Supreme Court won’t hear appeals from fossil fuel firms in climate change lawsuits

reader comments

122 with

Share this story

WASHINGTON—The Supreme Court on Monday declined to hear five appeals from the fossil fuel industry seeking to move climate change lawsuits it faces to the federal courts. The decision opens the door for Baltimore and other cities, states, and counties to pursue their claims for damages from climate-related extreme weather events, flooding, and sea-level rise in state courts.

Since the localities began filing their climate suits six years ago, they have, for the most part, seen state courts as the appropriate, and more advantageous, jurisdiction for seeking damages caused by climate change using product liability, deceptive advertising, and nuisance statutes.

They have contended that the industry has known for decades that burning fossil fuels produces greenhouse gases that warm the planet—harming local jurisdictions, their infrastructure, and, ultimately, their citizens.

“Since we filed this case nearly five years ago, the climate

crisis has worsened, the costs to Baltimore taxpayers are skyrocketing, and the defendants have pocketed trillions of dollars in profits while trying to dodge accountability for their deception," Sara Gross, chief of the Affirmative Litigation Division in the Baltimore City Department of Law, said in a statement.

Oil and gas companies, on the other hand, have sought to move these cases to federal courts where the focus would be less on local damages caused by extreme weather and more on national issues related to energy needs and greenhouse gas emissions under the federal Clean Air Act. ExxonMobil, Chevron, and Shell Oil Products were among the parties arguing that issues related to greenhouse gas emissions are "inherently federal."

Advertisement

The lawsuits before the high court were filed by Rhode Island, the cities of Baltimore, Honolulu, and Imperial Beach, California, and counties in California and Hawaii. Numerous other states, cities, and counties have filed similar suits.

"After decades of climate change deception by the fossil fuel defendants, and now nearly half a decade of delay tactics in our lawsuit to hold them accountable for it, our residents, workers, businesses and taxpayers are ready for their day in court," said Rhode Island Attorney General Peter F. Neronha.

The fossil fuel companies vowed to continue fighting the lawsuits and pursuing their jurisdictional arguments. "We will continue to fight these suits, which are a waste of time and resources and do nothing to address climate change," a spokesperson for ExxonMobil said. "Today's decision has no impact on our focus to invest billions of dollars into leading the way in a thoughtful energy transition that takes the world to net zero carbon emissions."

John Masslon, senior counsel at the Washington Legal Foundation, a conservative public law firm that filed an

amicus brief on behalf of the fossil fuel industry, said the jurisdictional argument is far from decided. “The issue of whether climate change litigation belongs in state or federal court is not going away,” Masslon said. “The Supreme Court will eventually have to resolve the circuit split on this critical issue. Kicking the can down the road will just help pad the bank accounts of lawyers at consumers’ expense.”

To date, at least five federal circuit courts of appeals have considered the jurisdictional issue and concluded that there were insufficient grounds to move the cases from the state courts to federal jurisdiction.

In March, a brief filed by the Biden administration also urged the court not to take up the appeals, arguing that no federal questions had been raised.

This story originally appeared on Inside Climate News.

https://arstechnica.com/?p=1934146

Access to abortion pill is spared; SCOTUS freezes lower court’s order

Enlarge / The US Supreme Court in Washington, DC, US, on Wednesday, April 19, 2023. Democrats oppose the Republican-led Congressional Review Act resolution to disapprove of the Department of Veteran Affairs’ interim rule on reproductive health care. Photographer: Al Drago/Bloomberg via Getty Images

reader comments

173 with

Share this story

The Supreme Court on Friday issued an order that will maintain status quo access to the abortion and miscarriage drug mifepristone as the legal battle over the Food and Drug Administration's approval and regulation of the drug continues. The court did not explain its reasoning, but noted that Justices Clarence Thomas and Samuel Alito dissented.

The ruling overrides an order from the Court of Appeals for the 5th Circuit in New Orleans, which would have curtailed access to the drug as the federal government pursues an appeal of a district court ruling. That ruling, issued by conservative District Judge Matthew Kacsmaryk on April 7, would have revoked access to the drug entirely, finding the FDA's 2000 approval of mifepristone was unlawful, as was the agency's subsequent actions.

A three-judge panel for the appeals court, however, determined that the plaintiff's in the case—a group of anti-abortion organizations and individuals, led by the Alliance for Hippocratic Medicine—had exceeded the statute of limitations in which they could have legally challenged the FDA's 2000 approval. But, the judges ruled in a 2-1 decision to allow the rest of Kacsmaryk's ruling, revoking the FDA's actions in 2016 and 2021, which eased restrictions and access to the drug.

If the restrictions had been reinstated, it would have meant mifepristone would only be available for seven weeks into a pregnancy, not 10; that women would be required to go to three in-person doctor visits, rather than just one, possibly via telemedicine; the drug would not be allowed to be dispensed through the mail; and that doctors would have again been required to report all non-fatal adverse events.

Advertisement
In an appeal to the high court, Danco Laboratories, the maker of mifepristone (brand name Mifeprex), said the appeals court ruling created “debilitating uncertainty” and a “regulatory mess.” It wrote in its appeal:

> *In order to distribute Mifeprex under something other than the 2023 REMS [the FDA’s latest regulations], Danco must: revise product labels, packaging, and promotional materials; recertify providers; and amend its supplier-and distributor-contracts and policies (among other things). All of these are currently based on the 2023 REMS. So is Danco’s current distribution model. Before Danco can make any changes, however, it must have a new REMS—which will require Danco to submit and FDA to approve a supplemental NDA (sNDA). That process typically takes months. It is unclear whether Danco can continue distributing Mifeprex while that sNDA is pending before FDA even though it would technically be misbranded, or whether doing so would expose Danco to civil and criminal penalties. And then Danco might be required to jump through all of these hoops again if the injunction is ultimately modified or rescinded on appeal.*

Further complicating the matter is a ruling from a district judge in Washington that barred the FDA from altering access to mifepristone in 17 states and the District of Columbia. And on Wednesday, GenBioPro, the maker of the generic mifepristone that was approved by the FDA in 2019, sued the FDA to block the agency from complying with any order to remove the generic from the market.

Overall, the case is the first time an inexpert district judge has ruled to vacate an FDA approval based partly on the argument that the FDA erred in its expert scientific analysis. If the anti-abortion groups ultimately prevail in the appeal, it will set a dangerous precedent, opening the floodgates for litigation to second-guess the FDA’s authority in regulatory

actions and approvals and throwing drug development into chaos, according to legal experts, former federal officials, and numerous members of the pharmaceutical and biotech industry.

The court of appeals has placed the case on an expedited schedule and plans to hear the first oral arguments on May 17.

https://arstechnica.com/?p=1933736

Tesla beats Autopilot lawsuit as jury rejects crash victim's claim

Getty Images | NurPhoto

reader comments

154 with

Share this story

Tesla today defeated a lawsuit that claimed its Autopilot technology caused a car crash that left the plaintiff with severe injuries.

"A California state court jury on Friday handed Tesla a sweeping win, finding that the carmaker's Autopilot feature did not fail to perform safely in what appears to be the first trial related to a crash involving the partially automated

driving software," Reuters reported.

Justine Hsu sued Tesla in Los Angeles County Superior Court in 2020, saying Tesla's Autopilot technology in her Model S malfunctioned and caused the car to swerve into the road's center median so fast that she had no time to react. The lawsuit said the airbag deployed improperly during the July 2019 crash, "caus[ing] numerous breaks in Hsu's jaw and the loss of multiple teeth."

Hsu's lawsuit said she had undergone three surgeries and continued to require medical treatment. "Because of the Autopilot failure, and the improper deployment of the airbags, Plaintiff Hsu suffered severe injuries, resulting in a broken jaw, broken teeth, and multiple injuries to her face, hands, and legs," the complaint said.

Hsu sought over $3 million in damages, while Tesla argued "that Hsu used Autopilot on city streets, despite Tesla's user manual warning against doing so," according to Reuters. In addition to rejecting Hsu's Autopilot claim, the jury "found that the airbag did not fail to perform safely, and that Tesla did not intentionally fail to disclose facts to her," Reuters wrote.

Tesla is expected to face more trials over its automated-driving technology. One pending case was brought by five Texas police officers who were injured in February 2021 when a Tesla Model X in Autopilot mode crashed into police vehicles that were stopped and had their flashing lights turned on. There's also an ongoing investigation by the National Highway Traffic Safety Administration into crashes involving Tesla cars using Autopilot.

https://arstechnica.com/?p=1933684

Twitter stops labeling Russia’s RT and China’s Xinhua as “state-affiliated media”

Enlarge / RT’s Twitter profile, no longer labeled as “Russia state-affiliated media.”

reader comments

318 with

Share this story

Twitter has removed “government-funded” and “state-affiliated” labels from media accounts, including those of public broadcasters in the US and the accounts of state-controlled news organizations in China and Russia. The RT and Xinhua Twitter accounts were previously labeled “Russia state-affiliated media” and “China state-affiliated media,” but those labels disappeared sometime yesterday or today.

RT describes itself on its Twitter profile as promoting “freedom over censorship, truth over narrative,” and the profile now has no indication that it’s controlled by the Russian government. China’s Xinhua state news agency, also now unlabeled by Twitter, calls itself “public media for the public good” that doesn’t “yield to the pressure of ideological stigmatization and political bias.”

Other state-affiliated media outlets had their labels removed by Twitter. “State-backed Dot Dot News posted a screenshot of its Twitter account on Friday with a caption that said: ‘the label is gone! China state-affiliated media is gone,'” the Hong Kong Free Press wrote. Dot Dot News is located in Hong Kong but is described as being pro-Beijing. Hong Kong broadcaster RTHK lost its state-affiliated media tag as well.

Chinese state media outlets Global Times, People’s Daily, and CGTN had their labels removed, the report said, adding that personal accounts of state-media journalists are no longer labeled. “Twitter is blocked in China, however many Chinese outlets, officials and journalists circumvent the block to use it,” the report said.

Twitter also recently stopped limiting the reach of tweets from certain government accounts by removing the “visibility filtering rules” previously applied to those accounts, NPR reported today. “The previous guardrails on government accounts in Russia, China and Iran have now been removed, according to two former Twitter employees who spoke to NPR on the condition of anonymity for fear of retribution,” NPR wrote.

Labels removed from NPR, PBS, CBC, and BBC

At the same time that state-affiliated labels were deleted, Twitter removed “government-funded” labels recently applied to NPR, PBS, and the Canadian Broadcasting Corporation (CBC). Twitter similarly removed the “publicly funded media” label recently applied to the BBC.

In early April, Elon Musk’s Twitter controversially labeled NPR as “US state-affiliated media,” the same designation typically applied to propaganda outlets controlled by governments in countries without substantial free press

protections. Musk later changed NPR's tag to "government-funded media," even though NPR gets less than 1 percent of its annual funding directly from the US government.

Advertisement
NPR stopped posting on Twitter in response. PBS and the CBC did the same after getting their own government-funded labels.

There was some speculation that the removal of government-funded and state-affiliated labels was accidental, given that it happened while Twitter was removing blue checkmarks from accounts that don't pay for a subscription. But the main Twitter policy page that described the government-funded and state-affiliated labels was deleted entirely, suggesting the change is intentional.

Twitter's media-labeling policy used to say that "State-financed media organizations with editorial independence, like the BBC in the UK or NPR in the US for example, are not defined as state-affiliated media for the purposes of this policy." Twitter removed that part after Musk decided to apply labels to NPR and the BBC.

You can still read the old policy at a different Twitter help page. That one was never updated to remove NPR and the BBC, so it was out of date even before this week.

The page also still explains Twitter's previous policy of labeling state-controlled media accounts. "We believe that people benefit from additional context when interacting with Chinese government and state-affiliated accounts," the page says. "Labels on state-affiliated accounts provide additional context about accounts that are controlled by certain official representatives of governments, state-affiliated media entities and individuals closely associated with those entities."

Label for independent public media “misleads audiences”

A group of public broadcasters called the Global Task Force for public media had called on Twitter to remove the government-funded label from organizations with editorial independence, specifically the Australian Broadcasting Corporation (ABC), the CBC, Korean Broadcasting System (KBS), and Radio New Zealand (RNZ).

“Twitter’s own policy defines government-funded media as cases where the government ‘may have varying degrees of government involvement over editorial content,’ which is clearly not the case with ABC, CBC/Radio-Canada, KBS or RNZ,” the group said. “The editorial independence of all four national public broadcasters is protected in law and enshrined in their editorial policies. Labelling them in this way misleads audiences about their operational and editorial independence from government.”

A CBC spokesperson said on Friday that the news organization is “reviewing this latest development and will leave our [Twitter] accounts on pause before taking any next steps.”

We asked NPR and PBS about the label removals and will update this article if we get any response. We contacted Twitter’s media relations email address today and received the customary auto-replied poop emoji in return.

https://arstechnica.com/?p=1933609

Twitter permanently suspended journalist who interviewed Matt Walsh’s hacker

reader comments

128 with

Share this story

This week, The Daily Wire podcast host Matt Walsh got hacked, leading a hacker called Doomed to gain unfettered access to his Twitter, Google, and Microsoft accounts. A journalist named Dell Cameron then tweeted to encourage the hacker to contact him and then published the resulting interview with Doomed for Wired. Tweeting out that story—Cameron confirmed on Mastodon—ultimately got the tech policy reporter permanently suspended from Twitter for violating the social platform’s policy on distributing hacked materials.

Now, Walsh is threatening to sue “members of the media who openly solicited stolen information” from his phone, he tweeted. Announcing that The Daily Wire’s team was assisting him with legal counsel, he warned journalists like Cameron that he could afford to hire “very good lawyers.”

Walsh could not immediately be reached for comment. Cameron declined to comment. Yesterday, Wired tweeted a statement from its managing editor, Hemal Jhaveri.

“WIRED learned Wednesday afternoon that senior reporter Dell Cameron’s Twitter account was permanently suspended after he

reported on Matt Walsh's Twitter account being hacked," Jhaveri's statement read. "Neither Dell's story nor his Twitter feed contained hacked materials. We do not believe his account violated Twitter's policy. We have not received any further explanation from Twitter and our attempts to reach Twitter's press office were met with the customary poop emoji. We ask that the account be reinstated, and that Twitter provide an explanation."

Since Cameron's suspension, there has been debate over whether the journalist's report violated Twitter's policy and whether Walsh has any legal standing to sue a journalist like Cameron for reporting on the hack.

Twitter sometimes defers to "editorial judgment"

Twitter's hacked materials policy was last updated in October 2020, after the scandal where the platform blocked a New York Post article reporting on Hunter Biden's hacked laptop.

The current policy targets hackers who illegally obtain private information, as well as groups "associated with a hack." It defines hacked materials as "information obtained through a hack" that "need not be personally-identifiable private information in order to qualify as hacked materials under this policy."

Advertisement
According to the policy, it's against the rules to share any "private information without consent, regardless of how the private information was obtained." It's also against the rules to post tweets linking to "hacked content hosted on other websites," which is possibly what Twitter considers Wired's report on the hack. On Thursday afternoon, Wired editor-in-chief Gideon Lichfield tweeted that Twitter told Cameron that he "had broken its rules" by "directly distribut[ing] content

obtained through hacking that contains private information, may put people in physical harm or danger, or contains trade secrets."

In Wired's report, Cameron interviews the hacker, who goes by the alias Doomed, and reveals that Doomed's motivation was to "stir up controversy and sow chaos on Twitter" by posting absurd tweets using Walsh's handle. Some of these tweets threw "jabs" at some of Walsh's conservative colleagues, including podcaster Joe Rogan and Daily Wire host Ben Shapiro.

To verify the hacker was the same person who seemingly had access to Walsh's accounts, Cameron reviewed "several screenshots" of hacked materials and described some of those screenshots in the report. He also quoted from some of the hacked emails, which, under Twitter's policy, could be considered hosting "hacked content." Lichfield contended in a tweet that the email quotes were "benign" and did not "publish hacked materials."

Twitter's policy, however, also includes an exception for when hacked materials are used as source materials that can "serve as the basis for important reporting by news agencies meant to hold our institutions and leaders to account." In that section, Twitter says it will "defer" to the "editorial judgment" of media outlets publishing hacked materials, which Twitter considers "indirect distribution."

Because Walsh is a public figure but not an "institution" or a "leader," it's possible that the exception for newsworthy reporting on hacks does not apply to the Wired story. But the policy also notes that the exception is only intended for when media outlets share the actual hacked materials, not when media outlets are simply "discussing hacked materials." The logic is a little circular. Twitter says that reports discussing hacked materials "would not be considered a violation of this policy unless materials associated with the hack are directly distributed in the text of a Tweet, in an

image shared on Twitter, or in links to hacked content hosted on other websites.”

Wired has asked Twitter to reinstate Cameron’s account, but for now, it remains permanently suspended, which is a fate normally reserved for “accounts engaged in the direct distribution of hacked materials which are found to be directly operated by hackers, hacking groups, or people acting for or on behalf of such hackers.”

https://arstechnica.com/?p=1933486

Man battling Google wins $500K for search result links calling him a pedophile

reader comments

102 with

Share this story

A Montreal man spent years trying to hold Google accountable for search results linking to a defamatory post falsely accusing him of pedophilia that he said ruined his career. Now Google must pay $500,000 after a Quebec Supreme Court judge ruled that Google relied on an “erroneous” interpretation of Canadian law in denying the man’s requests to remove the

links.

“Google variously ignored the Plaintiff, told him it could do nothing, told him it could remove the hyperlink on the Canadian version of its search engine but not the US one, but then allowed it to re-appear on the Canadian version after a 2011 judgment of the Supreme Court of Canada in an unrelated matter involving the publication of hyperlinks,” judge Azimuddin Hussain wrote in his decision issued on March 28.

Google did not immediately respond to Ars’ request to comment.

The plaintiff was granted anonymity throughout the proceedings. Google has been ordered not to disclose any identifiable information about him in connection to the case for 45 days. The tech company must also remove all links to the defamatory post in search results viewable in Quebec.

Described in the judge’s order as a “prominent businessman” in both the United States and Canada who was once at the “pinnacle of the commercial real-estate brokerage world,” the man discovered the defamatory post in April 2007 when he “Googled” himself after several clients declined to do business after a series of good meetings. He found that a website called RipoffReport.com had published the post in April 2006, falsely stating that he was a con man and “convicted of child molestation in 1984.” The founder of that website refused to remove the post—responding to emails that he never removed posts and asking the man to provide proof that he was never charged with the crime. Hussain described the website’s request as “a Kafkaesque reverse-burden demand to prove one’s innocence.”

The man then learned that it was too late to sue to have the RipOffReport post removed. In Canada, “the action must be brought within one year of its appearance, regardless of when the victim of the defamation sees the publication,” the judge’s order noted.

Advertisement
Unable to get the post scrubbed online, the man then turned to Google to at least make the post less discoverable. For years, Google went back and forth, sometimes complying with the requests to remove and sometimes refusing them, as the links kept resurfacing. Friends of the man testified that he had lost out on business due to the confusion when potential clients Googled his name, and one of his sons had to distance himself from his father because he worked in real estate.

After the man sued, Google first argued that under Section 230 of the Communications Decency Act in the US, the company was not liable for third-party content and had no obligation to remove the links. Pointing to the Canada-United States-Mexico free trade agreement, Google suggested that Quebec's law requiring companies to remove illegal content once they're aware of its existence wouldn't apply, partly because it conflicted with Section 230.

Hussain didn't buy into Google's logic, but he also didn't assess punitive damages because he said that Google had refused to remove the links under the "good faith belief" that it was legally allowed to ignore the man's requests. While this particular case sided with the plaintiff, however, Hussain also said that it likely wouldn't trigger a slew of similar cases forcing Google to remove links, writing in his order:

> *"This case raises unprecedented questions in Quebec law about the liability of a company like Google, which provides internet search-engine services, for making available to users of its search engine a defamatory internet post, made by a third party and appearing on the site of yet a different third party, despite being on notice that it is facilitating access to an illicit activity, namely defamatory content. However, the conclusion of the Court in the present judgment finding liability on the part of Google does not open the floodgates to defamation litigation against it or other*

Internet intermediaries."

Instead of compensatory and punitive damages originally sought—amounting to $6 million—the man was awarded $500,000 for moral injuries caused after successfully arguing that he lost business deals and suffered strains on his personal relationships due to being wrongly stigmatized as a pedophile.

Hussain described the plaintiff's experience battling Google to preserve his reputation as a "waking nightmare." Due to Google's refusals to remove the defamatory posts, the man "found himself helpless in a surreal and excruciating contemporary online ecosystem as he lived through a dark odyssey to have the Defamatory Post removed from public circulation," Hussain wrote.

The plaintiff, now in his early 70s, has the option to appeal the judge's order that Google may not release any of his identifiable information for 45 days. Ars could not immediately reach the plaintiff's lawyers to confirm if he would be appealing.

https://arstechnica.com/?p=1933437

Election conspiracist Mike Lindell must pay $5M to expert who proved him wrong

Enlarge / MyPillow CEO Mike Lindell speaks during the

Conservative Political Action Conference (CPAC) on March 4, 2023, in National Harbor, Maryland.
Getty Images | Alex Wong

reader comments

227 with

Share this story

Election conspiracy theorist Mike Lindell was ordered to pay $5 million to the electrical engineer and inventor who won the "Prove Mike Wrong" contest in which Lindell offered the prize to anyone who could prove that his data had nothing to do with the 2020 presidential election.

Lindell, the My Pillow CEO who helped finance Donald Trump's baseless election protests, was ordered to pay Robert Zeidman $5 million within 30 days in a ruling issued yesterday by the American Arbitration Association Commercial Arbitration Tribunal.

"Based on the foregoing analysis, Mr. Zeidman performed under the contract," a three-member arbitration panel wrote. The panel found that Zeidman proved the files provided by Lindell to contest participants did not contain actual data from the election.

Zeidman proved that Lindell's data "unequivocally did not reflect November 2020 election data. Failure to pay Mr. Zeidman the $5 million prized was a breach of the contract, entitling him to recover," the panel said.

"I am obviously really happy about the arbitrators' decision," Zeidman said in a press release issued by his lawyers. "They clearly saw this as I did—that the data we were given at the symposium was not at all what Mr. Lindell said it was. The truth is finally out there."

The arbitration “decision declares unequivocally that Zeidman proved Mike wrong,” the press release said. The arbitration panel’s ruling chided Lindell for defining “election data” too broadly:

> *In fact, it would be unreasonable to conclude that any data about the election is “election data.” Newspaper articles and broadcast news about the election are transmitted as data over the Internet, for example. It is unreasonable to conclude that any data file containing those accounts—or excerpts from such a file—would qualify as election data in a contest. If such data qualified, the Contest would not really be a contest at all.*

“This will be going to court!”

Lindell appears to be ready to challenge the ruling in court. “They made a terribly wrong decision! This will be going to court!” he told The Washington Post in a text message.

Advertisement
Lindell gave a similar response to CNN. “In a brief phone interview with CNN, Lindell said ‘this will end up in court’ and slammed the media and professed the need to get rid of electronic voting machines,” CNN reported.

Zeidman’s attorney, Brian Glasser, told The Washington Post that the arbitration decision can’t be appealed directly. Paraphrasing Glasser, the Post wrote that “Lindell could ask a federal court to quash it on the basis that it represented a ‘manifest injustice.’ The statutory grounds for such a claim are narrow, and it is ‘extremely rare’ for such a claim to succeed, according to Glasser.”

Lindell claimed he possessed a great deal of data captured from the Internet during voting in the November 2020 US election, and that his data showed China interfered with the

November 2020 election in several states.

“Mr. Lindell testified that he was frustrated that his statements about China’s election interference were not being taken seriously, and so decided to hold a ‘Cyber Symposium,'” the ruling said. “The purpose of the symposium was to provide the data he had to prove China’s interference in the November 2020 election. He invited the press, politicians, and cyber experts to attend the symposium, which took place in Sioux Falls, South Dakota, on August 10 and 11, 2021.”

Lindell promised to provide “cyber data and packet captures from the 2020 November election” and announced the Prove Mike Wrong contest. The contest announcement said that participants “have one goal. Find proof that this cyber data is not valid data from the November Election. For the people who find the evidence, 5 million is their reward.”

Lindell conceded at the arbitration hearing that he doesn’t have the ability to analyze the files himself and thus relied on experts who “assured him that the data was real and proved China’s interference with the election.”

https://arstechnica.com/?p=1933403

Twitter quietly edited its hateful conduct policy to drop transgender protections

Aurich Lawson | Stable Diffusion

reader comments

379 with

Share this story

Earlier this month, Twitter quietly removed transgender-specific protections from its hateful conduct policy, drawing criticism from advocates who say there has been a spike in anti-LGBTQ rhetoric since Twitter CEO Elon Musk took over the platform last year.

An archived version of Twitter's prior policy, dated April 7, clearly stated that Twitter prohibited "targeting others with repeated slurs, tropes or other content that intends to dehumanize, degrade or reinforce negative or harmful stereotypes about a protected category. This includes targeted misgendering or deadnaming of transgender individuals." ("Deadnaming" refers to calling a trans person by their former name.)

But on April 8, the policy language changed to strike that last line. That edit effectively removed transgender-specific protections that were first implemented in 2018 to address a disproportionate amount of hate speech targeting transgender users, The Verge reported that year.

"This is just one of many moves since Musk's takeover of Twitter that has made the platform more and more unsafe for LGBTQ people and advertisers," Sarah Kate Ellis, president and CEO of the Gay & Lesbian Alliance Against Defamation (GLAAD), told Ars.

Ellis told Ars that the policy update is "unacceptable" because of "the barrage of disinformation and hate about trans people from right-wing media personalities, politicians, and the extremists they bolster." She also said that Twitter's decision "only further erodes the trust between Twitter and

its users and advertisers."

Yesterday, Musk attempted to woo advertisers—many of which are worried about branded tweets appearing next to hate speech—back to Twitter while also standing his ground on his policy of limiting the reach of some hate speech rather than banning it entirely. While speaking at a Miami Beach marketing conference, Musk said "he was eager to hear legitimate concerns that advertisers might have about Twitter, but he emphasized that he wouldn't succumb to pressures to make changes he doesn't believe in," The Wall Street Journal reported.

"It's totally cool to say that you want to have your advertising appear in certain places of Twitter and not in other places," Musk told conference attendees. "But it is not cool to say what Twitter will do. And if that means losing advertising dollars, we'll lose them. But freedom of speech is paramount."

Advertisement

Musk has said that some advertisers have either returned to Twitter or are planning to soon. However, the WSJ reported that third-party data from market intelligence firm Sensor Tower showed that out of 100 top Twitter advertisers, 30 advertisers have spent nothing on Twitter so far this year, and 24 advertisers had reduced their spending on Twitter by 80 percent or more.

Some advertisers told Forbes that they were most concerned about racist tweets, but Kayla Gogarty, the deputy research director for the left-leaning nonprofit Media Matters, authored a study last December showing a significant spike in anti-LGBTQ rhetoric on Twitter since Musk took over.

Gogarty tracked retweets and mentions of nine accounts that frequently use the slur "groomer"—which is commonly used to refer to a right-wing conspiracy theory suggesting that LGBTQ

education is used to exploit minors—and documented an increase of over 1,200 percent. Before Musk became CEO, retweets and mentions of these accounts tweeted about “groomers” 3,600 times. After his takeover, the number jumped to 48,000. Gogarty told Ars that Twitter’s rollback of transgender protections “is another reason why advertisers” who don’t want branded tweets next to anti-LGBTQ rhetoric “should be very skeptical” about returning to the platform.

In November 2022, when Musk’s revamped Twitter Blue subscription initially rolled out, the digital rights organization the Electronic Frontier Foundation (EFF) reported that there was a “wave of abuse” from “anti-trans trolls, far-right extremists, and conspiracy mongers.” The abuse reportedly contributed to Musk’s decision to pause the Twitter Blue rollout, but Gogarty told Ars that since Twitter Blue has been available again, the blue check now “gives a veneer of credibility” to anti-LGBTQ users who expect that their paid subscription will increase the visibility of anti-LGBTQ posts on the platform.

At the marketing conference, Musk promised advertisers that his plan was to achieve a “sensible middle ground” where Twitter remains a “valuable” platform to brands by limiting the reach of hate speech instead of removing it.

“If somebody has something hateful to say, it doesn’t mean you should give them a megaphone,” Musk said. “We’re not going to recommend hateful content to people.”

This month, Twitter also published a blog post further explaining its plan to label potentially harmful speech and promising that “we will not place ads adjacent to content that we label.”

Gogarty told Ars that Media Matters would continue to monitor hate speech on the platform.

https://arstechnica.com/?p=1933162

FBI and others urge Meta to halt encryption plans, citing child abuse risk

Getty Images | Olemedia

reader comments

114 with

Share this story

The long-running battle over encryption between tech companies and law enforcement continues, with law enforcement agencies around the world calling on Meta to cancel plans for end-to-end encryption of Facebook and Instagram messages.

End-to-end encryption (often called “E2EE”) boosts security and privacy for all users, whether law-abiding or not. But government officials have long opposed plans to make the technology more widely available, citing the risk that terrorists, sex traffickers, child abusers, and other criminals will use encrypted messages to evade law enforcement.

The latest call to abandon encryption plans was made today by the Virtual Global Taskforce, a consortium of 15 law enforcement agencies, including two from the US: the FBI and ICE Homeland Security Investigations. The task force focuses specifically on child sexual abuse; other members include

Europol and agencies from the UK, Canada, Colombia, Australia, New Zealand, Kenya, the Philippines, the United Arab Emirates, the Netherlands, and South Korea.

“The announced implementation of E2EE on Meta platforms Instagram and Facebook is an example of a purposeful design choice that degrades safety systems and weakens the ability to keep child users safe,” the global task force said in a statement on the UK National Crime Agency’s website.

“Meta is currently the leading reporter of detected child sexual abuse to NCMEC,” the task force said, referring to the US-based National Center for Missing & Exploited Children. Meta hasn’t provided any indication “that any new safety systems implemented post-E2EE will effectively match or improve their current detection methods,” according to the group.

“The abuse will not stop just because companies decide to stop looking,” the group also said, accusing Meta and other tech companies of “blindfolding themselves to child sexual abuse.”

End-to-end encryption is available in Facebook Messenger and Instagram as an option, but the law enforcement statement was likely spurred by Meta’s plan to turn the security feature on by default in Facebook Messenger sometime this year. The Meta-owned WhatsApp already has end-to-end encryption enabled by default.

Advertisement

Meta: People don’t want us reading private messages

When contacted by Ars, Meta provided a statement in response to the Virtual Global Taskforce:

> *Most Americans already rely on apps that use encryption to*

> *safely transfer money, talk to doctors, and communicate privately. We don't think people want us reading their private messages, so have developed safety measures that prevent, detect and allow us to take action against this heinous abuse, while maintaining online privacy and security. As we continue to roll out our end-to-end encryption plans, we remain committed to working with law enforcement and child safety experts to ensure that our platforms are safe for young people.*

A Meta spokesperson said the company's plan to make end-to-end encryption the default in Facebook Messenger is still on track to be completed this year. "End-to-end encryption is already optional on Messenger. Our plan is to fully roll it out, and make it default for Messenger users, sometime in 2023. We provide regular updates on our progress," Meta said. The plan for default end-to-end encryption applies to Instagram messages, too, but the Instagram rollout may not happen in 2023, the spokesperson said.

Apple has had long-running disputes with the US government over encryption, and Facebook has faced a steady drumbeat of calls to remove encryption the past few years. "Since about 2018 the main narrative of law-enforcement and intelligence agencies has been that the end-to-end cryptography in messenger products such as WhatsApp makes life too easy for sexual predators, while the introduction of end-to-end encryption in Facebook Messenger is now claimed to pose an additional risk to children," said a 2022 paper by Ross Anderson, a security expert and professor at the University of Cambridge.

https://arstechnica.com/?p=1933073

Fox News to pay Dominion $788 million in settlement, ending defamation trial

Enlarge / A mobile billboard deployed by advocacy group Media Matters drives past a courthouse on April 17, 2023, in Wilmington, Delaware.
Getty Images | Jemal Countess

reader comments

260 with

Share this story

Fox News Network and Dominion Voting Systems today reached a $787.5 million settlement, ending a trial in Dominion's defamation lawsuit against Fox just before opening arguments would have been heard.

"Over two years ago, a torrent of lies swept Dominion and election officials across America into an alternative universe of conspiracy theories, causing grievous harm," Dominion attorney Justin Nelson said in a press conference today, according to CNN.

Nelson revealed the $787.5 million settlement figure during the press conference. He said the deal provides "vindication and accountability," showing that "the truth matters, lies have consequences."

The trial was originally scheduled to begin in Delaware Superior Court yesterday, but the start was delayed one day

because the sides were holding settlement talks. A 12-person jury was selected Tuesday, and opening statements were slated for this afternoon. But there was another delay, which was followed by the settlement announcement.

“We acknowledge the court’s rulings finding certain claims about Dominion to be false,” Fox said in a statement, according to Reuters. “This settlement reflects Fox’s continued commitment to the highest journalistic standards. We are hopeful that our decision to resolve this dispute with Dominion amicably, instead of the acrimony of a divisive trial, allows the country to move forward from these issues.”

Fox News apparently won’t have to apologize on air. “Under the terms of the settlement, Fox News will not have to apologize or admit to spreading false claims on network programming, according to a person familiar with the details of the agreement,” The New York Times wrote.

Judge ruled Fox News aired false statements

On March 31, Judge Eric Davis ruled that Fox News aired false statements about Dominion related to the 2020 presidential election. These statements were defamatory *per se* because they “claimed that Dominion committed election fraud; manipulated vote counts through its software and algorithms; is founded in Venezuela to rig elections for dictator Hugo Chavez; and paid kickbacks to government officials who used the machines in the Election,” he wrote.

Advertisement
“While the Court must view the record in the light most favorable to Fox, the record does not show a genuine issue of material fact as to falsity,” Davis wrote. Davis said it was “crystal clear” that none of the Fox News statements challenged by Dominion were true. “Therefore, the Court will

grant summary judgment in favor of Dominion on the element of falsity," he wrote.

If the trial had gone forward, jurors would have had to decide whether Fox News acted with actual malice. If Dominion won, jurors would have had to calculate damages to be awarded to Dominion, which asked for $1.6 billion.

Davis announced the settlement in court shortly before 4 pm ET, CNBC wrote. "Without you, the parties would not have been able to resolve their situation," Davis reportedly told jurors. "Although it's short, not the six weeks you've expected, you have done your duty."

We contacted Fox News and Dominion today and will update this article if we get additional information on the settlement terms.

Dominion separately sued Newsmax and One America News Network. Voting machine maker Smartmatic also sued all three networks.

Smartmatic attorney J. Erik Connolly reportedly issued a statement saying that "Dominion's litigation exposed some of the misconduct and damage caused by Fox's disinformation campaign," and "Smartmatic will expose the rest. Smartmatic remains committed to clearing its name, recouping the significant damage done to the company, and holding Fox accountable for undermining democracy."

Newsmax provided a statement saying it "believes that the facts at issue in Dominion's case against it are materially different from those that may have driven Fox to settle, and no conclusion about Newsmax should be drawn from that settlement. Newsmax stands by its coverage and analysis of the 2020 election and will continue to vigorously defend against the claim."

https://arstechnica.com/?p=1932901