IT Sector Accounts for Nearly One Third of U.S. Securities Litigation Risk in 1H 2026

AIJ aijourn.com/it-sector-accounts-for-nearly-one-third-of-u-s-securities-litigation-risk-in-1h-2026

BETHESDA, Md., July 31, 2026 /PRNewswire/ — Securities Analytics Research (SAR), a data analytics company specialized in the securities litigation risk of U.S. public companies, today published the *U.S. Securities Litigation Risk Report – 1H 2026*.

According to the semi-annual report, single-firm event study analyses on 11,557 corporate disclosures from a population of 4,648 U.S. public companies, indicate that NYSE and NASDAQ issuers exhibited approximately $17.4 trillion in market capitalization losses during the two-year period ending June 30, 2026. These losses reflect the cumulative, statistically significant single-day stock price declines associated with High-Risk Adverse Corporate Events ("ACEs") identified and analyzed through the proactive and uniform application of the court-approved event study methodology.

SAR's verifiably independent event study analyses on the universe of corporate disclosures involving both public statements and filings made with the U.S. Securities and Exchange Commission ("SEC") over the same trading session indicate that both average frequency and aggregate severity of High-Risk ACEs increased by 1.86% and 23.4%, respectively, relative to the two-year period ending December 31, 2025.

"Our data confirm that U.S. public companies are facing a demonstrable increase of $3.3 trillion, or 23.4%, in securities litigation risk based on the frequency and severity of high-risk adverse corporate events over the past six months. Notably, the IT sector alone accounts for nearly a third of this quantum," said Nessim Mezrahi, Co-Founder and CEO of SAR.

According to the report, eight of the eleven GICS® sectors exhibited an increase in the frequency of High-Risk ACEs during the first half of the year. In the aggregate, U.S. public companies face an increase of $3.29 billion in the two-year market capitalization loss accumulation relative to December 31, 2025. On average, market capitalization losses per High-Risk ACE have increased by $267.4 million, or 21.6%, over the preceding six months.

As of June 30, 2026, nearly 62% of U.S. securities litigation risk was embedded in the Financials, Health Care, and Information Technology sectors. Real Estate, Energy, and Financials saw the largest percentage increases in the average frequency of High-Risk ACEs during the preceding six months, at 21.8%, 16.0%, and 10.8%, respectively. Information Technology, Financials, and Health Care exhibited the greatest increase in market capitalization losses linked to High-Risk ACEs with $1,588.98, $738.75, and $289.16 billion respectively.

Health Care exhibited the highest median *SAR Risk Score*® at 27.55%, followed by Consumer Discretionary at 24.57%, and Consumer Staples at 24.45%. Information Technology continues to face the greatest market capitalization losses per High-Risk ACE, amounting to $3.39 billion, followed by Communication Services and Consumer Staples with $2.48 and $1.79 billion, respectively.

This independent, semi-annual U.S. equity risk management research report presents an appendix with the median *SAR Risk Score*® across all GICS® groups, industries, and sub-industries. The *SAR Platform*® equips users with the near real-time quantification of securities litigation risk with transparency at the corporate disclosure level and the probability of facing a securities class action lawsuit for companies listed on the NYSE or NASDAQ.

Privacy & Cybersecurity

Anthropic AI Models Hacked Three Organizations During Tests (2)

July 31, 2026, 3:34 AM PDT

Summary by Bloomberg AI AI Generated

- Anthropic PBC said its artificial intelligence models breached three organizations during cybersecurity tests that went awry, after performing a review of its own cybersecurity tests following OpenAI's announcement of a breach.
- The company reviewed 141,006 evaluation tests and found three instances in which its Claude AI tool accessed the internet and then hacked into "the real-world infrastructure of external organizations".
- The breaches involved three different Claude models and occurred when Anthropic was using evaluation environments built by the AI security firm Irregular, with Anthropic saying it could have done more to review network logs and evaluation transcripts.

Anthropic PBC said its artificial intelligence models breached three organizations during cybersecurity tests that went awry, a little more than a week after its chief rival, OpenAI, disclosed a similar incident.

Anthropic said in a blog post Thursday that it made the discovery after performing a review of its own cybersecurity tests, following OpenAI's announcement of a breach. In both the OpenAI and Anthropic tests, the AI models were able to access the internet from within testing environments that should have been sealed off, according to Anthropic's blog.

Here’s what we know so far about Anthropic’s AI models breaching three organizations during cybersecurity tests which went awry. Source: Bloomberg

The company said it reviewed 141,006 evaluation tests and found three instances in which its Claude AI tool accessed the internet and then hacked into “the real-world infrastructure of external organizations.” The earliest incidents date to April, the company said.

The affected organizations aren’t named in the blog.

When Anthropic’s models gained unauthorized access to the three organizations, it treated each of them as part of an exercise. The tests were “capture-the-flag” evaluations in which the models sought hidden information by breaching other systems, a common way to test hacking capabilities for both humans and AI. However, the older model continued its attack even after getting evidence that it was running on the open internet; Anthropic’s most recent model stopped after recognizing it was on the internet, according to the blog.

Anthropic headquarters in San Francisco on April 30, 2026.
Photographer: Jason Henry/Bloomberg

Read More: OpenAI Models Hacked Another Company’s Systems by Mistake

The spate of accidental AI-caused hacks is already prompting some politicians to call for federal guardrails or other oversight of AI technology. More than 1,100 staffers across artificial intelligence firms also signed a petition on Tuesday, as Bloomberg first reported, that calls on the US government to support a mechanism that would help “deliberately pace” AI development to prevent the technology from advancing too fast.

Neither Anthropic nor the organizations that were breached had noticed the intrusions. In its blog, Anthropic said it could have done more to review network logs and evaluation transcripts.

The company disclosed the breaches nearly four months after it announced that it had developed a new AI model known as Mythos that was so powerful and potentially dangerous that the company strictly limited its release.

The breaches involved three different Claude models: Opus 4.7, Mythos 5 and an internal research test model, according to the blog. Each of the models ran without the safeguards normally implemented in public tools. Claude compromised the organizations using basic techniques such as exploiting weak passwords, according to the blog.

The incidents all occurred when Anthropic was using evaluation environments built by the AI security firm Irregular. In every case, Anthropic specified to Claude that its environment was a simulation and that it had no internet access.

“Due to a misunderstanding between us and our evaluation partner, this was not the case,” the blog says. An Irregular spokesperson said the company appreciates Anthropic’s collaboration and transparency. The company’s investigation is ongoing, the spokesperson said.

Anthropic said it regularly runs tests that involve simulating real cybersecurity challenges, calling them critical steps in developing and releasing models. However, the company also said it drew several lessons from the incidents, including that tests involving powerful autonomous capabilities also require significant controls.

“Safety testing happens before a model is released precisely because we don’t yet know what it is capable of,” the company said in its blog. “Evaluation environments increasingly need to be held to the same security standard as any other system our models run in.”

Anthropic was honest about the human failings that contributed to the hack, said Alan Woodward, professor of cybersecurity at the University of Surrey. The AI “hasn’t gone rogue — you’ve asked it to do something and left the gate open,” he said. “I think Anthropic were admitting that.”

(Updates with comments in final paragraph.)

--With assistance from Anna Boyne.

[Bloomberg Law](#)

[Manage Newsletters](#)

Bloom Energy Investor Sues Over Short Seller’s China Accusations

July 31, 2026, 8:39 AM PDT

Bloom Energy Corp. failed to alert investors that the fuel cell maker sourced a rare earth metal from China through intermediaries, putting its supply chain at risk of disruption, a proposed class action said.

The investor’s lawsuit, filed Thursday in the US District Court for the Northern District of California, draws from a short-seller report that accused Bloom of indirectly relying on China for the metal, scandium.

Hunterbrook Media on July 8 said Bloom obfuscated its reliance on China, which the US has tense relations with, by routing shipments through other countries. China could cut off Bloom’s supply regardless of how indirectly the company obtained the scandium, its report said.

“If Bloom depends on Chinese scandium, China holds an off-switch on Bloom — and on the American data centers that may one day use its power,” Hunterbrook said.

Bloom’s share price dipped 5.7% to close at $254.29 that day.

Bloom creates power systems that can be used onsite for multiple industries. Bloom’s financials have benefited from burgeoning demand to power artificial-intelligence computing data centers, with the company posting quarterly earnings more than double expectations and raising its full-year guidance earlier this week.

The company uses scandium in its solid oxide fuel cells. Bloom has reiterated it’s not dependent on China for scandium oxide, and denied the Hunterbrook report as false and misleading.

The proposed class includes investors who got Bloom securities from Feb. 27, 2025, to July 8, 2026. During this time, Bloom and top executives touted its diversified sourcing of scandium and understated its reliance on China, according to the complaint.

Glancy Prongay Wolke & Rotter LLP and Century City, Calif.-based attorney Frank R. Cruz represent the suing investor, Sashanna Nevins.

Nevins seeks damages for alleged securities fraud by Bloom Energy, its CEO, chief financial officer, and two former CFOs.

Bloom didn't immediately respond to an email seeking comment.

The case is Nevins v. Bloom Energy Corp. , N.D. Cal., No. 3:26-cv-07944, complaint filed 7/30/26 .

To contact the reporter on this story: Gillian R. Brassil in Washington at gbrassil@bloombergindustry.com

To contact the editor responsible for this story: Brian Flood at bflood@bloombergindustry.com

Judge signals Anthropic likely to prevail in First Amendment fight with Pentagon

DJ dailyjournal.com/articles/393370-judge-signals-anthropic-likely-to-prevail-in-first-amendment-fight-with-pentagon

A federal judge indicated Thursday she was deeply skeptical that the Trump administration did not violate the First Amendment when it labeled Anthropic PBC a national security supply chain risk over its refusal to allow the government to use its AI models for lethal autonomous warfare or mass surveillance.

U.S. District Judge Rita F. Lin of San Francisco peppered attorneys for Anthropic and the U.S. Department of Justice with questions during a hearing on motions for summary judgment by both sides.

The judge, an appointee of President Joe Biden, did not issue a ruling from the bench, saying she would issue a written order. She issued a preliminary injunction blocking the supply chain risk designation in March.

"I don't see additional evidence from the government really justifying what it did," Lin said at the outset of the hearing. "If anything, the record has gotten worse for the government." *Anthropic PBC v. U.S. Department of War et al.*, 26-cv-01996 (N.D. Cal., filed March 9, 2026).

The legal battle is not over whether the Department of Defense must continue to use Anthropic's products but whether the supply chain risk designation was a retaliatory violation of the First Amendment and the Administrative Procedure Act.

Lin repeatedly expressed concern that Secretary of Defense Pete Hegseth's declaration that, aside from eliminating the company's contract with the Defense Department, that "no contractor, supplier, or partner that does business with the United States military may conduct any commercial activity with Anthropic."

One of Lin's questions concerned how to apply an influential 1968 U.S. Supreme Court ruling in which the justices ruled an Illinois school district's decision to fire a high school teacher, Marvin L. Pickering, after he wrote letters critical of the board to a local newspaper. *Pickering v. Board of Education of Township High School District 205*, 391 U.S. 563 (1968).

The judge asked how the Pickering framework would apply if a company that had taken the position it would not produce surveillance drones that could be used for lethal purposes and the government put up billboards across the country labeling the company and its CEO "enemies of the state," warning others not to do business with the company.

Senior Trial Counsel James W. Harlow of the Justice Department disagreed that the designation was unconstitutional or a violation of the APA, adding that the secondary boycott "does not exist."

But he argued that the Trump administration had "lost trust" in Anthropic, raising concerns that company would "poison" the models it provides to the military. "There should be deference to the judgment of these [Defense Department] officials," Harlow said during the hearing.

Michael J. Mongan, a partner with Wilmer Cutler Pickering Hale and Dorr LLP who represents Anthropic, told Lin that the government has provided no evidence to support its allegation, and that the government's trust argument was a response to public criticism by company officials.

"They are all violations of the First Amendment," he said.

The losing side is expected to appeal Lin's ruling to the 9th U.S. Circuit Court of Appeals and the case is expected to wind up before the U.S. Supreme Court, which is dominated by appointees of Republican presidents.

"Defendants' actions neither infringe Anthropic's First Amendment right to speak about AI policy nor do they deprive it of a vested liberty or property interest," Harlow wrote in a brief.

Mongan, however, said the government's actions violate the U.S. Constitution. "Speaking with the press is a core First Amendment activity," he said. "It doesn't make [Anthropic] a supply chain risk. ... There has been a campaign of retaliation."

The legal dispute has raised questions over whether the government's designation might harm the San Francisco company, one of the country's leading and most valuable AI labs, as it prepares to file for an initial public offering, possibly later this year.

Stanford report finds investor claims rising with AI boom

DJ dailyjournal.com/articles/393360

Securities class action filings jumped 30% during the first half of 2026, driven largely by lawsuits alleging companies misled investors about artificial intelligence, according to a report released Wednesday by the Stanford Law School Securities Class Action Clearinghouse and Cornerstone Research.

The report found 121 new securities class actions were filed during the first six months of the year. Fifteen involved AI-related allegations, putting such filings on pace to nearly double last year's total of 16.

"The intelligence might be artificial, but the litigation is real," Stanford Law School professor Joseph Grundfest, the principal investigator for the Securities Class Action Clearinghouse, wrote in an email to the Daily Journal.

"The incidence of shareholder lawsuits always follows the money," Boris Feldman, partner and global co-head of tech, media and telecoms of Freshfields, noted. "Right now, all of the money is going into AI and related industries, data centers and the like."

The report reflects that trend. It suggests the industry's rapid investment in AI infrastructure is already reshaping securities litigation. Securities class actions against technology companies rose from nine during the second half of 2025 to 24 during the first half of this year.

Five AI-related filings involved data centers and seven involved AI development, illustrating how litigation is tracking the industry's heavy spending.

Three of the 15 AI-related class actions were filed in federal courts within the 9th U.S. Circuit, according to the report. Two were filed in Washington state and one in Nevada. The 2nd Circuit also had three filings, followed by the 3rd Circuit with three. The 1st, 5th and 6th Circuits each had one. Overall, the 2nd and 9th Circuits continued to be the nation's busiest venues for securities class actions, accounting for 70% of all core federal filings.

UCLA Law School professor James Park said the surge reflects the risks that accompany overheated markets. "We are in frothy market conditions, so there is always a significant risk of a downturn," he said. "When there is a downturn like that, investors will have more traction in their lawsuits if these companies see their stock prices fall by 50% or so. The potential damages can be quite significant."

The report bears that out. Although AI-related lawsuits accounted for just 13% of all filings, they represented 73% of the report's Disclosure Dollar Loss, a measure of the decline in a company's market value following alleged corrective disclosures. Overall, Disclosure Dollar Loss rose from $299 billion in the second half of 2025 to $529 billion in the first half of 2026.

"Volatility in the market generally leads to, or is a predictor of class actions. When stock prices decline in response to disappointments by 15, 20, 25% there is a possibility that plaintiffs will file class actions alleging that the companies did not disclose relevant information that they possessed in a timely manner," Cornerstone Research Senior Vice President Sasha Aganin said.

Park said investor enthusiasm for AI has encouraged companies to make increasingly ambitious public statements about their technology, giving plaintiffs' lawyers more disclosures to scrutinize if stock prices later decline.

While many AI issues are new, others fall under established statute and case law, noted Rachel Geman, a partner at Lieff Cabraser Heimann & Bernstein.

"It may be, for example, that 'old' torts and statutes, like nuisance, are the sensible vehicles to address some environmental issues with data centers," she said. Geman was co-lead class counsel in a copyright lawsuit against Anthropic that settled for $1.5 billion on July 20.

Feldman said he is not concerned with an increase in cases. He said judges are accustomed to seeing shareholder class actions.

"It's rare to have any emergency litigation in [these suits] and it's possible that over the longer haul, the AI wave will generate more work for judges in the judicial system on intellectual property issues than on securities law issues," Feldman said.

Park said he believes the courts are accustomed to surges and have tools to dismiss weak claims.

"Are there a few cases that will go on to trial? Sure, but it's more of an exception rather than a rule," he said. "I think it will keep the courts a bit busier, lawyers busier, but I don't think there's a real crisis at this point."

Park compared today's AI boom to the internet bubble of the late 1990s. "There are certainly similarities. ... But we have stronger controls now." For Aganin, the recent increase in securities filings may signal a broader trend rather than a temporary spike. "What we are seeing now with these 15 filings in the first half of the year is likely only the start."

As AI technology evolves, the scope of litigation can expand. Grundfest, a former SEC commissioner, wrote that while securities fraud claims have largely centered on AI infrastructure spending, other types of lawsuits are already emerging.

"Cornerstone's data suggests that disclosures surrounding the massive capital expenditures required to build data centers and to develop frontier AI models now dominate private securities fraud litigation," wrote Grundfest, "At the same time, retail users are filing class action complaints alleging that AI has promoted suicides, given bad medical advice, and caused other harms.

"Clearly, no matter the outcome of these cases, AI firms are going to have to lawyer up."

DEEP DIVE

Data Brokers Deny a Million Pleas to Delete Personal Information

July 31, 2026, 2:00 AM

By Cassandre Coyer

Data brokers operating in California have denied or ignored more than 1 million requests in the past two years to delete personal information they collected from online users, according to a Bloomberg Law review of company disclosures and interviews with industry professionals.

In some cases, the brokers acknowledged rejecting nearly all the requests they got to delete consumers' private data, the analysis shows.

Marketing intelligence provider VisitIQ LLC said it denied more than 270,000 petitions out of the 363,000 or so it logged in 2024. HealthWise Data, which makes AI-driven inferences about patients, reported getting 98,000 data deletion requests that same year but complied with fewer than 10,000.

California's privacy law required those data broker firms and hundreds of others to publicly and accurately report, starting in January 2024, how many data deletion requests they had fielded and how they responded. It does not require them to report why they don't comply, but gives them the option to deny a request if they believe it is illegitimate or can't be verified.

The hammer falls Saturday in the closely watched, first-in-the-nation data privacy law: Brokers will be fined $200 a day if they fail to comply with valid requests within 45 days of them being filed through the state's new deletion system.

The registered brokers not only face some of the highest fines in the privacy space — some estimate penalties could reach billions of dollars — but they'll also have to process requests from more than 350,000 Californians already registered to use the tool, dubbed the Delete Request and Opt-Out Platform, or DROP.

The system reflects growing efforts to rein in the largely unchecked sharing and selling of the very personal data collected every time someone shops online, clicks on a link or doomscrolls.

Tom Kemp, the executive director of California's privacy agency, said the state already assessed tens of thousands of dollars in fines against three brokers it determined had filed inaccurate registration information.

CalPrivacy wants its data broker registry to be "a source of truth," Kemp told Bloomberg Law in an interview Thursday. "I want to be very clear that data brokers have a legal obligation to provide only true and correct information."

Shifting Blame

Most brokers reported complying with millions of deletion requests, according to Bloomberg Law's analysis of the 2024 totals they self-reported to the state.

That tally also shows nearly 890,000 such requests were denied that year, the last one for which updated data is available. Industry experts say that was certainly an undercount and the total grew last year.

Brokers with High Deletion Denial Rates

Registered data brokers that received at least 5,000 deletion requests, and denied at least half of those requests in full

Broker	Requests Received	Requests Denied	Percent of Requests Denied
Keyword Connects LLC	5,201	5,201	**100%**
Live Data Technologies, Inc.	45,865	45,853	**99.97%**
Online Advertising Network sp. z o.o.	6,879	6,877	**99.97%**
DTN, LLC	6,218	6,202	**99.74%**
33 Mile Radius LLC	62,584	62,190	**99.37%**
Convex Labs LLC	35,214	34,548	**98.11%**
DealerX Partners LLC	11,541	11,157	**96.67%**
MarketOps LLC	11,541	11,157	**96.67%**
HealthWise Data	98,275	88,648	**90.2%**
Sterling Data Company LLC	7,390	6,654	**90.04%**
Apollo Interactive, LLC	15,040	13,539	**90.02%**
33Across, Inc.	10,478	8,468	**80.82%**
Zeta Global	137,625	110,100	**80%**

Source: California Privacy Protection Agency

In disclosures to California's privacy agency, some data brokers attributed their high denial rates to what they describe as "bogus" or incomplete consumer requests, challenges they face verifying users' identities, and discrepancies between the personal information they hold and what consumers want deleted.

Some also blame the privacy companies that increasingly act as paid middlemen, signing up users by pledging, for a fee, to stop the sale or exposure of their personal information. Brokers say those contractors sometimes send illegitimate requests, muddying the numbers that end up reported as denials in the state's data broker registry.

“You’re not able to know: ‘OK, is that consumer real?’ ”said Jason Bier, chief privacy officer at Adstra LLC, a marketing solutions provider. And even if they are, Bier said, it’s not always clear that the named consumer actually asked for a deletion request to be submitted.

The privacy vendors, in turn, say brokers have become more adversarial, routinely challenging consumers’ requests about their data, or ignoring them altogether even after agreeing to remove the info.

“The brokers can’t be trusted to audit themselves,” said Rachel Vrabec, founder and CEO of Kanary, a data privacy solutions provider. “We’ve seen that time and time again.”

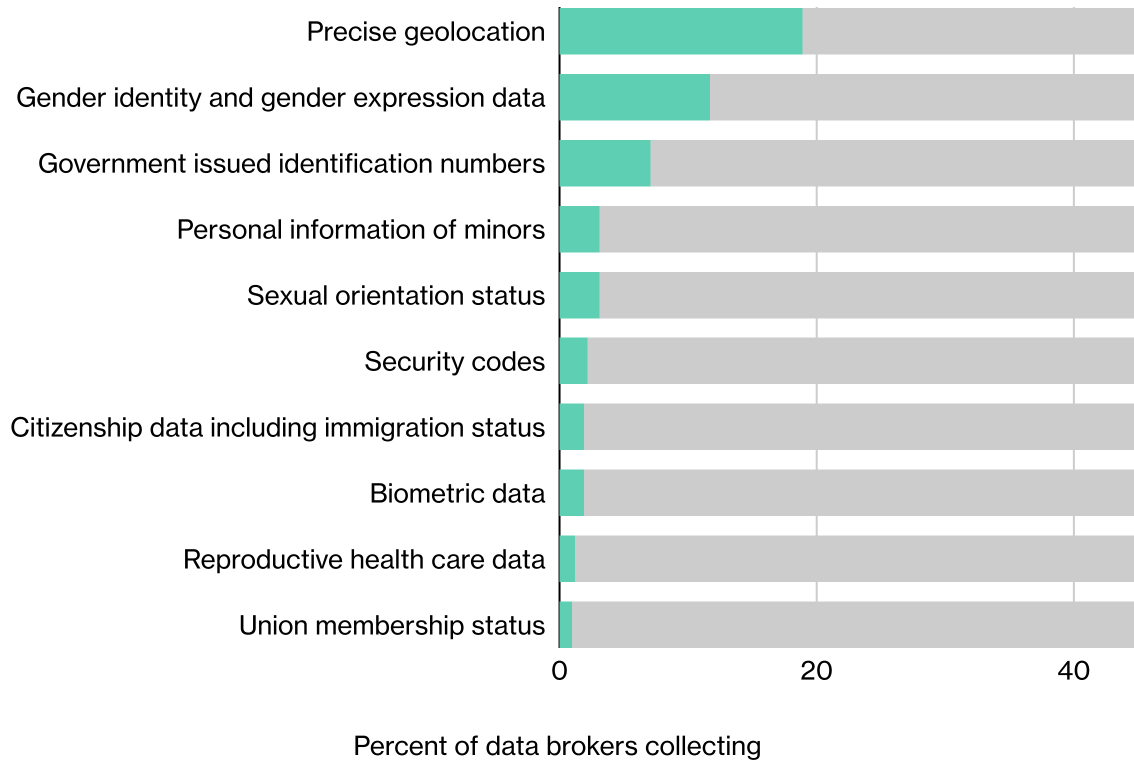
Expanding Regulation

California’s data deletion tool is a step beyond what other states such as Vermont, Texas, and Oregon — who also have launched registries — have done to tighten the leash on companies that many consumers don’t know are trafficking in their personal information.

The law and bolstered registry requires brokers to disclose if they collect sensitive information, such as kids’ data or precise geolocation, and whether some of their clients included law enforcement agencies or foreign actors, among others.

The public-facing data shows that some of the brokers that report denying consumers’ requests to get rid of their personal information are the same ones that collect sensitive details about them.

Sensitive Data Collected by Registered Data Brokers



Source: California Privacy Protection Agency

Bloomberg Law

Enformion LLC, which sells or shares data with federal and state governments and collects users' precise geolocation, didn't fully comply with any of the 80,000 data deletion requests it's gotten, according to information it furnished for the registry.

Zeta Global, which collects precise geolocation and users' sexual orientation, denied more than 110,000 out of the approximate 138,000 queries it received.

An Enformion spokesperson said in a statement the company processed all requests it could match to its records and that those denied were "overwhelmingly" requests with no matching record as opposed to requests they declined to honor.

Zeta Global declined to comment. VisitIQ and HealthWise Data didn't respond to requests for comment.

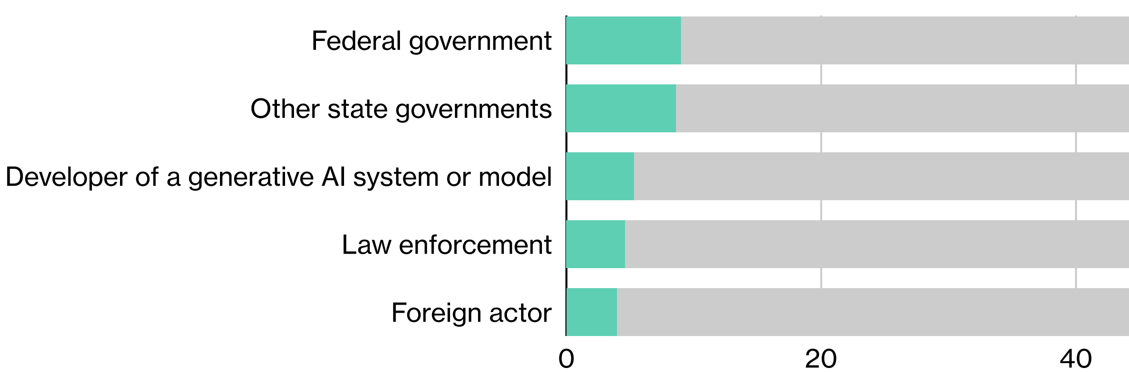
Even in instances where data removal is successful, consumers don't always get a guarantee their information will stay deleted.

Data broker Spokeo Inc. warns online users that it may not be able to honor their deletion requests over the long term because the same personal information might reappear in new records from public sources, according to the Electronic Privacy Information Center. Spokeo didn't respond to a request for comment.

High denial rates risk bringing heightened scrutiny to those brokers, even if they say they had legitimate grounds to challenge users' requests, according to one in-house professional at a registered data broker.

"I don't like it because I don't want to have CalPrivacy come audit us because they think that these numbers don't look right to them," said the professional, who requested anonymity because they were not authorized to publicly discuss the issue. Though, they added, "It's something we're expecting at some point."

Few Brokers Sell, Share Data with High-Risk Entities



Source: California Privacy Protection Agency

Bloomberg Law

John Doe, 'Yo Mama'

Some brokers attribute the high denial rates — or just the flood of requests they get in the first place — to the surge in data removal services that charge consumers up to a few hundred dollars a year to submit deletion requests. The industry was valued at $1.68 billion in 2024 and is expected to reach almost $8 billion by 2033, according to DataIntelo.

Data broker professionals assert that such services scrape the internet to find them then bombard them with deletion or opt-out requests without knowing if their firms actually hold information about their customers or if they are covered under an applicable privacy law.

David Stauss, whose law firm Stauss PLLC represents data brokers, described brokers fielding deletion requests filed on behalf of “Harry Styles” and “John Doe.” Others were signed with fictitious names like “yo mama.”

Privacy protection companies counter that brokers have intentionally made it more difficult for consumers to exercise their rights in the last few years.

“The data broker industry and the lawyers have colluded together to make it an even more of a pain in the ass to exercise either rights that you have or rights that you might have,” said Rob Shavell, co-founder and CEO of DeleteMe, a privacy protection company launched in the 2010s.

Vrabec, from Kanary, also pointed to a lack of resources and professionalism among some data brokers.

“A lot of these systems are built offshore, by ‘bros’ trying to make a buck,” she said. “Some of them, the big ones, are highly sophisticated data systems, but many of these databases are not.”

Under the Radar

Despite the focus on the issue and spread of data removal services, some well-known brands reported receiving few requests from consumers to get rid of their data.

General Motors received just 200 data deletion requests, according to its disclosure to California; Marriott International Inc. less than 350. And about 150 brokers said they didn't get a single consumer data deletion request in 2024.

These numbers are "really surprising to me," said Steve Lappenbusch, former head of privacy and compliance at People Data Labs, a registered data broker in California.

That trend will end as DROP kicks into full gear. All registrants in California will be on an even playing field: Requests sent to one broker will go to all of them.

The state's privacy agency said enforcement will fall to a strike force formed last fall. CalPrivacy has already brought about a dozen enforcement actions against brokers that have failed to register.

Other states will likely be watching California's model in the coming weeks. Connecticut in May became the first state to successfully emulate California's data deletion approach after consulting with CalPrivacy.

For privacy protection companies like DeleteMe, Kanary, and others, their work won't end come Aug. 1. Brokers on their list are still skirting California's registry, Shavell said. And even those registered continue to find ways around compliance, he said.

"God knows many people have really, really important reasons for not being exposed in these databases," he said. And brokers are still completely negligent in treating requests with a professional attitude, he said.

"Had they complied and had a constructive relationship with DeleteMe and others in our industry, maybe less strict laws that closed loopholes wouldn't be as necessary," Shavell said.

— *Graphics by Jon Meltzer/Bloomberg Law*

Fourth Circuit Emphasizes the Requirements and Implications of 'Comcast'

law.com/newyorklawjournal/2026/07/31/fourth-circuit-emphasizes-the-requirements-and-implications-of-comcast

The Fourth Circuit recently reversed class certification in an alleged securities fraud case against Boeing over aircraft safety statements, holding that Plaintiffs failed to satisfy the requirements of the Supreme Court's decision in *Comcast Corp. v. Behrend*.

In a thorough treatment of *Comcast* in a securities case, the panel distilled the burdens plaintiffs must satisfy. It held that plaintiffs must (i) identify a specific damages methodology, (ii) consistent with their liability theory, (iii) for calculating the type of damages they plead (such as specific alleged artificial inflation of the stock price due to particular statements) and isolating (or "disaggregating") an alleged corrective disclosure's impact, and (iv) concretely demonstrate how this can be measured on a class-wide basis.

Further, plaintiffs must put forth evidentiary proof that their damages methodology meets all of these requirements. Rooted in *Comcast* itself, *Boeing* sets forth reasoning that extends beyond the Fourth Circuit and the specific facts of the case.

Background

A January 2024 safety incident involving a Boeing 737 MAX allegedly caused the company's stock price to decline. Boeing investors soon sued Boeing and four executives in the Eastern District of Virginia for securities fraud under Sections 10(b) and 20(a) of the Securities Exchange Act.

The complaint alleged that, after two fatal 737 MAX crashes in 2018 and 2019, the Defendants repeatedly referenced Boeing's safety and manufacturing practices and its safety culture. Plaintiffs contended those statements were false or misleading because Boeing's manufacturing and quality-control practices allegedly remained unsafe, which plaintiffs claimed the January 2024 incident purportedly revealed.

Defendants moved to dismiss and plaintiffs opposed, arguing that the challenged statements were material and actionable in particularly safety-sensitive enterprises like the airline industry, or could become material if repeated over time. The district court denied the motion to dismiss and later granted plaintiffs' motion for class certification.

The Fourth Circuit's Reversal

In a unanimous decision, the Fourth Circuit held that plaintiffs must satisfy five requirements under *Comcast*:

1. Put forth an actual methodology and explain how it will measure damages and resolve predominance—i.e., that class-wide issues will predominate over individual ones—when applied to the specific case.

2. Show that the methodology can measure damages on a class-wide basis.

3. Identify a specific liability theory and show that the damages methodology is sufficiently consistent with that theory.

4. Support a just and reasonable, non-speculative inference of damages.

5. Supply evidentiary proof of all of the above, since Rule 23 is more than a mere pleading standard.

The Fourth Circuit held that plaintiffs failed each step, including because:

· Merely invoking the “out-of-pocket” method (the difference between inflation at purchase and at sale) only told the court what securities-fraud damages generally are, not how to determine any alleged artificial inflation in Boeing’s stock price on a given day. Along with generic references to two damages inputs (individualized transaction data and per-share inflation) and an unexplained event study, plaintiffs’ showing amounted only to “a series of maybes, perhapses and what ifs” that left the district court no way to rigorously evaluate their claim. This did not satisfy *Comcast*.

· Plaintiffs’ generic liability theory—that purported misstatements caused Boeing’s stock to trade at artificially high levels and resulted in a loss to shareholders when the price fell “after the truth emerged”—was plainly insufficient, as it described the theory in virtually all securities fraud cases. Further, plaintiffs’ contention that the challenged statements inflated the share price or maintained it at an artificially high level offered only alternative theories of liability. At the class certification stage, plaintiffs had to “tip their hand” as to their specific theory, because a court needs to be able to compare a plaintiff’s damages methodology to its liability theory.

· To the extent plaintiffs appeared to suggest they were adopting a constant-inflation measure, it was inconsistent with plaintiffs’ theory that 40 different misstatements concerning different topics over a three-year period, given different industry and macroeconomic conditions and evolving investor perceptions over time, could possibly have maintained the alleged fraud by an exact, constant percentage. The panel also refused to let a post-certification plaintiffs’ expert report cure these deficiencies, reasoning that Plaintiffs could “bob and weave” pre-certification until certification gives them “the leverage ... to use as a sword in litigation.”

The Fourth Circuit concluded certification was in error. The panel pointedly noted that “certification orders are not like participation trophies that are handed out to everyone on the tee ball team.”

Implications

Boeing re-emphasizes *Comcast’s* requirements in securities cases. It follows on other appellate courts that have reviewed *Comcast* certification issues under Rule 23(f).

The Fifth Circuit’s decision in Ludlow v. BP, PLC, for example, affirmed certification of a post-spill class whose conventional out-of-pocket model could be deployed on a class-wide basis, while rejecting a “pre-spill” class whose model rested on an inherently individualized inquiry. The Sixth Circuit’s recent *FirstEnergy* decision confirmed that *Comcast* applies regardless of single or multiple theories of liability and remanded for further consideration.

The Fourth Circuit’s decision in *Boeing* sets forth guidelines for the “rigorous analysis” Comcast demands and offers several important takeaways:

· Plaintiffs bear a significant burden to provide evidentiary proof at class certification and district courts must conduct a rigorous analysis. Boeing emphasizes that plaintiffs must advance evidentiary proof, and not just meet a pleading standard, at class certification, and that district courts must undertake a rigorous analysis of whether plaintiffs have met their burden. The Court of Appeals also noted that certification gives plaintiffs leverage to use as a sword in litigation and can “ratchet liability to potentially ruinous levels,” underscoring the practical stakes involved for defendants. This explicit recognition provides important context for class certification submissions and for seeking Rule 23(f) review where applicable.

· Plaintiffs must specifically explain how their methodology will measure damages in the specific case, not just broadly describe it. Simply referencing the out-of-pocket approach or noting that disaggregation is required or could be performed through an event study, without explaining their specific application and permitting a rigorous review, is not enough. Plaintiffs’ expert must concretely explain—not merely describe in generic terms—how to calculate the claimed damages, such as the artificial inflation allegedly caused by a specific challenged statement, and isolate a corrective disclosure’s price impact from confounding effects. Defendants will presumably target expert discovery on these points.

· Plaintiffs’ liability theory must likewise be specifically defined. Plaintiffs’ liability theory must be sufficiently specific to permit the court to test how well the proposed methodology matches it. A theory that investors were damaged by purchasing stock at inflated prices due to defendants' alleged fraud will not suffice. Nor may plaintiffs preserve uncommitted alternative theories. Defendants will presumably press plaintiffs to clarify and commit to a theory before certification briefing.

· Complexity of the pleaded fraud raises the bar for certification. The more sprawling and heterogeneous the pleaded fraud (more alleged misstatements, more subjects, longer class periods), the harder it will be to show a single damages methodology consistent with a single liability theory. Defendants facing a complex, multi-statement complaint, which is increasingly common in securities litigation, will likely focus on this in seeking to oppose class certification.

The Fourth Circuit is the latest court to address Comcast's application to securities class actions, but not the last. In May 2026, the Seventh Circuit granted Rule 23(f) review, on Comcast grounds, of a certification order in a separate securities action against Boeing, although the plaintiffs in that case have since sought to dismiss the interlocutory appeal following the district court's grant of a limited motion for reconsideration of its original class certification order.

More appellate courts may also weigh in on these issues, given the importance of class certification in securities cases.

Mealey's Litigation Procedure - 2nd Circuit Affirms Dismissal Of Securities Fraud Suit For Lack Of Scienter

In Brief

Second Circuit affirmed dismissal of securities fraud class action against Teladoc Health Inc. and executives, holding plaintiffs failed to adequately plead scienter regarding alleged misstatements.

Detailed Summary

The Second Circuit affirmed dismissal of a putative securities fraud class action against Teladoc Health Inc. and executives Jason Gorevic (CEO), Mala Murthy (CFO), Stephany Verstraete (Chief Marketing & Engagement Officer), and Richard Napolitano (Chief Accounting Officer). Lead plaintiff Leadersel Innotech ESG and additional plaintiff Hui Ma alleged defendants made false statements regarding integration of Livongo Health Inc. following an $18.5 billion merger and denied material competitive impacts, causing investor losses. The panel held plaintiffs failed to establish scienter under Section 10(b) of the Securities Exchange Act and SEC Rule 10b-5, finding no motive and opportunity beyond ordinary stock sales, inadequate allegations of conscious misbehavior or recklessness, and inapplicability of the core-operations doctrine. The court rejected arguments based on confidential witnesses, executive knowledge imputation, and corporate scienter. Section 20(a) control person claims also failed.
This summary is generated by AI technology. AI generated content should be reviewed for accuracy.

Body

A Second Circuit U.S. Court of Appeals panel affirmed the dismissal of investors' putative securities fraud class action against a virtual health care service provider and certain of its executives regarding alleged misstatements they made after the company's $ 18.5 billion merger with another health care company, finding that the investors had not adequately alleged scienter (In re Teladoc Health Inc. Securities Litigation, No. 25-1022, 2nd Cir., 2026 U.S. App. LEXIS 22196).

(Summary order available 57-260810-019R)

Judges Richard J. Sullivan, Joseph F. Bianco and Beth Robinson issued the summary order on July 27, finding that the investors did not prove motive or opportunity to benefit from the alleged misstatements and did not adequately plead that the executives consciously misbehaved or acted recklessly.

Judge Denise Cote of the U.S. District Court for the Southern District of New York dismissed the case against Teladoc Health Inc. and its executives (collectively, Teladoc) on March 21, 2025, finding that the investors who brought the suit had not adequately pleaded scienter. Judge Cote previously dismissed the case for failure to plead falsity, but the Second Circuit reversed that decision in a prior appeal.

Claims

In a December 2022 second amended complaint, investors including lead plaintiff Leadersel Innotech ESG and additional plaintiff Hui Ma sued the company and CEO Jason Gorevic, Chief Financial Officer Mala Murthy, Chief Marketing & Engagement Officer Stephany Verstraete and Chief Accounting Officer Richard Napolitano, seeking to represent those who purchased Teladoc common stock from Feb. 11, 2021, through July 27, 2022, "and were damaged thereby."

The investors alleged that Teladoc had falsely assured investors that Teladoc was successfully integrating Livongo Health Inc. Additionally, the investors alleged that Teladoc had falsely assuaged investors' concerns about competition, denying that competition was materially affecting Teladoc's business. They alleged that after the truth about these issues was revealed, Teladoc's investors lost billions.

The investors asserted a claim against all defendants for violating Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. 78j(b), and the accompanying regulation Securities and Exchange Commission Rule 10b-5, 17 C.F.R. 240.10b-5, and a claim against the executives for violating Section 20(a) of the Exchange Act, 15 U.S.C. 78t(a).

Falsity

Teladoc successfully sought dismissal for failure to state a claim, with Judge Cote in July 2023 concluding that many of the integration statements were inactionable puffery and as to the remainder, that the investors did not "adequately plead that any of these representations was false or materially misleading."

Leadersel and Hui Ma appealed, focusing on certain integration statements and the denial of leave to amend. Partway through the briefing, the Second Circuit granted a joint motion to simplify the appeal caption, which the parties said had been inconsistent with the District Court's, "incorrect and potentially misleading."

In a Sept. 24, 2024, ruling, a Second Circuit panel reversed and remanded the case, finding that the complaint adequately pleaded falsity with respect to the challenged statements. The panel said that on four "alleged misstatements regarding the status of the integration itself," it disagreed with the District Court. One of those statements consisted of "the risk warnings in Teladoc's 2021 Form 10-K." Among other things, the panel ruled the allegations were "sufficient to plausibly support a finding that, by the time of the filing of the 2021 Form 10-K in February 2022, the risks regarding the Livongo integration were not merely 'potential difficulties that Teladoc may encounter in the integration process'. . . but had already materialized and resulted in significant disruption to Teladoc's business," citing Set Cap. LLC v. Credit Suisse Grp. AG, 996 F.3d 64, 85 (2d Cir. 2021).

Finally, the panel declined to consider Teladoc's alternative argument that dismissal was warranted for failure "to adequately plead scienter and loss causation," stating that "the district court did not consider those arguments, and we decline to do so here in the first instance." It remanded the case to the lower court to address whether the investors adequately pleaded scienter and loss causation.

Renewed Motion

Back in the District Court, Teladoc filed a renewed motion to dismiss the case, arguing that scienter and loss causation had not been adequately pleaded. The motion addressed the four remaining statements at issue - two statements by Gorevic in early 2021 that the sales teams had been fully integrated; Verstraete's statement in late 2021 that the marketing data and tech stacks had been integrated; and the risk disclosures in Teladoc's 2021 Form 10-K.

On March 21, 2025, Judge Cote granted the motion, finding that the second amended complaint "does not provide strong circumstantial evidence of conscious misbehavior or recklessness with respect to any of the four statements that remain at issue in this case."

Among other things, the judge found that three integration problems covered by the Form 10-K's risk disclosure had materialized by the end of February 2022 and addressed the allegations of scienter for each. Judge Cote said the second amended complaint did not adequately allege that Gorevic knew enough about the sales integration problem with respect to the risk warning to adequately plead scienter. The judge further noted that the second amended complaint failed to plead Verstraete's scienter regarding the statement about the delay in Tableau integration. The lead plaintiff also failed to offer meaningful allegations that Gorevic, Murthy or Napolitano was aware of the salesforce integration issue.

Judge Cote denied the lead plaintiff's request to amend, noting that it had not identified how an amendment would address the second amended complaint's deficiencies and that the lead plaintiff was warned that it would likely not have another opportunity to amend the complaint.

Leadersel and Hui Ma appealed the decision to the Second Circuit.

Scienter

The panel affirmed, finding first that the investors provided no path to motive and opportunity other than the executives' stock sales. It found that "Plaintiffs' contention that Defendants sold stock to profit from their misstatements is far less compelling than the 'opposing inference' that these executives were simply selling their stock in the ordinary course."

It also found that the investors did not adequately plead that the individual defendants acted with conscious misbehavior or recklessness. First, it held that the investors failed to plead any facts suggesting that Gorevic knew that his misstatements about the Legacy Teladoc and Livongo sales teams being fully integrated and vague warnings that Teladoc may encounter integration issues were inaccurate because they were based on confidential witnesses who provided no relevant information.

The panel disagreed with the investors' argument that Murthy and Napolitano consciously misbehaved or were reckless because Murthy discussed increased competition at certain all-hands meetings between fall 2020 and spring 2022. It stated that the investors had not explained why the mention of competition implicitly revealed an understanding of Teladoc's integration issues rather than "any of the other reasons why a large business may struggle with its competitors." Nor did the investors explain how Murthy's knowledge should be imputed on Napolitano. Additionally, it found that "Verstraete's purported misstatement does not carry the same inference of knowledge as an officer's use of specific financial data."

The panel also found that the investors failed to plead scienter under the core-operations doctrine. It stated, "Though Teladoc's acquisition of Livongo for a record-breaking $ 18.5 billion was plainly important to the core operations of Teladoc, Plaintiffs have not plausibly pleaded that the details of the sales-team staffing arrangements and technical integration of marketing databases are sufficiently 'core' to the acquisition and Teladoc's operations to support a 'core operations' argument."

The panel disagreed with the investors' argument that the District Court erred in rejecting their allegations that Teladoc possessed corporate scienter because the individual defendants and other nondefendant executives possessed scienter. It found that the allegations against the nondefendant executives did not provide evidence of their knowledge of any falsity and did not connect them to the alleged misstatements.

Because the panel found the investors failed to establish that Teladoc violated Rule 10b-5, it found that their Section 20(a) claims against the individuals also failed.

Leadersel Innotech is represented by Carol C. Villegas, Irina Vasilchenko and Matthew J. Grier of Labaton Keller Sucharow LLP in New York.

Teladoc, et al. are represented by Abigail Frisch Vice in Washington, D.C., and Daniel J. Kramer, Audra J. Soloway and Dylan O. Smith in New York, all of Paul, Weiss, Rifkind, Wharton & Garrison LLP.

Privacy & Cybersecurity

Reddit Advances AI Scraping Suit Against Perplexity, SerpApi (1)

July 31, 2026, 8:16 AM PDT; Updated: July 31, 2026, 9:44 AM PDT

Summary by Bloomberg AI **AI Generated**

- Perplexity AI Inc. and SerpApi LLC must face most of Reddit Inc.'s copyright suit, despite claims that Reddit lacks standing to sue over users' work.

- The US District Court for the Southern District of New York said Reddit's allegation of copyright infringement, including its own protected arrangement of the work, constituted harm sufficient to allow it to sue.

- The court ruled that Reddit's claims that Perplexity and SerpApi circumvented protections and took user content in bulk fell within the area the Digital Millennium Copyright Act was enacted to protect.

Perplexity AI Inc. and SerpApi LLC must face most of Reddit Inc.'s copyright suit despite the web-scraping AI companies' claims that the social media platform lacks standing to sue over users' work.

Reddit's allegation of copyright infringement — including its own protected arrangement of the work — constituted harm sufficient to allow it to sue Perplexity and SerpApi even if the company hasn't alleged economic harm, the US District Court for the Southern District of New York said Friday.

Reddit also claimed reputational harm through circumvention of its technical measures designed to protect its site from scraping and to protect user privacy, Judge Paul A. Engelmayer added.

The 63-page decision pushes forward a lawsuit in the critical landscape of what AI and other data-scraping companies can and can't do. The ruling granting Reddit standing to sue overcomes a major hurdle as legal professionals — and Engelmayer — had expressed uncertainty over the platform's ability to sue over over works it didn't itself create.

But ultimately Engelmeyer determined Reddit's claims that Perplexity and SerpApi circumvented protections and took user content in bulk fell within the area the Digital Millennium Copyright Act was enacted to protect. He noted the DMCA's broad language that "any person injured... may bring a civil action... for such violation."

SearchGuard as TPM

Reddit's complaint said Perplexity used the scraping tools of three co-defendants — including SerpAPI — to circumvent Reddit's security measures and gain access to valuable copyrighted content created by the social media site and its users. The claims focus in large part on the defendants' evasion of Google SearchGuard, which blocks large-scale automated copying of search results, including content found on Reddit.

Perplexity and SerpApi argued that SearchGuard isn't a "technical protective measure" under the DMCA because human users can seamlessly access the protected content. They noted a federal circuit court has said the DCMA doesn't apply to mechanisms that control one form of access but leave another wide open.

But that was dicta that wasn't part of the ruling in that case, and "denying statutory coverage for a measure designed to prevent bulk electronic circumventions" doesn't flow from the DMCA's text, Engelmayer said. That argument "is in tension, if not outright antithetical, to the DMCA's purposes," he said.

Further, SearchGuard effectively blocked automated access and intentionally allowed human access, whereas the print cartridge at issue in the cited opinion simply had a fairly easy workaround.

The defendants also argued a TPM must be authorized by the copyright owner, and that neither Reddit nor its users authorized Google to use them. But Engelmayer said "that is wrong" because Reddit plausibly alleged that users authorized the platform to protect their interests by signing the user agreement, and Reddit itself has various licensing partnerships that recognize the protections of Google.

Engelmayer did toss Reddit's claims that SerpApi violated another subsection of the DMCA that requires not only that the TMP prevent access, but that it also prevents reproduction of the copyrighted works. Reddit only argued that SearchGuard prevented access, not that it controlled what was possible once access was achieved, he said.

The judge also dismissed some state law unjust enrichment and unfair competition claims as preempted by the Copyright Act, though it allowed civil conspiracy claims to advance.

Bartlit Beck LLP and Wollmuth Maher & Deutsch LLP represent Reddit. Weil, Gotshal & Manges LLP represents SerpApi. Keker, Van Nest & Peters LLP represents Perplexity.

The case is Reddit Inc. v. SerpApi LLC, S.D.N.Y., No. 1:25-cv-08736, 7/31/26.

Drugmakers, retailers must face 'maximum strength' claim in decongestant false ad litigation in US

reuters.com/legal/litigation/drugmakers-retailers-must-face-maximum-strength-claim-decongestant-false-ad-2026-07-30

NEW YORK, July 30 (Reuters) - A federal appeals court on Thursday revived portions of nationwide litigation in which consumers accused drugmakers such as Procter & Gamble (PG.N), opens new tab and retailers such as CVS (CVS.N), opens new tab of selling billions of dollars of over-the-counter decongestants that didn't work.

The litigation comprised about 100 lawsuits filed after a U.S. Food and Drug Administration advisory panel found in September 2023 that oral phenylephrine, an ingredient in such products as Vicks NyQuil Severe Cold & Flu and Advil Sinus Congestion & Pain, was no better than a placebo.

A three-judge panel of the 2nd U.S. Circuit Court of Appeals in Manhattan said the Federal Food, Drug and Cosmetic Act preempted most of the consumers' state law-based claims, saying the defendants followed FDA labeling requirements.

But the court revived claims over decongestants labeled "maximum strength," because various defendants added that phrase on their own. It also revived claims over brand-name drugs approved through the federal New Drug Application process, because the defendants could have updated labels to reflect the latest science.

"The limitations on consumer plaintiffs' state law remedies may appear unfair, particularly when the FDA's own agency review has confirmed that oral PE does not work as a decongestant and when studies have impugned oral PE's efficacy for 20 years," Circuit Judge Denny Chin wrote. "The fix, however, must flow not from litigation but from the FDA."

LITIGATION 'FAR FROM OVER'

Thursday's decision also said consumers lacked standing to pursue a civil racketeering claim accusing the defendants of defrauding the public and the FDA.

Jonathan Selbin, a lawyer for the consumers, said they were "obviously disappointed" with parts of the decision and reviewing their next steps.

"For over a decade these manufacturers made billions of dollars selling products with a decongestant that they long knew — in many cases based on their own studies — was entirely ineffective at decongesting," he said. "This case is far from over."

Procter & Gamble makes Vicks NyQuil Severe Cold & Flu, while Haleon (HLN.L), opens new tab makes Advil Sinus Congestion & Pain. Some of the other defendants included Bayer (BAYGn.DE), opens new tab, GSK (GSK.L), opens new tab, Kenvue (KVUE.N), opens new tab, Costco (COST.O), opens new tab, Target (TGT.N), opens new tab, Walgreens and Walmart (WMT.O), opens new tab, as well as CVS.

Lawyers for those companies did not immediately respond to requests for comment.

The appeals court returned the litigation to U.S. District Judge Brian Cogan in Brooklyn, who dismissed it in October 2024.

In November 2024, the FDA proposed removing oral phenylephrine as an ingredient in over-the-counter oral cold medications.

Securities

SEC Pauses Nasdaq’s Bid to Delist Small Companies After Protest

July 30, 2026, 2:19 PM PDT

The Securities and Exchange Commission reversed course and halted a new rule that would let Nasdaq Inc. quickly boot struggling companies from its stock exchange after small firms voiced procedural concerns.

The regulator informed Nasdaq in a letter Wednesday that it was staying the exchange operator’s rule until further notice. The SEC earlier this month had approved the plan allowing the exchange to kick out companies if their market worth, based on the value of their listed securities, dipped below $5 million for 30 straight days.

The SEC and Nasdaq declined to comment.

The measure is an attempt to clean up trading in so-called penny stocks, or companies that typically trade below $5 a share. The smallest companies on Nasdaq have been plagued by wild swings in their share prices amid allegations of social media-fueled trading manipulation.

Read More: Wall Street’s Stamp of Legitimacy Fuels Suspected Pump-and-Dumps

The rule, proposed by the exchange operator in January, drew support from Wall Street firms that have warned about potential pump-and-dump trading schemes, especially among tiny companies listed in the US but based in Asia.

Some small companies have pushed back though, arguing the attempts to stop scams would also punish law-abiding startups.

A group representing small businesses petitioned the SEC to pause the rule, as did Cemtrex Inc., a New York-based tech company, which said it would face de-listing if the measure goes into effect. The company and the small business group’s requests were able to stay the rule because the measure was not cleared by a formal commission vote.

A Lesson in Jury Instruction Hygiene: The Ninth Circuit Undoes a Trade Secrets Verdict Over a Flipped Burden of Proof | Business Information & News | FE

The federal Defend Trade Secrets Act (DTSA) and its state-law counterparts cover much of the same ground, but they are not identical. One potential difference was discussed in our recent client alert: under the DTSA, a plaintiff must prove its trade secrets were not readily ascertainable through proper means, while California's model civil instructions treat ready ascertainability as an affirmative defense the defendant must prove.

That distinction became dispositive in Comet Technologies USA, Inc. v. XP Power, LLC, Nos. 23-15601, 23-15709 & 25-745 (9th Cir. July 14, 2026), after Comet dismissed its California claims mid-trial but the district court retained a jury instruction placing the burden on the defendant, XP. A divided Ninth Circuit panel held that the error required vacating the $40 million judgment and remanding for a new trial.

Background

Comet alleged that three engineers left for XP Power with thousands of confidential documents detailing Comet's products, R&D strategy, and underlying technologies. Using that information, XP was allegedly able to create designs and a development plan for its new product lines in just nine days. Comet sued under the DTSA and California's Uniform Trade Secrets Act but then, mid-trial, voluntarily dismissed the state law claims. The jury returned a $40 million verdict—$20 million in compensatory damages and $20 million in punitive damages—and the district court later entered a permanent injunction and awarded over $17 million in attorneys' fees.

The Instructional Error

The appeal turned on a single jury instruction: Instruction 20. Originally proposed by XP when both federal and state claims were pending, Instruction 20 told the jury that XP bore the burden of proving that Comet's alleged trade secrets were "readily ascertainable by proper means." Once Comet dropped the state claims, XP asked the court to revise the instruction to reflect the DTSA's plaintiff-side burden. The district court declined, and the instruction went to the jury unchanged.

Comet raised two arguments to save the verdict. First, it argued that XP invited the error by later supporting Instruction 20 at the final charging conference. The panel disagreed: XP had already lodged a timely, specific objection that the court ruled on definitively, and its later position reflected a choice between an imperfect instruction and no instruction on ready ascertainability at all. Arguing in the alternative did not waive the preserved objection.

Second, Comet argued the error was harmless. It contended that a separate "independent economic value" instruction effectively covered ready ascertainability, and that its evidence of non-ascertainability was overwhelming anyway. The majority rejected both points. The two elements are related but distinct: information can be valuable without being secret, and secret without being valuable. And the jury heard sharply conflicting expert testimony on whether the trade secrets could have been reverse-engineered or found in public sources.

The Dissent

Judge Bumatay agreed that the instruction was erroneous but dissented on harmlessness. In his view, Comet's technical files, calibration data, schematics, and test results amounted to overwhelming—and largely unrebutted—evidence that the information was not readily ascertainable. He also noted that the jury found the trade secrets derived "independent economic value because [they were] secret"—a finding he viewed as closely tied to the ready-ascertainability inquiry. And he viewed the jury's $20 million compensatory-damages award as further confirmation: because the jury awarded damages based on the value of the benefit XP obtained through misappropriation, the verdict suggested the jury believed XP could not have obtained the information through proper means.

The Concurrence

The majority did not reach XP's remedies challenges. But Judge Hamilton, sitting by designation, wrote separately to address a remedies question likely to recur on remand: whether awarding unjust-enrichment damages for avoided costs and a permanent injunction is an impermissible double recovery. He would say no. Avoided-cost damages strip the defendant of a past benefit, while an injunction prevents future harm. Requiring a plaintiff to choose between them, he warned, could let a misappropriator pay avoided costs and effectively purchase a license to keep using the stolen information.

Key Takeaways

Comet offers three practical lessons. First, whenever claims change during trial, immediately re-audit the instructions and verdict form. Second, preserve objections expressly and on the record; a fallback argument after an adverse ruling may not amount to invited error, so long as the initial objection was clear and timely. Third, Judge Hamilton's concurrence gives trade secret plaintiffs a useful argument for combining avoided-cost damages with injunctive relief.

Chancery Addresses Stockholder Inspection Rights and Personal Jurisdiction | Business Information & News | FE

Orchid Global Inc. v. Salamon, C.A. No. 2025-0605-LWW (Del. Ch. April 10, 2026)

California statutory law provides certain inspection rights to stockholders of corporations with their principal place of business in California. Prior Delaware authority, JUUL Labs, Inc. v. Grove, 238 A.3d 904 (Del. Ch. 2020), addressed these statutory rights and held that Delaware law governs stockholder inspection rights for a Delaware corporation under the internal affairs doctrine. Here, a corporation sued one of its stockholders in Delaware who was seeking an inspection under California law in the California courts. The Court of Chancery, however, dismissed the case, finding that it lacked personal jurisdiction over the stockholder, a California resident whose only Delaware connection was stock ownership. The corporation's forum-selection bylaw did not provide a basis for finding the stockholder consented to jurisdiction, as its express terms did not cover corporation-initiated suits against its stockholders.

Data breach roundup: Lawsuits strike healthcare, fintech sectors | Secondary Sources | National

Healthcare

Healthcare technology provider **Craneware Inc.** faces a proposed class action filed July 27 in the U.S. District Court for the Southern District of Florida. The complaint alleges the company failed to protect personally identifiable information and protected health information from a cyberattack. Mariya Weekes of Milberg PLLC represents the plaintiff. *Crawford v. Craneware Inc.,* No. 26-cv-62061, *complaint filed* (S.D. Fla. July 27, 2026).

Unlimited Technology Systems LLC, a Cincinnati-based healthcare technology company, faces a proposed class action filed July 23 in the U.S. District Court for the Southern District of Ohio. The suit alleges the company failed to protect PII and PHI from unauthorized access that occurred between Oct. 5 and 10, 2025. The compromised data included names, health insurance and patient balance information, medical information, driver's licenses, and Social Security numbers, the complaint says. Terence R. Coates of Markovits, Stock & DeMarco LLC, Gary M. Klinger of Milberg PLLC and Leanna A. Loginov of Shamis & Gentile PA represent the plaintiff. *Ishmael v. Unlimited Technology Systems LLC*, No. 26-cv-721, *complaint filed* (S.D. Ohio July 23, 2026).

Education

Glendale Community College District, a California public community college, faces a proposed class action filed July 27 in the U.S. District Court for the Central District of California. The complaint alleges the college failed to protect students' PII from a cyberattack conducted by the ShinyHunters cybercriminal group between May 27 and June 9. The group stole more than 62 gigabytes of data, the suit says. The compromised PII included Social Security numbers, academic records, government-issued IDs, immunization compliance logs, and personal information such as names, genders, birthdates, email addresses, physical addresses and phone numbers, according to the complaint. Rachele R. Byrd and Stephanie Aviles of Wolf Haldenstein Adler Freeman & Herz LLP and James F. Woods, Annie E. Causey and Olivia E. Pizzo of Woods Lonergan PLLC represent the plaintiff. *Davis v. Glendale Community College District,* No. 26-cv-8278, *complaint filed* (C.D. Cal. July 27, 2026).

Financial technology

YouLend US LLC, a fintech company that provides businesses with financing services, faces a proposed class action filed July 24 in the U.S. District Court for the Northern District of Georgia. The complaint alleges the company failed to protect customers' PII from unauthorized access that occurred between June 5 and 9. The compromised data included names, addresses, Social Security numbers and financial information, the suit says. Casondra Turner of [Milberg PLLC] and William B. Federman of [Federman & Sherwood] represent the plaintiff. *Kirakosyan v. YouLend US LLC*, No. 26-cv-4174, *complaint filed* (N.D. Ga. July 24, 2026).

Benefits technology

Bridgeway Benefit Technologies LLC, a Baltimore-based company that provides software that unions use to manage health, pension, eligibility, claims and contribution information, faces a proposed class action filed July 28 in the U.S. District Court for the District of Maryland. The complaint alleges the company failed to protect union members' PII from unauthorized access that occurred between March 5 and May 19. The compromised data included names and Social Security numbers, the suit says. Leanna A. Loginov of [Shamis & Gentile PA] and Brittany Resch of [Strauss Borrelli PLLC] represent the plaintiff. *Williams v. Bridgeway Benefit Technologies LLC*, No. 26-cv-2938, *complaint filed* (D. Md. July 28, 2026).

Manufacturing

Bunn Commercial LP, a Springfield, Illinois-based global manufacturer of dispensed beverage equipment, faces a proposed class action filed July 27 in the U.S. District Court for the Central District of Illinois. The complaint alleges the company failed to protect employees PII from a data breach discovered Nov. 29, 2025. The compromised data included names, Social Security numbers and health insurance information, the suit says. Laura Van Note of [Cole & Van Note] represents the plaintiff. *Beaman v. Bunn Commercial LP*, No. 26-cv-3240, *complaint filed* (C.D. Ill. July 27, 2026).

Home improvement

Bath Fitter Franchising Inc., a Springfield, Tennessee, company that manufactures and installs custom acrylic bathtub and shower liners, faces a proposed class action filed July 23 in the U.S. District Court for the Middle District of Tennessee. The complaint alleges an unauthorized third party gained access to the company's computer systems, compromising employees' PII and PHI including Social Security numbers, birthdates, financial account numbers, health and safety information, passport information, and driver's license information. J. Gerard Stranch IV, Grayson Wells and Miles McDowell of Stranch, Jennings & Garvey PLLC and Samuel J. Strauss and Raina C. Borrelli of Strauss Borrelli PLLC represent the plaintiff. *Bobeck v. Bath Fitter Franchising Inc.*, No. 26-cv-1048, *complaint filed* (M.D. Tenn. July 23, 2026).

Transportation fleet safety

SafetyFirst Systems LLC, a Parsippany, New Jersey-based driver and fleet safety company, faces a proposed class action filed July 28 in the U.S. District Court for the District of New Jersey. The complaint alleges the company failed to protect PII from a Sept. 15, 2025, cyberattack in which an unauthorized actor accessed and exfiltrated data from the company's IT network. The compromised data included names, Social Security numbers and driver's license numbers, the suit says. James E. Cecchi and Jason H. Alperstein of Carella Byrne Cecchi Brody & Agnello PC, Jeff Ostrow of Kopelowitz Ostrow PA, and Mariya Weekes of Milberg PLLC represent the plaintiff. *Page v. SafetyFirst Systems LLC*, No. 26-cv-9510, *complaint filed* (D.N.J. July 28, 2026).
By Westlaw Today

Fourth Circuit Reverses Class Certification in Boeing Securities Fraud Case | Business Information & News | FE

The Situation: In State of Rhode Island Office of the General Treasurer v. The Boeing Company, No. 25-1492 (4th Cir. July 20, 2026), the Fourth Circuit opined on the level of proof that securities class-action plaintiffs, at the time of class certification, need to provide concerning their damages methodology in order to meet the standard articulated in Comcast Corp. v. Behrend, 569 U.S. 27 (2013).

The Result: The Fourth Circuit held that the plaintiffs' proof was insufficient because their damages expert offered only a "menu of options" rather than a specific methodology shown to be consistent with the plaintiffs' liability theory.

Looking Ahead: This decision establishes the Fourth Circuit as having a rigorous standard for evaluating damages methodologies at the class-certification stage in securities fraud cases. Both within and outside the Fourth Circuit, the Boeing decision will be an important tool for defendants seeking to defeat class certification in securities class actions.

Background

The case arises from statements that Boeing and its executives made about the company's safety practices following two crashes of 737 MAX aircraft and a worldwide grounding of the 737 MAX fleet. The plaintiffs alleged that a series of 75 statements made across five years falsely reassured investors about changes to Boeing's manufacturing and safety practices that were, in fact, not being implemented. Furthermore, the plaintiffs alleged that the truth began to emerge when another 737 MAX experienced a severe in-flight issue in January 2024, after which Boeing's stock price dropped by 8%.

The bulk of the plaintiffs' complaint survived a motion to dismiss, after which the parties proceeded to class certification. In support of their effort to show that damages could be determined on a class-wide basis, the plaintiffs' expert opined that a non-exhaustive "menu of options" would allow him to calculate damages on a class-wide basis later in the case. Those options included a number of different approaches to damage calculations, such as constant-dollar inflation, constant-percentage inflation, and an undefined variable approach. The expert did not specify which methodology he would use, nor did he or the plaintiffs describe how any damages methodology was consistent with their theory of liability. Nonetheless, the district court granted the plaintiffs' motion for class certification. Boeing petitioned for review under Rule 23(f), and the Fourth Circuit decided to hear the case.

The Fourth Circuit Announces a Five-Part Test for Class Certification

The Fourth Circuit articulated five requirements that plaintiffs must satisfy under Comcast to obtain class certification:

First, plaintiffs must put forth an actual damages "methodology"—not merely a generic legal description of what damages are. As the court emphasized, "[m]ethodologies require more than a legal description of what damages are generically—they must explain how damages will be measured in a specific case." If the model does not even attempt to explain how damages will be measured, "it cannot possibly establish that damages are susceptible of measurement across the entire class."

Second, the methodology must demonstrate that damages are measurable on a class-wide basis, though it may incorporate some individualized inputs such as purchase and sale data.

Third, the damages methodology must be consistent with plaintiffs' theory of liability. This requires plaintiffs to clearly identify both comparators—the theory of liability, stated with enough factual specificity, and the methodology—and then demonstrate that they are sufficiently consistent with each other.

Fourth, the methodology must permit "a just and reasonable inference" of damages and cannot be "speculative." Calculations need not be exact, but arbitrary measurements, applied merely because they happen to be class-wide, would reduce Rule 23(b)(3)'s predominance requirement "to a nullity."

Fifth, plaintiffs must support all of the above with "evidentiary proof." Rule 23 "does not set forth a mere pleading standard," and this evidentiary burden applies even where certification issues overlap with the merits.

Applying those five elements, the Fourth Circuit concluded that the plaintiffs failed to meet them across the board. The plaintiffs' expert did not select a specific methodology to use and only said that damages could be measured by determining the inflation in stock price caused by the misstatement, which simply recited the legal test for damages in securities cases. Nor did the plaintiffs tie a damages methodology to a theory of liability. The court observed that this failure was particularly acute given that the plaintiffs based their case on dozens of alleged misstatements over a multi-year period, making it difficult to identify the impact of any specific misstatement at any given point in time on Boeing's stock price. The court thus reversed the grant of class certification and remanded to the district court for further proceedings.

Guidance for District Courts Going Forward

The Fourth Circuit provided additional guidance to district courts on conducting Comcast analysis at the certification stage:

Rigorous analysis is mandatory. District courts must conduct a "rigorous analysis," taking a "close look" at whether plaintiffs' damages methodology satisfies the five requirements, even where that analysis overlaps with the merits.

Both comparators must be specifically identified. A court must have both the damages methodology and the liability theory properly and specifically identified so that it can perform the required consistency comparison.

Post-certification reports cannot cure certification-stage failures. The panel held that even if at the merits stage, post-certification, an expert opines on a specific damages calculation using a specific methodology, that would not cure the failure to present that analysis in the pre-certification stage, given Comcast's requirement for the court to perform a rigorous pre-certification analysis.

Three Key Takeaways

Comcast applies in securities class actions. Comcast was originally decided in the antitrust context. The Fourth Circuit unambiguously held that Comcast applies in Section 10(b) securities class actions, joining the Third, Fifth, and Sixth Circuits.

Plaintiffs' damages methodology faces heightened scrutiny at the class-certification stage. Plaintiffs cannot defer their approach to damages to the end of the case, but instead must present a specific, committed methodology at the time of certification. There is also a greater risk now for plaintiffs alleging a wide array of misstatements over an extended time period, as the breadth and diversity of the allegations will be treated as directly relevant to whether a single damages methodology can consistently apply across the class.

Potential for further judicial guidance. The Fourth Circuit framed its holding as consistent with other circuit courts and distinguished the Second Circuit's approach in Waggoner v. Barclays PLC, 875 F.3d 79 (2d Cir. 2017), on the facts. Defendants in securities class actions in any circuit should closely monitor these developments, as there may be additional judicial guidance in the future, including possibly from other circuit courts and the Supreme Court.

References

COMCAST CORPORATION; FOURTH CIRCUIT SEMINARS; BOEING CO; SECOND CIRCUIT COURT OF APPEAL

Amazon Shares Jump as Cloud Sales—and Spending—Accelerate

WSJ **wsj.com**/tech/ai/amazon-earnings-q2-2026-amzn-stock-3daf95f7

Amazon.com AMZN 15.58%increase; up pointing triangle cloud-computing sales are accelerating, and so are the company's investments in data centers to serve cloud customers. Investors are happy with that combination.

The company reported higher-than-expected revenue from Amazon Web Services on Thursday—continuing a streak of growth for its cloud-computing business—and raised its capital expenditures forecast for the year to $220 billion, a $20 billion increase.

Amazon shares gained more than 9% in after-hours trading, ticking upward after Chief Executive Andy Jassy disclosed the capex increase on a call with analysts and investors to discuss second-quarter results. He attributed part of the increase to the higher cost of memory chips for data centers.

"We've long believed AWS could become a few-hundred-billion-dollar-revenue business, and now believe it'll be at least double that—and very possibly be a trillion-dollar annual revenue business for us in time," Jassy said.

Sales by AWS, a major profit driver, grew 37% year-over-year to $42.2 billion for the quarter, its fastest growth rate in 18 quarters, the company said.

Amazon's revenue grew 20% to $200.6 billion, and net income was $62.6 billion. Both were ahead of analysts' estimates.

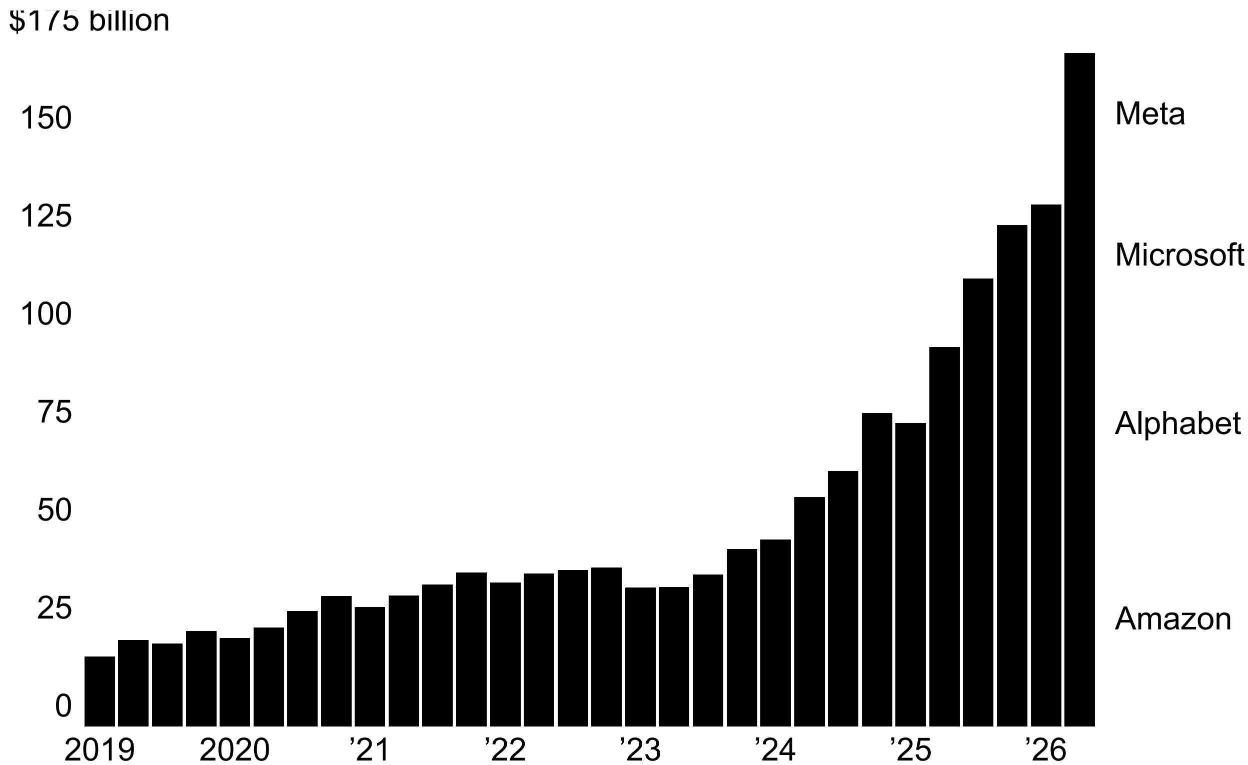
The company said that second-quarter net income included nonoperating pretax other income of $53.4 billion, primarily from its investments in Anthropic.

The revenue results were above the company's guidance of $194 billion to $199 billion.

The company reported negative free cash flow of $7.6 billion. It forecast revenue for the third-quarter of between $197 billion and $202 billion and operating profit between $22.5 billion and $26.5 billion.

Amazon said it spent $54.2 billion on purchases of equipment and property in the second quarter.

Capital expenditures, quarterly



Note: Data are for calendar quarters and include finance leases.

Investors recently have shown signs of skittishness about the steep spending on AI efforts by leading tech companies, particularly when it isn’t paired with obvious returns. Shares of Meta Platforms fell 9% Thursday following an earnings report in which it disclosed a narrowing of free cash flow to less than $1 billion and a higher floor on capital spending. Earlier this month, Google parent Alphabet GOOGL 6.81%increase; up pointing triangle boosted its estimated capital expenditures and descended into negative free cash flow, sparking a 7% selloff.

Amazon has been among the most aggressive hyperscalers on capital spending, and it also has the largest cloud business, through which it sells computing power to customers including OpenAI and Anthropic.

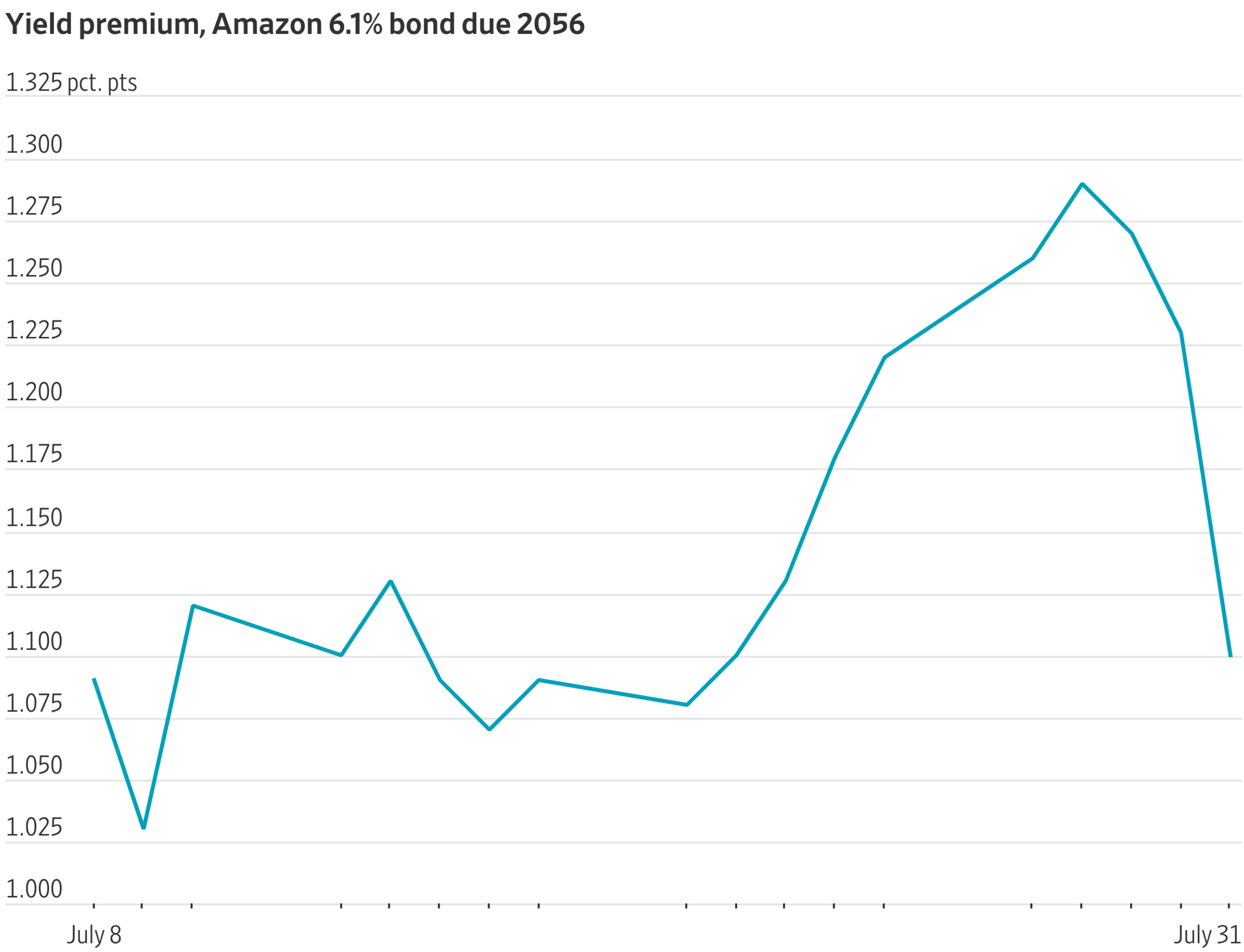
Amazon has been an Anthropic investor since 2023 and in April said it would invest as much as $25 billion in new capital into the fast-growing AI developer. As part of the agreement, Anthropic said it would purchase more than $100 billion of Amazon’s cloud services.

Amazon this week weighed in on a debate around whether and how to regulate open-weight AI models, including those developed in China. The company was among those to sign a letter advocating for access to open models, urging U.S. policymakers to exercise caution on potential restrictions.

“Successful leadership in AI will not be built around a single model or a single approach,” Amazon Web Services CEO Matt Garman said on X.

Hyperscaler Bonds Get Lift From Amazon Earnings

WSJ wsj.com/livecoverage/stock-market-today-dow-sp-500-nasdaq-07-31-2026/card/hyperscaler-bonds-get-lift-from-amazon-earnings-6gl8v2xo8YrMhmxUxFFM



Source: MarketAxess

Amazon.com’s strong earnings are providing a boost to battered AI hyperscaler bonds.

Amazon shares jumped 15% Friday after the company reported accelerating cloud-computing sales. The momentum carried over to its bonds: the extra yield, or spread, investors demand to hold its 6.1% bonds due in 2056 over Treasurys dropped to 1.1 percentage point from 1.23 percentage point Thursday, according to MarketAxess.

Bonds backed by other hyperscalers also rallied relative to Treasurys, including those issued by Meta Platforms, Alphabet and Oracle. Investors have been demanding higher yields to hold those bonds in recent weeks [amid increasing concerns] over how much the companies will borrow and spend to fund chip purchases and the construction of data centers.

Microsoft Posts Biggest One-Day Market-Cap Gain for Any U.S. Company

WSJ wsj.com/finance/stocks/microsoft-posts-biggest-one-day-market-cap-gain-for-any-u-s-company-b8713761

Tension between Silicon Valley's astronomical AI spending and Wall Street fears that it won't pay off had been sending markets on a wild ride. Then Microsoft MSFT 3.02%increase; up pointing triangle gained nearly half a trillion dollars in one day.

The company's stock surged 16% after its earnings quelled concerns that investments on data centers, chips and more would outpace the company's ability to generate cash. Microsoft's $450 billion one-day gain in market capitalization was the largest by any U.S. business, ever.

On the other hand was Meta META 3.28%increase; up pointing triangle Platforms. Shares dived 8% following projections that free cash flow would turn negative in the latter half of this year for the first time since the Instagram-parent went public in 2012. Meta stock's 11th consecutive decline notched its longest losing streak on record.

A day after Federal Reserve Chairman Kevin Warsh showed reluctance to raise interest rates, sparking a steep selloff in stocks and bonds, Microsoft's outlook won out. Major indexes rebounded, led by the Nasdaq composite's 2.8% gain. The S&P 500 climbed 1.7%, and the Dow Jones Industrial Average rose 1.2%, or 614 points, with Microsoft responsible for around 360 of them.

The divergent responses to Meta and Microsoft hinted at how Wall Street will answer a question at the heart of the AI trade: whether companies pouring hundreds of billions annually into the tech race can show investors the money. If not, Silicon Valley's onetime cash-printing machines will have to increasingly finance their expansion through debt—just as that debt is getting more expensive.

"I think there's a recognition that this trend can't go on forever," said Jack Ablin, founding partner at money manager Cresset. "They're going to need to start seeing revenue growth."

Though some investors interpreted Warsh's lack of guidance Wednesday as a signal to pare back risk, traders Thursday piled on more. Oracle, which is heavily reliant on debt to fund its capital expenditures, zoomed 8.3% higher. Amazon shares climbed 3.9% before it reported its quarterly results. That stock jumped in after-hours trading after the company beat analysts' expectations.

The hyperscalers' still-growing spending plans also helped fuel a turnaround in chip stocks that have been battered in recent weeks. Nvidia and Broadcom both advanced, while Micron, Sandisk, Western Digital and Intel each posted double-digit gains.

All three major indexes remain in the red in July, thanks in part to new supplies of big-tech stocks flooding markets and ripple effects from a downturn in the chip-heavy South Korean stock market. Retail traders dumped tech shares in recent days, analysts say, as did highflying AI-focused hedge fund Situational Awareness.

That pressure has at least momentarily flushed some AI concerns out of the market, said Trevor Slaven, Barings' global head of asset allocation and multiasset portfolio solutions. Add in a big growth in profits elsewhere in Corporate America, and he is tactically bullish on stocks.

"This is a one, two, three-month view," Slaven said. "It's going to be more volatile on the way up and the way down." Longer term, he added, "the competitive nature of [the AI build-out] almost necessarily means that you will overspend."

Excluding data-center deals, hyperscalers this year are on track to issue about $250 billion in debt for their capital expenditures, a figure estimated to grow to $400 billion in 2027, Goldman Sachs projected recently. The bank's analysts expect the companies will add another $1.3 trillion over the following three years.

Of that group of five companies—Amazon, Oracle, Alphabet, Meta and Microsoft—Microsoft relies on debt far less than its peers. The company's free-cash flow last quarter totaled $19.6 billion, whereas Meta generated less than $800 million.

Big swings in AI stocks have reversed before, and some traders saw Thursday's moves in the two companies' shares as an opportunity to swoop in.

Individual investors bought the dip in the Facebook parent, according to flow-tracking firm Vanda Research, snapping up $36 million of shares and making it the second-most popular stock of the session. On the other end of that list was Microsoft, which saw roughly $167 million in net retail outflows.

Still, with inflation elevated and longer-dated Treasury yields near their highest levels in years, tightening financial conditions are forcing investors to parse such companies' performances more closely.

"Investors have become too myopic about the words 'AI' and 'data center' and they're not stepping back and looking at what's going on," said Richard Bernstein, global head of macro investing at Janus Henderson. "As the free money is going away, investors are starting to look at fundamentals again. We're starting to take out the speculative fervor."

Why Courts Are Pushing Back On Greenwashing Laws

(July 31, 2026, 3:20 PM EDT)--

—

Two state legislatures sought to address greenwashing by drawing bright lines, specifying exactly what businesses could and could not say about the environmental attributes of their products, with penalties for noncompliance. In the first half of 2026, two federal courts concluded that this approach could not survive constitutional scrutiny.

In Retail Energy Advancement League v. Brown, the U.S. Court of Appeals for the Fourth Circuit on May 15 **ordered** a preliminary injunction against the core speech restriction of Maryland's S.B. 1, a 2024 law dictating which terms electricity suppliers could use to market renewable energy products.[1]

And on July 14, in California League of Food Producers v. Bonta, the U.S. District Court for the Southern District of California enjoined S.B. 343, the state's truth-in-labeling statute governing recyclability claims on products and packaging.[2]

Both courts applied the same constitutional framework — the intermediate scrutiny test derived from the U.S. Supreme Court's 1980 decision in Central Hudson Gas & Electric Corp. v. Public Service Commission. Both found the states fell short.

These rulings land at a moment when companies, regulators and consumers alike are struggling with the same fundamental question: What counts as greenwashing?

The decisions reveal a tension at the heart of environmental marketing regulation. States want clarity. Industry wants freedom to communicate. And courts are not prepared to let legislatures resolve that tension by flatly banning categories of truthful commercial speech.

That reluctance carries implications well beyond Maryland and California. It will shape how greenwashing litigation and enforcement unfold nationally, push future state efforts toward disclosure-based models rather than categorical bans, and leave the boundaries of permissible environmental marketing to be defined through case-by-case litigation rather than statutory bright lines.

Maryland's S.B. 1

Maryland enacted S.B. 1 in 2024 in response to concerns about consumer confusion in the renewable energy marketplace. After the state deregulated its electricity market, many residential customers selected green options, paying a premium under the impression they were buying electricity generated from wind or solar sources.

In reality, because all electricity is indistinguishable once it enters the regional power grid, these suppliers were purchasing renewable energy credits, or RECs, which are intangible instruments representing one megawatt-hour of renewable generation, rather than delivering physically traceable renewable power to anyone's home.

To address that concern, S.B. 1 prohibited covered suppliers from using terms such as "clean," "green," "eco-friendly," "carbon-free" or "100% renewable" unless their product was at least 51% backed by qualifying RECs.

Critically, Maryland's definition of a qualifying REC carried a geographic limitation: Credits had to originate within the PJM Interconnection, the regional grid operator spanning a noncontiguous territory of the eastern U.S. stretching from North Carolina through the mid-Atlantic states and into parts of the Midwest, including northern Illinois.

A supplier fully backed by RECs from a Texas wind farm could not market its product as "green" in Maryland, while a competitor using RECs from the Chicago area could, even though both sets of RECs represent the same underlying renewable generation attributes.

The statute also imposed mandatory disclosure requirements explaining how RECs function and what consumers were actually purchasing.

The Retail Energy Advancement League and Green Mountain Energy Co. challenged the law on First Amendment grounds, lost at the U.S. District Court for the District of Maryland in December 2024 and appealed. Seven states filed an amicus brief supporting the challengers, underscoring the national stakes in how far a state could go in restricting environmental marketing claims.

The Fourth Circuit's Analysis

On May 15, a unanimous Fourth Circuit panel reversed in part. Writing for the court, U.S. Circuit Judge Henry Floyd applied Central Hudson's four-part test without deciding whether strict scrutiny might also apply, because the law failed even under intermediate review.

The court rejected Maryland's argument that terms like "green" or "100% wind" are inherently misleading simply because no consumer's home is physically wired to a turbine. A supplier backed by wind-generated RECs could use those terms truthfully, the court reasoned, and the state had not shown that every possible use of the regulated language deceives consumers.

Turning to whether S.B. 1 adequately advanced Maryland's consumer protection interest, the court identified a critical mismatch in the geographic REC limitation.

The statute allowed a supplier to market electricity as "100% renewable" using RECs from northern Illinois while prohibiting an identical claim from a competitor whose RECs came from Texas. The court observed that a Baltimore consumer would be no less confused upon learning that their RECs came from greater Chicago than upon learning they came from West Texas.

The geographic distinction, in other words, did nothing to address the underlying confusion about what RECs are and how they work. The only thing actually resolving consumer confusion, the court noted, was the disclosure requirement — not the speech restriction.

Finding the speech restriction failed to materially advance the state's interest, the court ordered a preliminary injunction against that provision. The court treated S.B. 1's separate disclosure requirement differently.

Compelled disclosures are subject to a more lenient First Amendment test than outright speech restrictions: Under Zauderer v. Office of Disciplinary Counsel, a mandatory disclosure will be upheld so long as it is purely factual and uncontroversial, reasonably related to the state's interest in preventing consumer deception, and not unjustified or unduly burdensome. The Fourth Circuit did not decide whether Maryland's disclosure requirement meets that standard.

Because the Maryland Public Service Commission had issued materially revised disclosure language after the district court ruled, the Fourth Circuit remanded for the district court to evaluate the new version in the first instance. In doing so, however, the court flagged specific concerns for the district court to consider on remand, including whether language describing how REC purchases support regional renewable development reads more like policy advocacy than a purely factual statement, and whether the length of the mandated disclosure risks drowning out suppliers' own marketing messages.

California's S.B. 343: A Similar Outcome on Different Facts

On July 14, two months after the Fourth Circuit's decision, the Southern District of California reached a parallel conclusion regarding S.B. 343, California's truth-in-labeling law governing recyclability claims.

Enacted in 2021 and set to take effect on Oct. 4, S.B. 343 made it a criminal and civil offense to display recycling symbols — including the ubiquitous chasing arrows — or make any recyclability claim on products or packaging unless a set of rigid statewide criteria were satisfied, including a requirement that the product's material type be collected by recycling programs serving at least 60% of California's population and sorted by facilities serving at least 60% of programs statewide.

Penalties included fines up to $2,500 per violation and up to six months' imprisonment, and enforcement was available to private plaintiffs as well as the California attorney general.

A coalition of trade associations and industry groups sued to block the law before it took effect, arguing that it was unconstitutionally vague and violated the First Amendment.

As in the Maryland case, the court's July 14 ruling came on a motion for a preliminary injunction, meaning the plaintiffs needed only to show a likelihood of success on the merits, not a final adjudication of the law's constitutionality. The court granted that motion, enjoining California's attorney general from enforcing S.B. 343 while the litigation proceeds.

In reaching that result, the court found four separate provisions of S.B. 343 unconstitutionally vague, including requirements that materials "routinely become feedstock" — a term the statute never defined — and that packaging comply with the perpetually evolving Association of Plastic Recyclers design guide.

On First Amendment grounds, the court applied Central Hudson and concluded that California failed to demonstrate the law would materially advance its stated interests in improving recycling rates or reducing consumer confusion. The evidence instead indicated that manufacturers would simply strip recyclability messaging from their packaging entirely to avoid liability — leaving consumers with less information, not more.

The court also found the law more extensive than necessary. It prohibited even qualified, truthful recycling instructions and allowed no middle ground between full compliance and criminal exposure.

The Paradox of Bright-Line Greenwashing Rules

These cases reveal a fundamental paradox. Legislatures enact bright-line environmental marketing rules precisely because greenwashing is hard to define.

If a term like "green" or "recyclable" is inherently ambiguous, the legislative instinct is to standardize its meaning — to declare that only products meeting specific criteria may wear the label.

In theory, this protects consumers and gives industry a clear compliance target. In practice, these courts found the approach constitutionally infirm for the same reason it was legislatively attractive: The regulated terms are not inherently deceptive. They are potentially misleading in some contexts and perfectly accurate in others.

The First Amendment does not permit states to solve a nuanced problem with a categorical ban. And when a statute's rigid criteria fail to track the actual source of consumer confusion — as Maryland's geographic REC restriction demonstrably did — the court will find an inadequate fit between the speech restriction and the governmental interest.

What These Decisions Tell Us

The absence of bright-line rules does not eliminate greenwashing disputes; it redirects them.

By blocking these statutory regimes, courts have not resolved the underlying ambiguity of environmental marketing claims. They have simply returned the question to its previous state: one governed by generally applicable consumer protection statutes, the Federal Trade Commission's Green Guides, and the judgment of enforcement agencies and courts evaluating claims on a case-by-case basis.

Without a statutory definition of "green" or "recyclable" to serve as a safe harbor, every environmental marketing claim remains potentially actionable under unfair and deceptive acts and practices statutes, false advertising laws, and consumer class action theories.

The interpretive ambiguity that made these statutes attractive to legislators in the first place now reverts to the domain of litigation, where the boundaries of permissible environmental claims will be drawn one case at a time.

Rigid rules present their own trade-offs.

Both courts highlighted a recurring theme: Bright-line environmental marketing restrictions can suppress truthful speech.

California's scheme threatened to criminalize the chasing-arrows symbol on packaging that is, in fact, recyclable in most of the state. Maryland's regime barred a supplier from describing its product as "green" even when that product was fully backed by renewable energy credits, solely because those credits originated outside a defined geographic boundary that the Fourth Circuit described as "curious" and underinclusive.

Both laws pushed regulated parties toward silence rather than compliance, and both courts treated that chilling effect as evidence of constitutional deficiency.

Disclosure mandates remain on firmer constitutional ground, but only if properly tailored.

Neither court categorically rejected state authority to require transparency.

The Fourth Circuit explicitly left open the possibility that Maryland can compel factual disclosures about RECs, so long as those disclosures are accurate, neutral and not so extensive that they drown out the speaker's own message. California's general false advertising laws and the FTC Green Guides remain enforceable.

Future state efforts that rely on mandated disclosures rather than categorical speech bans may find a more receptive judicial audience.

However, the Fourth Circuit's guidance on remand suggests that even disclosure requirements will face scrutiny if they venture beyond purely factual content or become so lengthy that they overwhelm the speaker's own message.

Regulatory fragmentation is likely to persist.

These decisions will not discourage other states from experimenting with greenwashing legislation, and states with similar REC-based marketing rules or recyclability labeling requirements can expect courts to apply the same skepticism to rigid statutory definitions and categorical line-drawing.

The precise line between permissible disclosure mandates and impermissible speech restrictions will vary by circuit and subject matter, and the Maryland and California decisions, while instructive, are preliminary rulings whose underlying cases will continue to develop on remand.

Conclusion

What emerges from the first half of 2026 is a legal landscape where both regulators and regulated parties face heightened uncertainty. These decisions demonstrate that bright-line environmental marketing restrictions must be narrowly tailored to satisfy First Amendment scrutiny.

At the same time, the absence of such restrictions does not mean the absence of legal exposure under existing consumer protection and false advertising regimes.

As states continue to grapple with how to regulate environmental marketing claims, and as courts continue to test those efforts against constitutional limits, the greenwashing landscape is likely to remain unsettled for some time.

Calif. Wiretap Ruling May Reshape Pixel Tracking Litigation

The wave of website privacy litigation is forcing courts to answer a technical question: Can browser communications between a user, a website and its analytics providers constitute an illegal wiretap?

The answer is complicated by the fact that courts are increasingly being asked to apply legacy frameworks such as the federal Wiretap Act and the California Invasion of Privacy Act to browser architectures that did not exist when these regulations were drafted.[1] As a result, many pixel tracking complaints rely on descriptions that oversimplify or mischaracterize how browsers execute code, establish network connections and transmit information.

On July 10, the U.S. District Court for the Northern District of California**issued a ruling** in In re: Blue Shield of California Privacy Litigation that exposes this disconnect, providing a blueprint for how courts evaluate the mechanics of internet traffic.[2]

U.S. District Judge Yvonne Gonzalez Rogers shared that the plaintiff's "procurement-based theory of liability is not cognizable," and that "they have failed to state a claim against Blue Shield because they have not alleged sufficient facts to support a cognizable theory of liability under the Wiretap Act."

This decision may prove to be one of the most significant rulings to date in the growing wave of website privacy litigation. While the court allowed portions of the plaintiffs' privacy claims to proceed, it dismissed the federal Wiretap Act claim, drawing a significant line in the sand between deploying website analytics technology and unlawful interception of electronic communications.

This distinction matters because much of today's website privacy litigation depends upon characterizing ordinary internet communications as covert interceptions. As courts increasingly confront technical questions about browser architecture, the decision suggests that successful claims will require more than simply alleging that a website embedded a tracking pixel or analytics script.

What the Court Actually Held

The case arose from allegations that Blue Shield embedded Google and Meta technologies into portions of its member portal, allowing user interactions with health-related webpages to be transmitted to third-party vendors.[3] The plaintiffs asserted numerous privacy claims, including violations of the federal Wiretap Act.

The district court, however, distinguished between allegations that Blue Shield had deployed analytics technology and allegations that it had unlawfully intercepted communications during transmission. While the court permitted certain state law claims involving the disclosure of sensitive medical information to continue, it dismissed the federal wiretap theory.

That distinction may become increasingly important as privacy litigation continues to migrate from traditional data breach claims toward challenges involving ordinary website functionality.

Why the Procurement Theory Failed

One of the most significant aspects of the decision is the court's treatment of what the plaintiffs characterized as the procurement of interception technology.

The plaintiffs argued, in essence, that by purchasing, integrating or deploying third-party analytics tools, Blue Shield had procured an unlawful interception of electronic communications. The court rejected that theory, recognizing that installing software does not itself constitute an interception under the federal Wiretap Act.

To sustain a claim under the Wiretap Act, a complaint must satisfy the statutory definition of an "interception" under Title 18 of the U.S. Code, Section 2510, traditionally requiring a compelled, surreptitious interception by an uninvited third party splicing into a transmission line.[4]

That court conclusion reflects an important technological reality.

Modern websites routinely deliver JavaScript, images, style sheets and other executable resources to a visitor's browser. The mere presence of code on a server, or even the delivery of that code to a browser, does not establish that an unlawful interception has occurred. The question is instead about if communications were intercepted in ways that are problematic with the statutes.

The Next Battleground: From Procurement to Use

The dismissal of the procurement theory is unlikely to end pixel litigation. More likely, it will reshape it.

The focus for future cases is likely to shift from alleging that website operators merely purchased or installed tracking technologies, to arguing that defendants actively used those technologies to disclose users' communications, identity and information.

That shift places greater emphasis on the underlying mechanics of browser communications.

Future litigation will likely center less on whether a tracking script exists and more on precisely how information moved from the user's browser to the alleged third party.

Browser Architecture Matters

Understanding that distinction requires separating legal characterizations from how web applications actually operate.

When a user visits a website, the website's server responds by delivering content, including HTML, JavaScript and other resources, to the user's browser. The browser, operating on the user's own device, determines which instructions to execute and whether additional network requests should be initiated.

In other words, the browser — not the server — establishes outbound connections to retrieve additional resources unless prevented by browser settings, extensions, consent management platforms or other user controls.

This sequence is entirely different from the classic conception of a wiretap, in which an outside party secretly inserts itself into an existing communication channel and captures information during transmission.

Whether that distinction will ultimately affect any case will depend upon the specific implementation at issue. Nevertheless, the case suggests that courts are increasingly willing to examine these underlying technical mechanics rather than accepting generalized allegations about interception.

Service Providers Versus Third-Party Eavesdroppers

The decision also highlights another issue likely to receive greater attention in future litigation: the legal status of analytics vendors.

Wiretap statutes generally contemplate an unauthorized third party secretly intercepting communications between two other participants. Website operators, by contrast, typically characterize vendors such as Google and Meta as contractually authorized service providers operating pursuant to written data processing agreements and master services agreements.

Whether a particular vendor relationship satisfies that characterization will depend upon the governing contracts, the services performed and the specific facts alleged. Nevertheless, defendants are increasingly relying on these contractual relationships to argue that vendors function as authorized processors, rather than independent eavesdroppers.

Transparency may also become increasingly important. Privacy notices that identify analytics providers and explain their role in website operations do not necessarily resolve every statutory question, but they may undermine allegations that website operators secretly inserted unknown parties into users' communications.

Why Technical Evidence Will Become More Important

As litigation moves beyond generalized allegations regarding website pixels, forensic evidence is likely to assume a more prominent role.

Future cases may increasingly require courts to evaluate browser network logs, HTTP request sequences, JavaScript execution, consent management platforms and the precise timing of communications between browsers, websites and service providers.

The distinction is not merely semantic. It goes directly to whether the statutory concept of interception accurately describes what occurred.

Practical Lessons for Legal Teams

The decision provides several practical lessons for companies:

Defendants should carefully document vendor relationships, including data processing agreements that establish vendors as instruction-bound service providers.[5]

Organizations should ensure that privacy notices accurately disclose analytics technologies and identify third-party processors involved in website operations.

Counsel should work to preserve browser logs, network diagrams and architectural documentation explaining how communications actually occurred.

Litigators should recognize that browser architecture is no longer a peripheral technical issue. Increasingly, it is becoming central to the legal analysis itself.

Looking Ahead

The decision is unlikely to slow the pace of pixel tracking litigation. Instead, it may redirect it.

Plaintiffs will likely continue refining theories that characterize ordinary website operations as unlawful interceptions, while defendants will increasingly emphasize the mechanics of browser communications and the contractual relationships governing third-party service providers.

As those competing narratives evolve, courts will be asked to reconcile decades-old wiretap statutes with internet architectures that bear little resemblance to the communications systems those laws were originally designed to regulate.

The In re: Blue Shield of California Privacy Litigation suggests that courts are becoming more willing to undertake that technical analysis. For litigants on both sides, understanding how browsers actually transmit information may prove just as important as understanding the statutes themselves.

PE-Backed Jersey Mike's Makes Public Debut After $1B IPO

law360.com/articles/2507829

(July 30, 2026, 2:21 PM EDT)-- Private equity-backed sandwich chain Jersey Mike's hit the public markets Thursday after raising $1 billion in its initial public offering steered by Simpson Thacher & Bartlett LLP and Davis Polk & Wardwell LLP.

The Tinton Falls, New Jersey-based company sold roughly 43.5 million shares for $23 apiece, hitting the midpoint of its **marketed range** of between $21 and $25 each.

Jersey Mike's began trading on the New York Stock Exchange on Thursday under ticker symbol JMKE.

The company, backed by private equity giant Blackstone and the Abu Dhabi Investment Authority, commands a market value of $7.3 billion, according to IPO research firm Renaissance Capital.

Of the shares sold in the offering, Blackstone and the Abu Dhabi Investment Authority sold around 29.7 million shares, while Jersey Mike's sold around 13.8 million, according to a filing with the U.S. Securities and Exchange Commission. The private equity firms also granted the underwriters a 30-day option to buy up to an additional roughly 6.5 million shares, the filing said.

Jersey Mike's said it plans to use the proceeds from the shares it sold in the offering to repay certain debt and for general corporate purposes.

Founded in 1956, Jersey Mike's has grown to include 3,300 stores across all 50 states and two countries, with "nearly all" locations being franchised, according to the filing.

"We are Jersey Mike's: A high-growth franchisor of fast-casual, submarine-style sandwich restaurants specializing in authentic, hand-crafted, craveable subs," the company said in its SEC filing. "Built over 70 years on one uncompromising belief — that a truly great sub sandwich can change your day and that a truly great brand changes its community — Jersey Mike's is now one of the largest and fastest-growing limited-service restaurant brands based on U.S. systemwide sales and unit growth."

The offering is expected to close Friday.