The Role Of Operational Data In Tech Platform Liability Suits

By **Paul Hinton, Farooq Javed and James Sappenfield** (April 20, 2026)

Paul Hinton

Farooq Javed

James Sappenfield

In the U.S., litigation has become a de facto substitute for the regulation of major technology platforms.

State attorneys general and other government enforcement authorities are increasingly examining, evaluating and enforcing how large technology platforms design, operate and oversee their systems.[1]

At the same time, private plaintiffs have brought high-profile personal injury suits raising similar questions about the safety, moderation and product design of technology platforms.[2]

Jury awards in March against Meta Platforms Inc. and Google LLC, along with continued advocacy by victim and public interest groups, have renewed calls for legislative reform.[3][4]

For now, however, oversight continues to occur largely through civil proceedings. Plaintiffs are advancing claims under tort, product liability, public nuisance, privacy, consumer protection, labor, and public health law, and seek discovery of internal research, moderation records, transaction data and safety metrics.

In these cases, the inquiry focuses on how platform governance systems function, as reflected in underlying data. Whether a platform acted reasonably may turn on what its own operational data reveal about the design, implementation and performance of those systems across large user populations. Evaluating those questions requires a structured, data-intensive analysis of platform conduct at scale.

The Rise of Regulation by Litigation

Recent cases illustrate the scope of potential liability facing technology platforms under this model of regulation by litigation.

More than 40 state attorneys general and private plaintiffs have brought actions against ByteDance Ltd., Meta and Google, alleging that their platforms — including TikTok, Instagram, Facebook and YouTube — have exposed underage users to various mental health and safety harms.[5]

Jury awards further underscore this trend. On March 24, in a verdict in New Mexico v. Meta Platforms Inc., a jury in the First Judicial District Court of New Mexico found Meta liable on all counts, and said Meta must pay $375 million to the state of New Mexico on claims that Meta concealed the scope of mental health harms affecting underage users.[6]

On March 25, in K.G.M. v. Meta Platforms Inc., a Los Angeles County Superior Court jury returned a verdict awarding damages to private plaintiffs against Meta and Google for harms associated with their allegedly addictive platform designs.[7]

These claims, brought under consumer protection and public health laws, focus on whether specific platform design features, engagement mechanics and moderation practices created or amplified risk.[8]

The inquiry in these cases is not limited to what platforms said publicly; it focuses on how their systems were designed and operated in practice. Investigations have sought internal research on teen mental health, product design risk assessments, engagement metrics, and detailed moderation and enforcement records.

The central question is how these platforms were designed and governed, and whether known risks were adequately addressed in their operation. Defendants, in turn, must often demonstrate that they acted reasonably in the design and oversight of systems that generate — and rely on — billions of data points capturing interactions between users and content.

Other high-profile disputes follow a similar pattern. Litigation involving Uber, filed on March 10, 2025 — i.e., Uber Technologies Inc. v. U.S. Judicial Panel on Multidistrict Litigation, in the U.S. Court of Appeals for the Ninth Circuit — has examined ride-level safety data, background check protocols, and incident reporting systems in assessing claims related to rider safety.[9]

Actions involving Airbnb related to housing regulations and safety practices have required production of host-level listing and booking data, along with internal compliance controls.[10] And more broadly, enforcement actions and private litigation have addressed issues involving privacy and digital tracking of user information,[11] labor regulation and compensation practices,[12] and the distribution of illicit content.[13]

In each instance, the claims rely on established statutory authority — often developed before the modern platform economy reached its current scale — while requiring detailed analysis of how operational systems actually function.

Several structural factors help explain the rise of this approach. Unlike in Europe, the U.S. does not have a single digital platform regulatory statute. Instead, legacy internet regulations — including liability shields for user-generated content, data privacy rules and certain general statutory protections, such as those against deceptive practices — create a patchwork of rules. This patchwork continues to shape liability boundaries and has focused litigation on product design and platform conduct rather than offending content.

By comparison, the European Union's Digital Services Act regime provides ongoing inspection and oversight of large platforms. While in Europe, platforms respond to regulatory investigations,[14] in the U.S. they face enforcement actions and private claims, through which their conduct is examined in detail and standards of behavior are tested.

Taken together, these developments mean that questions of liability increasingly turn on how platform systems perform in practice, as reflected in underlying data and operational records.

Analyzing Platform Conduct at Scale

Litigating requires analysis of platform conduct at scale using large volumes of operational data. These inquiries focus on whether moderation protocols were applied consistently, whether safety mechanisms operated as intended, whether identified risks were addressed, and whether algorithmic systems were appropriately designed and supervised.

Addressing these questions requires analysis of operational metadata, system logs, and code across time, user populations and geographies. In practice, these analyses tend to fall into four categories: (1) system-level data analysis; (2) empirical testing of governance systems; (3) sampling and scalable review; and (4) backtesting and artificial intelligence-enabled analysis.

System-Level Data Analysis

Enforcement actions and litigation involving technology platforms routinely rely on large and detailed datasets, including:

- User-level transaction records;
- Content-level moderation histories;
- Records of algorithmic decisions and associated metadata;
- Enforcement and escalation logs; and
- Incident reporting and remediation timelines.

For example, in ride-sharing contexts, ride-level and incident-level data may be used to evaluate reporting rates, response times, repeat-event patterns, and geographic variation in safety outcomes.

In matters involving short-term rental platforms, listing and booking data may be used to assess whether compliance controls were applied consistently across hosts and markets.

Analysis of these data can reveal patterns that are directly relevant to legal claims. Trends over time, jurisdictional variation, and differences across user segments can provide evidence regarding how governance systems operate in practice and whether they function consistently with stated policies.

Empirical Testing of Governance Systems

Questions concerning platform design or moderation practices often require quantitative evaluation. These analyses may include:

- Measuring incident rates before and after policy changes;
- Assessing detection accuracy, including false positive and false negative rates;
- Evaluating the degree of ambiguity in moderation decisions;
- Analyzing response times and remediation outcomes; and
- Comparing enforcement patterns across user groups or time periods.

In cases involving alleged harms to teenage users, for example, these methods may be used to evaluate whether platform design changes, warning systems, age-based restrictions or usage limits affected exposure to risks of harm. These analyses can become central to assessing whether safeguards operated as intended and whether risk mitigation measures were effective.

Sampling and Scalable Review

Given the scale of platform activity, reviewing every transaction or moderation decision is rarely feasible. Statistically grounded sampling methods allow for representative evaluation

while managing cost and complexity. Properly designed samples may be used to examine subsets of users, transactions or moderation decisions and to assess enforcement consistency and system performance across large populations.

Sampling provides a structured and methodologically defensible way to evaluate complex systems in litigation and enforcement contexts.

Backtesting and AI-Enabled Analysis

Where governance rules are embedded in automated systems or structured review processes, they may be evaluated through backtesting against historical data. Analytical models can apply policy logic to prior datasets to assess how safeguards operated and whether outcomes aligned with design expectations.

In content moderation contexts, for example, prior decisions may be reevaluated under alternative policies to assess how outcomes would differ.

AI agents — customized software systems that can apply defined rules or policies across large datasets — extend these capabilities by enabling automated testing of enforcement logic, evaluation of alternative parameters, and identification of anomalies or edge cases. These tools can be used to replicate aspects of moderation or compliance processes at scale, generating structured outputs that support evaluation of system behavior and performance.

Taken together, these analytical approaches provide a framework for evaluating how platform systems operate in practice and can play a central role in assessing whether platforms meet applicable standards of care.

Conclusion

State attorneys general, enforcement agencies and private plaintiff firms are applying established statutory frameworks and tort law to challenge how platforms design, govern and operate their systems, with liability turning on how those systems perform in practice.

Assessing these questions requires structured analysis of operational data using empirical methods such as system-level analysis, sampling, backtesting and the use of AI agents. These approaches make it possible to evaluate platform conduct at scale and to test whether governance systems functioned effectively and as intended.

Current trends indicate that litigation will continue to shape how standards for platform safety and governance are defined and applied.

In this environment, platform data, internal controls and governance systems are not only operational tools — they are sources of evidence that will be scrutinized in enforcement actions and private litigation.

Paul Hinton and Farooq Javed are principals, and James M. Sappenfield is a senior associate, at The Brattle Group.

Brattle principal Mark Sarro contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] For example, New Mexico's state attorney general, Raúl Torrez, sued Meta in 2023, accusing it of misleading consumers about the safety of its platforms, and won a jury damages award of $375 million on March 24, 2026. Cecilia Kang and Eli Tan, "Meta Ordered to Pay $375 Million Over Child Safety Violations," The New York Times, March 24, 2026. "Mr. Torrez said he would ask the judge, Bryan Biedscheid, for additional financial penalties during a bench trial that is scheduled to start May 4. Mr. Torrez also plans to ask the court to force changes to Meta's apps to make them safer for young users."

[2] For example, in a bellwether personal injury case, Meta and YouTube must pay a plaintiff a combined $6 million after a jury found that they knowingly designed features that were addictive and harmful for a young user. Mark Abramson, Cecilia Kang, Ryan Mac, and Eli Tan. "Meta and YouTube Found Negligent in Landmark Social Media Addiction Case," The New York Times, March 25, 2026.

[3] Clough, Craig, "Jury Doubles Damages Against Meta, Google In LA Bellwether," Law 360, March 25, 2026, https://www.law360.com/corporate/articles/2452908.

[4] Salvatore, Cara, "Meta Owes $375M In NM Trial Over Harm to Teens," Law 360, March 24, 2026. https://www.law360.com/articles/2457141/meta-owes-375m-in-nm-trial-over-harm-to-teens.

[5] (State of Arizona ex rel. Kris Mayes, Attorney General, et al. v. Meta Platforms, Inc., et al. (N.D. Cal., filed Oct. 24, 2023)). Ortutay, Barbara, "States Sue Meta Claiming its Social Platforms are Addictive and Harm Children's Mental Health,"AP News, October 24, 2023, https://apnews.com/article/metachildrenteensharmslawsuit-17858802d76143d358e38ee15150dc94; "Judge Allows Virginia's Lawsuit Against TikTok to Move Forward," 29News, Oct. 27, 2025, https://www.29news.com/2025/10/27/judge-allows-virginias-lawsuit-against-tiktok-move-forward/.

[6] Salvatore, Cara, "Meta Owes $375M In NM Trial Over Harm to Teens," Law 360, March 24, 2026. https://www.law360.com/articles/2457141/meta-owes-375m-in-nm-trial-over-harm-to-teens.

[7] Clough, Craig, "Jury Doubles Damages Against Meta, Google In LA Bellwether," Law 360, March 25, 2026, https://www.law360.com/corporate/articles/2452908.

[8] (State of Arizona ex rel. Kris Mayes, Attorney General, et al. v. Meta Platforms, Inc., et al. (N.D. Cal., filed Nov. 22, 2023)). See, e.g., Complaint for Injunctive and Other Relief, Arizona v. Meta Platforms, Inc., No. 4:23-cv-05448-YGR (N.D. Cal. Nov. 22, 2023), https://www.azag.gov/sites/default/files/2025-06/Doc%2073-2%20Complaint%20%28limited%20redactions%29%20-11.22.2023%20%281%29.pdf.

[9] See, e.g., Elias, Paul, "California Sues Uber in Startup's Latest Legal Woe," APNews, December 10, 2014, https://apnews.com/general-news-small-business-b3b70d1d0e314a83aa14188bb4d9c2a9; Uber Techs., Inc. v. U.S. Jud. Panel on Multidistrict Litig., No. 23-3445, slip op. (9th Cir. Mar. 10, 2025), https://law.justia.com/cases/federal/appellate-courts/ca9/23-3445/23-3445-2025-03-10.html.

[10] (Bodin et al. v. The City of New Orleans (E.D. La., filed Feb. 14, 2025); Airbnb, Inc. v. New York City Mayor's Office of Special Enforcement (Supreme Court, New York County, Aug. 8, 2023)). See, e.g., Brook, Jack, "Airbnb Sues New Orleans After it Adopts Sweeping Regulations Governing Short-Term Rentals," AP News, February 18, 2025, https://apnews.com/article/airbnb-lawsuit-new-orleans-f72e801422838e5686e54c2ac72ebcf1; https://www.nycourts.gov/reporter//pdfs/2023/2023_32740.pdf.

[11] Privacy: Scarcella, Mike, "Google Defeats Bid for Billions of Dollars of New Penalties in US Privacy Class Action," Reuters, January 30, 2026, https://www.reuters.com/sustainability/boards-policy-regulation/google-defeats-bid-billions-dollars-new-penalties-us-privacy-class-action-2026-01-30/.

[12] (Rodriguez et al. v. Google LLC (N.D. Cal., filed July 14, 2020); Seattle Office of Labor Standards settlement with Portier, LLC d/b/a Uber Eats (announced Aug. 26, 2025); Labor Compensation: Kroman, David, "Uber Eats agrees to $15 million settlement with Seattle," The Seattle Times, August 26, 2025, https://www.seattletimes.com/seattle-news/politics/uber-eats-agrees-to-15-million-settlement-with-seattle/.

[13] (Mayor and City Council of Baltimore v. X Corp., X.AI Corp., X.AI LLC, and Space Exploration Technologies Corp. (Circuit Court for Baltimore City, filed Mar. 24, 2026)); Illicit content: Eberhart, Maria, "What Baltimore's Lawsuit Against Grok Says About how States and Cities Can Regulate AI," Technical.ly, March 25, 2026,https://technical.ly/civics/baltimore-grok-lawsuit-ai-oversight/.

[14] Adam Satariano, "Snapchat Investigated in Europe Over Child Safety Policies," March 26, 2026.