn't so complicated when a platform makes recommendations. It's not censorship if YouTube decides not to

recommend your video to other users. And it should be uncontroversial that, if YouTube is going to recommend a video, the site should first verify that the video is worth watching.

What if YouTube staffers thought more like journalists? Journalists understand that they have a responsibility to do more than just run whatever story will get them the most readers, viewers, or clicks. They try to verify claims before reporting them as true, and they will spike a story if it's not newsworthy.

Of course, journalists aren't perfect. News organizations do still publish clickbait and inaccurate information from time to time. But most journalists at least try to use their power responsibly, even if we don't always succeed.

YouTube has vastly more influence over people's information diets than any contemporary media organization. Yet YouTube seems far less concerned about using its power responsibly. Far from steering people away from inaccurate and conspiratorial information, YouTube's automated algorithms seem to steer people toward this kind of misinformation because (as a former Facebook employee once put it) "bullshit is highly engaging."

Defenders of online platforms argue that it's not feasible to do human content curation at the scale of a platform like YouTube. That might be true if the goal is to take down the worst content. But the argument doesn't make sense if you're talking about YouTube's recommendations.

There's no reason YouTube's recommendations need to be personalized. YouTube could recommend the same set of videos to every YouTube visitor in a particular country—just as Ars Technica recommends the same articles to everyone who visits our home page. Or it could apply limited personalization algorithms to choose among a subset of videos that have been

pre-screened by human reviewers for accuracy and quality.

Instead, YouTube recommends a lot of toxic videos to its users because YouTube has made a business decision to prioritize "engagement" over all competing values. That decision is having negative consequences in Brazil, the United States, and around the world. It's time for YouTube to rethink its approach.

YouTube says it's working to improve its system

The Times story on Brazil was based on research done at Harvard and the University of Minas Gerais in Brazil. In a Monday tweet, YouTube disputed the team's findings.

"We had a team across product and engineering try to reproduce the recommendation results found by the University of Minas Gerais and Harvard's researchers, and it was unable to do so," YouTube wrote.

YouTube also says that since January, it has been "reducing recommendations of borderline content and videos that could misinform users in harmful ways. We're bringing this to Brazil by the end of this year."

But whether or not this will be enough remains to be seen. It may not be easy to predict in advance which types of content will prove harmful to users. A better approach would be to first drastically scale back automated recommendations—then only resume using them if and when the company is confident it can do so responsibly.

https://arstechnica.com/?p=1550009

Frontier network outages get worse in NY, triggering state investigation

Enlarge / A Frontier Communications van.

reader comments

37 with 30 posters participating

Share this story

Frontier Communications customers are reporting more outages and longer repair times, and state government officials have decided to investigate.

NY Public Service Commission (PSC) staff reported “that several Frontier Communications subsidiaries have significant service-quality problems, including escalating complaint rates, lengthy repair durations, and localized network reliability issues,” a PSC announcement Thursday said.

PSC staff is seeking more detailed information from Frontier on customer trouble reports and “will work with Frontier to develop and implement a plan to improve poor localized network reliability conditions,” the announcement said.

Frontier’s problems go far beyond New York. The company last week reported lower revenue and a $5.45 billion goodwill impairment charge, and it warned investors that its revenue will continue to decline in future quarters. Frontier has 3.63 million broadband subscribers in 29 states, down from 3.86 million a year ago. Frontier’s employee count has also dropped from 21,718 to 19,872 in the past year.

New York isn’t the only state investigating the company’s service. An investigation by the Minnesota Commerce Department this year found that Frontier has failed to properly maintain its telecom network and failed to give refunds or bill credits to customers affected by outages that have sometimes lasted for months.

Frontier’s website says it has “invested nearly $540 million since 2011 in the New York network,” allowing it “to offer faster broadband speeds to approximately 85,000 New York households in the upgraded service areas.”

But Frontier’s average Internet download speeds in New York are just 7.4Mbps, by far the lowest of any major provider in the state, according to Broadband Now. The maximum speed offered by Frontier in New York is 50Mbps, the broadband research group says.

Frontier serves 221,000 customer lines in New York and lost 30,000 customers in 2018, the PSC staff report said.

It’s not unusual for old copper networks to offer slow Internet speeds and poor reliability for both phone and Internet access. But the PSC report said Frontier’s problems go beyond the norm:

> *Staff has become increasingly concerned with the service quality of Frontier, especially in its Citizens, Frontier Rochester, Frontier New York, and Ausable Valley subsidiaries. The PSC Complaint rate has significantly increased in the last several years for these Frontier companies. In addition, Staff has responded to a significant number of network reliability complaints and inquiries from local, county, and State government representatives, including emergency response entities. These complaints include long repair durations and repeated out-of-service conditions, as well as Internet access and speed issues.*

The report listed service quality statistics for 61 phone companies, of which eight are Frontier subsidiaries. The PSC report also raised concerns about Taconic Telephone Corp. and Windstream but devoted the most time to Frontier. The report said the PSC was already performing "a multi-month review of Taconic's performance" and is following up with Windstream about its statistics "to determine if more focus is needed."

Frontier's numbers

One standard the PSC uses to judge network quality is the percentage of "central office entities" or switches that have 5.5 or fewer customer trouble reports per hundred access lines per month. That isn't a hard standard to meet, as all but eight of the 61 phone companies "achieved the minimum service requirement in 100% of their measurement opportunities," the PSC said. Four of the eight that failed to do so were the Frontier subsidiaries that the PSC is concerned about.

Frontier's "Ausable Valley had the lowest value in that column with 87.5% of its measurement opportunities met in 2018," the report said. Frontier's Citizens subsidiary clocked in at 98.2%, Frontier Communications of New York was at 99.17%, and Frontier of Rochester hit 98.6 percent.

Another measure is the number of annual complaints made directly to the PSC. Most complaints are made only to the companies themselves and not to the state government, so this rate tends to be very low. Only seven of the 61 companies had any complaints made directly to the PSC during 2018, and three of those were Frontier subsidiaries.

There were 1.025 complaints per thousand lines during the year for Frontier Communications of New York in 2018, 0.496 per thousand for Frontier of Rochester, and 0.412 per thousand for Frontier's Citizens division. These are all higher than the state's recommended level of 0.075 PSC complaints per 1,000 access lines.

More data is needed to figure out exactly what's going on in each part of Frontier's network, the PSC report said. The PSC said it intends to "identify the root causes of recurring outages, as well as develop a plan to improve network reliability performance."

The report also said:

> *Staff will request that Frontier perform an analysis of its customer trouble report and timeliness of repair data at a level more geographically granular than the central office to identify the localized causes of recurring outages, and [staff will] interview its local supervisors and technicians to help identify network plant/facility elements that are substantial contributors to poor network reliability performance. Staff will work with Frontier to review the findings of this data analysis and to develop a plan to resolve the recurring outages and will report to the Commission if further action becomes necessary.*

When contacted by Ars, Frontier said it takes the PSC "concerns seriously and is committed to delivering quality service to the New York communities and customers we serve. We will review the report and respond to the Commission in the appropriate forum."

https://arstechnica.com/?p=1549949

Alleged kingpin of massive, deadly fentanyl-laced pill

scheme stands trial

reader comments

68 with 40 posters participating

Share this story

Utah man Aaron Shamo, 29, will stand trial starting today over federal charges that he allegedly ran a deadly, multimillion-dollar counterfeit opioid racket on the black market amid the country's devastating opioid epidemic.

Federal prosecutors allege that Shamo and his accomplices pressed hundreds of thousands of counterfeit pills in the basement of Shamo's suburban Salt Lake City home and sold them on the dark Web to customers all across the US, making millions in the process. The pills resembled prescription opioid painkillers, such as oxycodone, but they were actually fakes laced with the highly potent and deadly opioid fentanyl, which Shamo allegedly imported from China illegally.

Prosecutors linked the pills to dozens of customer deaths, according to the Associated Press. However, Shamo is charged in connection to only one death, that of a 21-year-old who died in 2016 after snorting a fentanyl-containing pill that was made to resemble prescription oxycodone.

Fentanyl is 50 to 100 times more potent than morphine, according to the Centers for Disease Control and Prevention. Public health experts at the agency say that illicit forms of the drug—such as the pills in Shamo's case—have largely driven a massive third wave of opioid overdose deaths in the country. Overdose deaths involving synthetic opioids other than

methadone (largely fentanyl) surged almost 47% from 2016 to 2017, killing 28,400 people in 2017.

Enlarge / Three waves of the opioid epidemic

The case against Shamo follows a crackdown on the influx of Chinese fentanyl by US federal prosecutors. In October of 2017, for instance, the Department of Justice indicted two men in China for selling fentanyl directly to US customers. In January of 2018, a congressional report highlighted the problem, noting how easy it was for Americans to have fentanyl shipped directly to them from China.

Cash and pills

The case against Shamo began to come together in June 2016 when US customs agents intercepted a package of fentanyl allegedly addressed to someone receiving it on Shamo's behalf. After that, agents intercepted additional fentanyl shipments from a Chinese company called Express, which federal prosecutors are also investigating.

Federal prosecutors allege that once Shamo and his accomplices received the fentanyl, they cut the powder with fillers and dyes and pressed them into pills that resembled prescription drugs. They then allegedly sold them on a dark Web marketplace called Pharma-Master, which sometimes processed 20 to 50 orders a day.

At the end of 2016, federal investigators nabbed a single day's worth of outgoing packages from Shamo's alleged operation. The 52 packages shipped on one day included 35,000 fentanyl-laced pills in total. A single package in that collection was estimated to have a wholesale value of $400,000. The packages were addressed to homes in 26 states.

When federal agents raided Shamo's home later in 2016, they found a pill press still running in the basement and more than $1 million in cash stuffed into garbage bags.

Shamo's family says that he is being unfairly singled out in the case and that others involved were more deeply involved but are now getting off easier.

"He was brought in and saw the opportunity for making money, and he didn't truly understand the danger behind what he was doing, how dangerous the drugs were," Shamo's father Mike Shamo told the AP. "I think he was able to separate what he was doing because he never saw the customer. To him, it was just numbers on a screen."

https://arstechnica.com/?p=1549959

AI researchers have a plan to pay patients for data

iStock/Getty Images

reader comments

21 with 17 posters participating

Share this story

Robert Chang, a Stanford ophthalmologist, normally stays busy prescribing drops and performing eye surgery. But a few years ago, he decided to jump on a hot new trend in his field: artificial intelligence. Doctors like Chang often rely on eye imaging to track the development of conditions like glaucoma. With enough scans, he reasoned, he might find patterns that could help him better interpret test results.

That is, if he could get his hands on enough data. Chang embarked on a journey that's familiar to many medical researchers looking to dabble in machine learning. He started with his own patients, but that wasn't nearly enough, since training AI algorithms can require thousands or even millions of data points. He filled out grants and appealed to collaborators at other universities. He went to donor registries, where people voluntarily bring their data for researchers to use. But pretty soon he hit a wall. The data he needed was tied up in complicated rules for sharing data. "I was basically begging for data," Chang says.

Chang thinks he might soon have a workaround to the data problem: patients. He's working with Dawn Song, a professor at the University of California-Berkeley, to create a secure way

for patients to share their data with researchers. It relies on a cloud computing network from Oasis Labs, founded by Song, and is designed so that researchers never see the data, even when it’s used to train AI. To encourage patients to participate, they’ll get paid when their data is used.

That design has implications well beyond healthcare. In California, Governor Gavin Newsom recently proposed a so-called “data dividend” that would transfer wealth from the state’s tech firms to its residents, and US Senator Mark Warner (D-Va.) has introduced a bill that would require firms to put a price tag on each user’s personal data. The approach rests on a growing belief that the tech industry’s power is rooted in its vast stores of user data. These initiatives would upset that system by declaring that your data is yours and that companies should pay you to use it, whether it’s your genome or your Facebook ad clicks.

In practice, though, the idea of owning your data quickly starts looking a little… fuzzy. Unlike physical assets like your car or house, your data is shared willy-nilly around the Web, merged with other sources, and, increasingly, fed through a Russian doll of machine learning models. As the data transmutes form and changes hands, its value becomes anybody’s guess. Plus, the current way data is handled is bound to create conflicting incentives. The priorities I have for valuing my data (say, personal privacy) conflict directly with Facebook’s (fueling ad algorithms).

Song thinks that for data ownership to work, the whole system needs a rethink. Data needs to be controlled by users but still usable to others. “We can help users to maintain control of their data and at the same time to enable data to be utilized in a privacy preserving way for machine learning models,” she says. Health research, Song says, is a good way

to start testing those ideas, in part because people are already often paid to participate in clinical studies.

Meet Kara

This month, Song and Chang are starting a trial of the system, which they call Kara, at Stanford. Kara uses a technique known as differential privacy, where the ingredients for training an AI system come together with limited visibility to all parties involved. Patients upload pictures of their medical data—say, an eye scan—and medical researchers like Chang submit the AI systems they need data to train. That's all stored on Oasis' blockchain-based platform, which encrypts and anonymizes the data. Because all the computations happen within that black box, the researchers never see the data they're using. The technique also draws on Song's prior research to help ensure that the software can't be reverse-engineered after the fact to extract the data used to train it.

Chang thinks that privacy-conscious design could help deal with medicine's data silos, which prevent data from being shared across institutions. Patients and their doctors might be more willing to upload their data knowing it won't be visible to anyone else. It would also prevent researchers from selling your data to a pharmaceutical company.

Sounds nice in theory, but how do you incentivize people to actually snap pictures of their health records? When it comes to training machine learning systems, not all data is equal. That presents a challenge when it comes to paying people for it. To value the data, Song's system uses an idea developed by Lloyd Shapley, the Nobel Prize-winning economist, in 1953. Imagine a dataset as a team of players who need to cooperate to arrive at a particular goal. What did each player contribute? It's not just a matter of picking the MVP, explains James Zou, a professor of biomedical data science at Stanford who isn't involved in the project. Other data points

might act more like team players. Their contribution to overall success may be conditioned on who else is playing.

In a medical study that uses machine learning, there are lots of reasons why your data might be worth more or less than mine, says Zou. Sometimes it's the quality of the data—a poor quality eye scan might do a disease-detection algorithm more harm than good. Or perhaps your scan displays signs of a rare disease that's relevant to a study. Other factors are more nebulous. If you want your algorithm to work well on a general population, for example, you'll want an equally diverse mix of people in your research. So, the Shapley value for someone from a group often left out of clinical studies—say, women of color—might be relatively high in some cases. White men, who are often overrepresented in datasets, could be valued less.

Put it that way and things start to sound a little ethically hairy. It's not uncommon for people to be paid differently in clinical research, says Govind Persad, a bioethicist at the University of Denver, especially if a study depends on bringing in hard-to-recruit subjects. But he cautions that the incentives need to be designed carefully. Patients will need to have a sense of what they'll be paid so they don't get low-balled and receive solid justifications, grounded in valid research aims, for how their data was valued.

What's more challenging, Persad notes, is getting the data market to function as intended. That has been a problem for all sorts of blockchain companies promising user-controlled marketplaces—everything from selling your DNA sequence to "decentralized" forms of eBay. Medical researchers will have concerns about the quality of data and whether the right kinds are available. They'll also have to navigate restrictions a user might put on how their data can be used. On the other side, patients will need to trust that Oasis' technology and promised privacy guarantees work as advertised.

The clinical study, Song says, aims to start resolving some of

those questions, with Chang's patients testing the application first. As the marketplace expands, researchers might make calls for specific kinds of data, and Song envisions partnering with doctors or hospitals so that patients aren't totally alone in figuring out what types of data to upload. Her team is also looking into ways of estimating the value of particular data before the AI systems are trained so that users know roughly how much they'll make by giving researchers access.

Wider adoption of the data ownership idea is a ways off, Song admits. Currently, companies mostly get to choose how they store user data, and their business models mostly depend on holding it directly. Companies, including Apple, have embraced differential privacy as a way to privately gather data from your iPhone and enable features like Smart Replies without revealing individual personal data. But Facebook's core ad business, of course, doesn't work like that. Before any smart math tricks for valuing data are useful, regulators need to sort out rules for how data is stored and shared, says Zou. "There is a gap between the policy community and the technical community on what exactly it means to value data," he says. "We're trying to inject more rigor into these policy decisions."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1549429

At Defense Distributed, few

glimpses of life after Cody Wilson

reader comments

43 with 26 posters participating, including story author

Share this story

- Nathan Mattise
- The US Marshals sent this updated wanted poster to media when Wilson was finally apprehended following his time evading arrest in Taipei.
- Defense Distributed's new leader, Paloma Heindorff, holds up the letter from the Department of State that started all the company's legal battles.
  Defense Distributed

It's been nearly a year since 3D-printed firearms activist Cody Wilson was arrested for the alleged sexual assault of a female minor. Yesterday, he appeared in an Austin, Texas courtroom and plead guilty to lesser charges that will likely see Wilson register as a sex offender and serve multiple years probation. He won't be able to possess any firearms and must consent to keystroke/remote monitoring during that time.

But long before Wilson's plead, his situation quickly prompted an unexpected change in leadership at Defense Distributed, the now-infamous Austin, Texas-based digital printing and firearms company he started in 2012. News of an arrest warrant for Wilson came on September 19, 2018, and Paloma Heindorff was named the company's new director less than a week later on September 25.

At the time, Heindorff stated that Wilson would no longer have any involvement with the company. She also promised business

would continue on as normal and that she would likely take a different approach publicly than her outspoken, interview-friendly predecessor.

Ars called Defense Distributed this week to see if the company would provide an update on things in the year post-Wilson. Could Defense Distributed at least share any updated figures on sales or fundraising from the last year? The last available data on those topics came during Heindorff's introductory press conference, when she mentioned the Defense Distributed legal fund had eclipsed $400,000 and that the company had sold 3,000 Ghost Gunner milling machines (that, at roughly $1,500 each, would've provided about $4.5 million in revenue).

But Stephen Sheftall, who handles sales communication at the company among his duties, said the company had no use for media at this time and wouldn't be doing any interviews in the foreseeable future. Heindorff, however, has done at least one extended interview since settling into her new role. Back in February, Reason.com sat down with Heindorff about four months into her tenure.

"I'm not going to say it was the best promotion I've ever got, but from a business standpoint we've done incredibly well—minimal disruptions to the daily operations," she said. "Cody's departure has affected us less than people think, and I understand why people would think it would be chaos. He was incredibly powerful figurehead. But there are quite a bit of us working back there. It's been more of a personal effect than, 'Oh, now we can't run the company.' The company is doing just fine."

Court cases: One onto appeals, another slowly moves

Even if Defense Distributed hasn't been doing as much direct press, there have been some notable public happenings

involving the company during Heindorff's first year at the helm. For starters, Defense Distributed has continued its legal efforts revolving around the online distribution of 3D-printed gun CAD files. While several states took action against untraceable, self-milled or printed "ghost guns" in 2018, Defense Distributed brought its own case called *Defense Distributed v. Grewal* (the attorney general of New Jersey is Gurbir Grewal), which had its day in court back in January. The case centered on a newly enacted state law, SB2465, aimed at regulating "ghost guns" and the promotion or distribution of related files online. Such laws led to Defense Distributed and similar companies taking down gun milling and printing information from their websites. (In Defense Distributed's case, the company instead continues to offer this info for sale via a USB stick to eligible customers.)

Ultimately, the case was dismissed in February, though the judge made that decision based on jurisdiction rather than the merits of the case. But less than two weeks later, the New Jersey AG revealed one of the documents that led to the case initially being heard had been faked by an IP address in Slovakia.

"It's really the info they're trying to stifle, otherwise they would've written different laws," Heindorff told Reason.com when asked to reflect on the state battles around that time. "How disrespectful to one's subjects, I'll call them. The general [populace] cannot be trusted with this info."

After the case's dismissal, a New Jersey judge eventually also denied Defense Distributed's motion to seek an injunction (PDF) for the law pending an appeal. As the company revealed on its Legio blog in April, Defense Distributed is now appealing *Defense Distributed v. Grewal* in the Third Circuit Court of Appeals. Initial filings have been made, but there are no upcoming court dates currently scheduled.

Defense Distributed v. Grewal was not Defense Distributed's

only legal crusade, however. In fact, that was entirely separate from perhaps the more wide-reaching legal case, *State of Washington v. Department of State.* In this, Washington alongside several other states pursued legal action initially because they believed that, when the Department of Justice settled its five-year legal battle with Defense Distributed in July 2018 and allowed the CAD files in question to be reposted online, that action violated the Constitution. But in a November 2018 filing, government lawyers for the defense explained that rule changes being considered by the State Department at the time would make any legal conflicts in *Washington* moot.

By February 2019, US District Judge Robert Lasnik got tired of waiting. He denied the Department of State's motion to stay the case and allowed the proceedings to move forward. The plaintiffs soon filed a motion for summary judgment that month, and the two sides have gone back and forth on timelines and submitting supporting documents in either direction since. One of the defendants' main arguments, as outlined in a June filing, seems to be the states' lack of "traceability and redressability"—essentially, the fact that these files are now out there and can't be taken offline makes this litigation moot in their view. Motions from both sides were delivered by early June, but there is no public timetable for the case's next steps.

Enlarge / r/defense_distributed no longer exists as of summer 2019. Previously, Defense Distributed employees and customers used the forum to interact, and 3D-printing gun enthusiasts would share tips, videos, and more.

Out of court, pressure from Big Tech and Congress

During Heindorff's young tenure, Defense Distributed has also faced increased pressure outside of the courts from big tech companies. This summer, Facebook seemed to clarify that "A Page representing a real brick-and-mortar store, legitimate website or brand" could promote 3D-printed firearms "only for sale off of our services and as long as those retailers comply with all applicable laws and regulations." But currently, Facebook company policy also states that "3D gun printing files or instructions to manufacture firearms using 3D printers or CNC milling machines, including links to websites where such files or instructions are made available, may not be shared by anyone" on Mark Zuckerberg's giant social media platform. Defense Distributed does not maintain an official brand page on the platform, and private groups that have popped up for Defense Distributed customers typically explicitly ask members to avoid posting "DEFCAD OR OTHER

LINKS!”

Other social media sites cracked down on distribution of 3D printed gun files and information this summer as well. Just weeks after the nonprofit gun violence news outlet The Trace found Twitter users freely distributing 3D-printed gun design files, Twitter introduced a new policy banning such actions entirely in June. And on reddit, a longtime subreddit devoted to Defense Distributed, r/defense_distributed, was banned for violating that site’s rules about posting prohibited goods or services.

“Facebook won’t allow anyone to share any links to our products. On YouTube, if videos reference Defcad codes, they get removed. These corporations are saying knowledge of this knowledge is too dangerous for people to have,” Heindorff told Reason.com several months before this summer’s social media saga. “The plans for this gun were downloaded a million times five years ago, but apparently the knowledge this even exists is too dangerous to talk about. That’s crazy to me.”

As The Trace reported, such bans haven’t stopped the spread of 3D-printed gun information. Users wanting to discuss and swap information about 3D-printed firearms simply took their discourse elsewhere. On Keybase, a platform from dating site OkCupid that has end-to-end encryption, expiring messages, and the option for users to verify their identities through social media accounts, a group called Deterrence Dispensed quickly rose into the top 10 most popular Keybase teams within two weeks of the reddit ban. Entire platforms have sprung up to fill similar voids elsewhere: GunStreamer has become a gun-focused video site; Spee.ch is a blockchain-based media site where Deterrence Dispensed has made blueprints available for things like AR-15s and handgun frames.

But things may only get trickier for Defense Distributed and 3D-printed gun advocates from here. States such as New York and Washington have taken New Jersey’s lead and passed their

own legislation addressing 3D-printed guns in recent weeks. And some politicians at the federal level also continue to call for bans on 3D-printed guns.

Congressman Ted Deutsch (D-Fla.) and Senator Ed Markey (D-Mass.) put forth the 3D Printed Gun Safety Act of 2019 in late June as the latest example. If eventually made into law, the bill would make it illegal to "intentionally distribute, over the Internet or by means of the World Wide Web, digital instructions in the form of Computer Aided Design files or other code that can automatically program a three-dimensional printer or similar device to produce a firearm or complete a firearm from an unfinished frame or receiver." So far, however, there hasn't been any formal movement and this proposal remains one of 110 gun bills Congress currently has on the table.

Listing image by Defense Distributed

https://arstechnica.com/?p=1528945