Buyers of Razer’s bogus “N95” Zephyr masks get over $1 million in refunds

“The Razer Zephyr was conceived to offer a different and innovative face covering option for the community,” the company said at the time. “The FTC’s claims against Razer concerned limited portions of some of the statements relating to the Zephyr. More than two years ago, Razer proactively notified customers that the Zephyr was not a N95 mask, stopped sales, and refunded customers.”

FTC: Only 6 percent of US purchases were refunded

The FTC lawsuit casts doubt on the earlier availability of refunds, saying that Razer “allegedly implemented” a refund policy. Razer provided refunds for less than 6 percent of Zephyr purchases in the US, the FTC said.

“While Defendants purport to have instituted a policy of fully refunding consumers concerned about the filters on January 9, 2022, Defendants did not promote that policy in its January emails to consumers or on its website,” the FTC said.

That’s a reference to a Razer email sent to mask buyers acknowledging that the mask “is not a medical device nor certified as an N95 mask.” The FTC said the Razer email to consumers “did not invite or otherwise indicate that consumers who believed they were purchasing an N95 mask when they purchased the Zephyr could request a refund from Razer.”

Razer customers who sought refunds ran into several kinds of problems, the FTC said. Some “were told that they could not receive a refund because they were outside of Razer’s standard 14-day return policy,” while others “were told that they could not receive a full refund because they had used the disposable filters provided with the Zephyr when they bought the Zephyr in October 2022 or because the Zephyr was no longer sealed and unused,” the lawsuit said.

“Numerous customers were deterred from, or confused regarding their ability to, obtain full refunds because of statements by Defendants’ customer service representatives that they were ineligible for full refunds,” the lawsuit said.

We contacted Razer today and will update this article if it provides further comment.

https://arstechnica.com/tech-policy/2025/01/razer-sold-bogus-n95-mask-for-100-in-2021-users-finally-get-refunds/

Elon Musk could be China’s pick to buy TikTok, report says

TikTokers could also flock to YouTube, which remains one of the most profitable platforms for creators on the planet. But that would surely rile some YouTube users who dislike YouTube Shorts clogging up the homepage.

Rather than move to a popular US app, however, many contrarian

TikTokers are eyeing other Chinese-owned apps, including ByteDance-owned Lemon8. Both Lemon8 and an app owned by another Chinese company called Xiaohongshu—which Americans know as Red Note—reached the top two spots in Apple's App Store rankings Monday, Business Insider reported.

On Red Note, TikTokers are gathering under a hashtag, "TikTokrefugee," The New York Times reported. As of Tuesday, the hashtag had been viewed more than 100 million times and referenced in 2.5 million comments.

According to a Times review of TikTok videos, TikTokers said they were moving to Red Note because "they wanted to show they do not share Washington's concerns about TikTok's ties to China." But TikTokers could be in for a rude awakening if TikTok is banned and the Chinese-owned app they choose as their new home quickly becomes the next app to be blocked in the US within a few months.

Under the Protecting Americans from Foreign Adversary Controlled Applications Act that would force TikTok's sale or require a ban, any "foreign adversary controlled" social media app with more than 1 million monthly active users could be banned. ByteDance and TikTok are both singled out by the law, meaning any meaningful spike in US users on other ByteDance apps would likely trigger scrutiny.

It's unclear if Red Note would be as easily targeted by the government, but any Chinese-owned social media app that meets very basic requirements—allowing more than a million monthly active users to share content that can be viewed by others—could potentially be banned if the Supreme Court upholds the law.

An analyst at the market research company Emarketer, Jasmine Enberg, told The Independent that TikTokers recommending apps like Lemon8 "may not be aware of the possible implications for the other ByteDance apps because the law does not identify

them.”

https://arstechnica.com/tech-policy/2025/01/elon-musk-could-be-chinas-pick-to-buy-tiktok-report-says/

Mastodon’s founder cedes control, refuses to become next Musk or Zuckerberg

And perhaps in a nod to Meta’s recent changes, Mastodon also vowed to “invest deeply in trust and safety” and ensure “everyone, especially marginalized communities,” feels “safe” on the platform.

To become a more user-focused paradise of “resilient, governable, open and safe digital spaces,” Mastodon is going to need a lot more funding. The blog called for donations to help fund an annual operating budget of $5.1 million (5 million euros) in 2025. That’s a massive leap from the $152,476 (149,400 euros) total operating expenses Mastodon reported in 2023.

Other social networks wary of EU regulations

Mastodon has decided to continue basing its operations in Europe, while still maintaining a separate US-based nonprofit entity as a “fundraising hub,” the blog said.

It will take time, Mastodon said, to “select the appropriate jurisdiction and structure in Europe” before Mastodon can then “determine which other (subsidiary) legal structures are needed to support operations and sustainability.”

While Mastodon is carefully getting re-settled as a nonprofit in Europe, Zuckerberg this week went on Joe Rogan’s podcast to call on Donald Trump to help US tech companies fight European Union fines, Politico reported.

Some critics suggest the recent policy changes on Meta platforms were intended to win Trump’s favor, partly to get Trump on Meta’s side in the fight against the EU’s strict digital laws. According to France24, Musk’s recent combativeness with EU officials suggests Musk might team up with Zuckerberg in that fight (unlike that cage fight pitting the wealthy tech titans against each other that never happened).

Experts told France24 that EU officials may “perhaps wrongly” already be fearful about ruffling Trump’s feathers by targeting his tech allies and would likely need to use the “full legal arsenal” of EU digital laws to “stand up to Big Tech” once Trump’s next term starts.

As Big Tech prepares to continue battling EU regulators, Mastodon appears to be taking a different route, laying roots in Europe and “establishing the appropriate governance and leadership frameworks that reflect the nature and purpose of Mastodon as a whole” and “responsibly serve the community,” its blog said.

“Our core mission remains the same: to create the tools and digital spaces where people can build authentic, constructive online communities free from ads, data exploitation, manipulative algorithms, or corporate monopolies,” Mastodon’s blog said.

https://arstechnica.com/tech-policy/2025/01/mastodon-becomes-n

onprofit-to-make-sure-its-never-ruined-by-billionaire-ceo/

New York starts enforcing $15 broadband law that ISPs tried to kill

1.7 million New York households lost FCC discount

The order said quick implementation of the law is important because of "developments at the federal level impacting the affordability of broadband service." About 1.7 million New York households, and 23 million nationwide, used to receive a monthly discount through an FCC program that expired in mid-2024 after Congress failed to provide more funding.

"For this reason, consumer benefit programs assisting low-income households—such as the ABA—are even more critical to ensure that the digital divide for low-income New Yorkers is being addressed," the New York order said.

New York ISPs can obtain an exemption from the low-cost broadband law if they "provide service to no more than 20,000 households and the Commission determines that compliance with such requirements would result in 'unreasonable or unsustainable financial impact on the broadband service provider,'" the order said.

Over 40 small ISPs filed for exemptions in 2021 before the law was blocked by a judge. Those ISPs and potentially others will be given one-month exemptions if they file paperwork by Wednesday stating that they meet the subscriber threshold. ISPs must submit detailed financial information by February 15 to obtain longer-term exemptions.

“All other ISPs (i.e., those with more than 20,000 subscribers) must comply with the ABA by January 15, 2025,” the order said. Failure to comply can be punished with civil penalties of up to $1,000 per violation. The law applies to wireline, fixed wireless, and satellite providers.

Charter Spectrum currently advertises a $25-per-month plan with 50Mbps speeds for low-income households. Comcast and Optimum have $15 plans. Verizon has a low-income program reducing the cost of some home Internet plans to as low as $20 a month.

Disclosure: The Advance/Newhouse Partnership, which owns 12.3 percent of Charter, is part of Advance Publications, which also owns Ars Technica parent Condé Nast.

https://arstechnica.com/tech-policy/2025/01/new-york-starts-enforcing-15-broadband-law-that-isps-tried-to-kill/

Supreme Court lets Hawaii sue oil companies over climate change effects

On Monday, the Supreme Court declined to decide whether to block lawsuits that Honolulu filed to seek billions in damages from oil and gas companies over allegedly deceptive marketing campaigns that hid the effects of climate change.

Now those lawsuits can proceed, surely frustrating the fossil fuel industry, which felt that SCOTUS should have weighed in on this key “recurring question of extraordinary importance to the energy industry” raised in lawsuits seeking similarly high damages in several states, CBS News reported.

Defendants Sunoco and Shell, along with 15 other energy companies, had asked the court to intervene and stop the Hawaii lawsuits from proceeding. They had hoped to move the cases out of Hawaii state courts by arguing that interstate pollution is governed by federal law and the Clean Air Act.

The oil and gas companies continue to argue that greenhouse gas emissions “flow from billions of daily choices, over more than a century, by governments, companies, and individuals about what types of fuels to use, and how to use them.” Because of this, the companies believe Honolulu was wrong to demand damages based on the “cumulative effect of worldwide emissions leading to global climate change.”

“In these cases, state and local governments are attempting to assert control over the nation’s energy policies by holding energy companies liable for worldwide conduct in ways that starkly conflict with the policies and priorities of the federal government,” oil and gas companies unsuccessfully argued in their attempt to persuade SCOTUS to grant review. “That flouts this court’s precedents and basic principles of federalism, and the court should put a stop to it.”

https://arstechnica.com/tech-policy/2025/01/supreme-court-lets-hawaii-sue-oil-companies-over-climate-change-effects/

Judge ends man’s 11-year quest to dig up landfill and recover $765M in bitcoin

A British judge ruled against a man who wants to excavate a landfill where he says a hard drive with access to thousands of bitcoins was mistakenly dumped over 11 years ago.

Since 2013, James Howells has been hoping to recover a laptop hard drive that he says contains the private key for cryptocurrency which he says he mined in 2009. We wrote about it at the time, noting that the value of a bitcoin had just passed $1,000, making 7,500 bitcoins worth $7.5 million.

The alleged number of bitcoins has changed a bit, with Howells now saying he lost 8,000 bitcoins. The bitcoin price exceeded $100,000 last month and was worth over $95,636 as of this writing, or $765 million for 8,000 bitcoins.

High Court Judge Keyser KC issued his ruling yesterday, siding with the defendant in *Howells v. Newport City Council*. Howells has no realistic chance of success at trial, the judge ruled. Howells sought “an order that the defendant either deliver the hard drive or allow his team of experts to excavate the landfill in order to find it, and (in the alternative) compensation equivalent to the value of the Bitcoin that he can no longer access.”

Landfill authority owns the trash

The council said that excavating the landfill site would let harmful substances escape into the environment, endangering residents with “potentially serious risks which raises public health issues and environmental concerns,” the ruling said.

The judge found no “reasonable grounds for bringing this case,” saying it has “no realistic prospect of succeeding if it went to trial and that there is no other compelling reason why it should be disposed of at trial.” He granted summary judgment for the defendant, dismissing the claim.

The ruling quotes the Control of Pollution Act 1974, which states that “anything delivered to the authority by another person in the course of using the facilities shall belong to the authority and may be dealt with accordingly.” Howells “submitted that section 14(6)(c) merely says that anything so delivered shall belong to the authority but does not say that it shall cease to belong to its former owner,” the ruling said. The judge disagreed, writing that “the words ‘shall belong to the authority’ are unqualified and unrestricted.”

https://arstechnica.com/tech-policy/2025/01/judge-ends-mans-11-year-quest-to-dig-up-landfill-and-recover-765m-in-bitcoin/

Misconfigured license plate readers are leaking data and video in real time

In just 20 minutes this morning, an automated license-plate-recognition (ALPR) system in Nashville, Tennessee, captured photographs and detailed information from nearly 1,000 vehicles as they passed by. Among them: eight black Jeep Wranglers, six Honda Accords, an ambulance, and a yellow Ford Fiesta with a vanity plate.

This trove of real-time vehicle data, collected by one of Motorola's ALPR systems, is meant to be accessible by law enforcement. However, a flaw discovered by a security researcher has exposed live video feeds and detailed records of passing vehicles, revealing the staggering scale of surveillance enabled by this widespread technology.

More than 150 Motorola ALPR cameras have exposed their video feeds and leaking data in recent months, according to security researcher Matt Brown, who first publicized the issues in a series of YouTube videos after buying an ALPR camera on eBay and reverse engineering it.

As well as broadcasting live footage accessible to anyone on the Internet, the misconfigured cameras also exposed data they have collected, including photos of cars and logs of license plates. The real-time video and data feeds don't require any usernames or passwords to access.

Alongside other technologists, WIRED has reviewed video feeds from several of the cameras, confirming vehicle data—including makes, models, and colors of cars—have been accidentally exposed. Motorola confirmed the exposures, telling WIRED it was working with its customers to close the access.

Over the last decade, thousands of ALPR cameras have appeared in towns and cities across the US. The cameras, which are manufactured by companies such as Motorola and Flock Safety, automatically take pictures when they detect a car passing by.

The cameras and databases of collected data are frequently used by police to search for suspects. ALPR cameras can be placed along roads, on the dashboards of cop cars, and even in trucks. These cameras capture billions of photos of cars—including occasionally bumper stickers, lawn signs, and T-shirts.

“Every one of them that I found exposed was in a fixed location over some roadway,” Brown, who runs cybersecurity company Brown Fine Security, tells WIRED. The exposed video feeds each cover a single lane of traffic, with cars driving through the camera’s view. In some streams, snow is falling. Brown found two streams for each exposed camera system, one in color and another in infrared.

https://arstechnica.com/security/2025/01/misconfigured-license-plate-readers-are-leaking-data-and-video-in-real-time/

EU “energetically” probing disinformation, right-wing bias on X, report says

The European Commission (EC) is planning to “energetically” advance its probe into content moderation on X (formerly Twitter), potentially ordering changes at Elon Musk’s social network in the coming months, Bloomberg reported.

Since 2023, the EC has been investigating X for possible violations of the Digital Services Act (DSA). Notably, it’s

the group’s first formal probe under the DSA, which requires very large online platforms to meet strict content moderation and transparency standards to ensure user safety, reduce misinformation, prevent illegal/harmful activity, and facilitate “a fair and open online platform environment.”

In a letter to European lawmakers viewed by Bloomberg, EC tech commissioner Henna Virkkunen and justice chief Michael McGrath apparently confirmed that the investigation into X will end “as early as legally possible.”

When the sweeping probe was first announced, the EC explained it would investigate X “in areas linked to risk management, content moderation, dark patterns, advertising transparency, and data access for researchers.”

At that time, the EC was concerned about “the dissemination of illegal content in the context of Hamas’ terrorist attacks against Israel” on X. The investigation is partly focused on X’s potential failure to detect and remove illegal content required by the DSA, as well as on the effectiveness of X’s Community Notes and other “related policies mitigating risks to civic discourse and electoral processes.”

Since then, Musk has become more heavily involved in right-wing politics, campaigning for US president-elect Donald Trump and increasingly using X to support right-wing figures globally, most recently in a posting rampage concerning United Kingdom “grooming gangs.” The Financial Times reported that Musk’s UK posts appeared to be fueled by a few X accounts that seemingly appeared on his “For You” page, with one former Twitter exec in Europe, Bruce Daisley, suggesting that “Musk has seemingly become the first tech leader to fall down the rabbit hole of radicalization by his own product.”

https://arstechnica.com/tech-policy/2025/01/eu-energetically-probing-disinformation-right-wing-bias-on-x-report-says/

US sues six of the biggest landlords over “algorithmic pricing schemes”

The Justice Department says that landlords did more than use RealPage in the alleged pricing scheme. “Along with using RealPage’s anticompetitive pricing algorithms, these landlords coordinated through a variety of means,” such as “directly communicating with competitors’ senior managers about rents, occupancy, and other competitively sensitive topics,” the DOJ said.

There were “call arounds” in which “property managers called or emailed competitors to share, and sometimes discuss, competitively sensitive information about rents, occupancy, pricing strategies and discounts,” the DOJ said.

Landlords discussed their use of RealPage software with each other, the DOJ said. “For instance, landlords discussed via user groups how to modify the software’s pricing methodology, as well as their own pricing strategies,” the DOJ said. “In one example, LivCor and Willow Bridge executives participated in a user group discussion of plans for renewal increases, concessions and acceptance rates of RealPage rent recommendations.”

DOJ: Firms discussed “auto-accept”

settings

The DOJ lawsuit says RealPage pushes clients to use “auto-accept settings” that automatically approve pricing recommendations. The DOJ said today that property rental firms discussed how they use those settings.

“As an example, at the request of Willow Bridge’s director of revenue management, Greystar’s director of revenue management supplied its standard auto-accept parameters for RealPage’s software, including the daily and weekly limits and the days of the week for which Greystar used ‘auto-accept,'” the DOJ said.

Greystar issued a statement saying it is “disappointed that the DOJ added us and other operators to their lawsuit against RealPage,” and that it will “vigorously” defend itself in court. “Greystar has and will conduct its business with the utmost integrity. At no time did Greystar engage in any anti-competitive practices,” the company said.

The Justice Department is joined in the case by the attorneys general of California, Colorado, Connecticut, Illinois, Massachusetts, Minnesota, North Carolina, Oregon, Tennessee, and Washington. The case is in US District Court for the Middle District of North Carolina.

https://arstechnica.com/tech-policy/2025/01/big-landlord-settles-with-us-will-cooperate-in-price-fixing-investigation/

Dirty deeds in Denver: Ex-

prosecutor faked texts, destroyed devices to frame colleague

How we got here

Choi was a young attorney a few years out of law school, working at the Denver District Attorney's Office in various roles between 2019 and 2022. Beginning in 2021, she accused her colleague, Dan Hines, of sexual misconduct. Hines, she said at first, made an inappropriate remark to her. Hines denied it and nothing could be proven, but he was still transferred to another unit.

In 2022, Choi complained again. This time, she offered phone records showing inappropriate text messages she allegedly received from Hines. But Hines, who denied everything, offered investigators his own phone records, which showed no texts to Choi.

Investigators then went directly to Verizon for records, which showed that "Ms. Choi had texted the inappropriate messages to herself," according to the Times. "In addition, she changed the name in her phone to make it appear as though Mr. Hines was the one who had sent them."

At this point, the investigators started looking more closely at Choi and asked for her devices, leading to the incident described above.

In the end, Choi was fired from the DA's office and eventually given a disbarment order by the Office of the Presiding

Disciplinary Judge, which she can still appeal. For his part, Hines is upset about how he was treated during the whole situation and has filed a lawsuit of his own against the DA's office, believing that he was initially seen as a guilty party even in the absence of evidence.

The case is a reminder that, despite well-founded concerns over tracking, data collection, and privacy, sometimes the modern world's massive data collection can work to one's benefit. Hines was able to escape the second allegation against him precisely because of the specific (and specifically refutable) digital evidence that was presented against him—as opposed to the murkier world of "he said/she said."

Choi might have done as she liked with her devices, but her "evidence" wasn't the only data out there. Investigators were able to draw on Hines' own phone data, along with Verizon network data, to see that he had not been texting Choi at the times in question.

Update: Ars Technica has obtained the ruling, which you can read here (PDF). The document recounts in great detail what a modern, quasi-judicial workplace investigation looks like: forensic device examinations, search warrants to Verizon, asking people to log into their cell phone accounts and download data while investigators look over their shoulders, etc.

https://arstechnica.com/tech-policy/2025/01/dirty-deeds-in-denver-ex-prosecutor-faked-texts-destroyed-devices-to-frame-colleague/