

AI

Compliance and privacy risk in AI washing



Photo: Thibault Renard/Getty Images



Kiley Kio, FTI Consulting; Dera Nevin, FTI Consulting

October 9, 2026 • 5 min read



We address the gaps between a company's claims and its actual AI capabilities or practices.



The promise of artificial intelligence has generated enormous commercial momentum and with it, a growing pattern of misrepresentation of its use. AI washing, the gaps between what companies claim their AI does and what it actually delivers or how it uses data, has become a defining compliance and governance challenge



of the current era. Regulators across jurisdictions are responding with escalating enforcement, and the consequences for enterprises caught on the wrong side of that gap are increasingly severe.

AI washing occurs when organizations misrepresent, exaggerate, or fabricate the role of AI and how it's used. The term gained formal regulatory currency in March 2024, when the SEC analogized it to greenwashing and framed AI washing as a fundamental deception applied to a new technology domain. Since then, US federal regulators have brought more than a dozen enforcement actions targeting AI washing, with penalties ranging from six-figure civil settlements to criminal fraud indictments. Securities class action filings with AI-related allegations roughly doubled from 2023 to 2024. As of late 2025, the Federal Trade Commission noted it will “hold accountable actors that use AI to violate the law or deceive consumers about the capabilities of their generative AI.”

The commercial pressure to appear AI-forward is immense. More than [two-thirds of S&P 500 companies now cite AI](#) in their quarterly earnings calls, an unprecedented level over the past decade. Yet independent analyses consistently find that the vast majority of organizations remain in early-stage AI adoption, with a limited number generating measurable business impact from AI deployments.

Manifestations of AI washing

AI washing can be considered in four key categories, each carrying different risk profiles. These include:

1. **Technical capability inflation:** Overstating the accuracy, autonomy, or sophistication of actual AI systems. For instance, claiming high detection accuracy for a system that independent testing shows performing near random chance.



- **Governance washing:** Overstating commitments to responsible, ethical, or compliant AI practices without corresponding internal controls, policies, or oversight structures. This risk is particularly acute from a privacy and data compliance perspective. AI implementations that outpace an organization's governance commitments can silently erode existing data protection controls, creating discrepancies between what an organization's privacy program says it does and what their AI systems are actually doing with personal data.
- **Strategic signaling:** Using AI terminology in earnings calls, SEC filings, and investor presentations to inflate perceived innovation or market value without corresponding operational reality.
- **Marketing washing:** Labeling products "AI-powered" when they rely on rule-based logic, manual human labor, or minimal machine learning. Marketing washing is often identified only after a product failure or regulatory inquiry surfaces the gap.

Top challenges

Numerous risks can arise when organizations over-rely on AI systems with capabilities that have been misrepresented, whether by internal teams or external vendors. Vendor concentration in AI supply chains creates single points of failure that compound when underlying capabilities are overstated or remain static in comparison to rapidly evolving technologies. Additionally, enterprises that repeat vendor AI claims in their own customer or investor communications can inherit that misrepresentation and its regulatory consequences.

The issues legal, compliance, privacy, and technology teams most commonly encounter include vendor claims that are not verified, enterprise AI claims outpacing internal reality, governance commitments



that exist only on paper, no centralized AI inventory, and misalignment between cross-functional teams.

The organizations best positioned in this environment will be those that treat AI governance not as a documentation exercise, but rather as an operational discipline that runs alongside every AI-related decision they make.

From a governance perspective, organizations may have published AI ethics principles, responsible AI frameworks, or governance policies; however, few have operationalized those commitments into the day-to-day processes that govern how AI systems are built, deployed, and monitored. The result: The gap between the published policy and the lived practice may result in a form of governance washing that becomes increasingly visible to regulators reviewing documentation in the context of enforcement inquiries.

Managing AI washing risk

The gap between AI washing as a defined risk and AI washing as a managed risk is primarily an execution problem. Having the right expertise to cut through these issues in practice can accelerate an organization's path from awareness to operational governance, reduce deployment and procurement timelines without sacrificing rigor, and produce documentation that is defensible to regulators, investors, and boards. The following recommendations address areas that are most likely to attract regulatory scrutiny.

Close the gap between governance commitments and practice

Regulators and plaintiffs' counsel reviewing AI washing allegations and AI-related data privacy violations do not evaluate governance by reading policy documents. A polished responsible AI framework sitting



above an absent or inconsistent operational process is not a mitigating factor, and may become a credibility problem. Closing that gap requires two things that are distinct but mutually reinforcing.

The first is process integration, likely using defined standard operating procedures – embedding AI review checkpoints into software development and procurement lifecycles, establishing escalation protocols when AI use or AI's use of data deviates from stated claims, and creating audit mechanisms that verify governance and privacy policies are being followed in practice rather than merely published.

The second is to solidify board-level ownership of AI oversight. Board visibility creates accountability and ensures governance commitments receive adequate resourcing.

Focus on claim accuracy

Currently, enforcement against companies making false or unsubstantiated claims about their own AI capabilities has continued and intensified, while enforcement against neutral AI tool providers has curtailed. This means the live risk for most enterprises is not whether they are building or selling AI tools; rather, it is whether the claims they make about those tools are accurate.

The practical implication is straightforward. Invest compliance resources in the substantiation of specific, affirmative AI claims rather than in broad AI governance posturing. A company that makes three well-documented AI capability claims is in a materially stronger position than a company that makes 30 undocumented ones.

Build an AI inventory before a regulator asks for one

In significant AI washing enforcement actions to date, the primary investigative question has been the same – “What does this system



actually do, and what documentation exists to support the claims made about it?”

Organizations that cannot answer these questions with current, specific, and defensible documentation are relying on goodwill they may not receive. AI inventories should document each system in use, the claims made or intended to be made about it, the evidence base for those claims, and the date of last validation

Tighten vendor due diligence

The enterprise that inherits a vendor’s misrepresentation by passing it downstream does not escape liability by pointing back to the vendor, particularly if they made no independent review of that claim. Having the right framework to evaluate vendor AI claims can compress deployment and procurement timelines while building a defensible evidentiary record.

Companies should ensure they review the design and execution of AI-specific vendor due diligence to ensure their programs are tailored to specific AI-technology risks. AI vendor due diligence programs should include tailored due diligence questionnaires, technical claims verification, and independent performance benchmarking. Procurement frameworks should be updated to require vendors to specify the AI and machine-learning techniques actually in use, provide independent performance evidence, and commit contractually to the representations made during the sales process. Where a vendor will not provide that documentation, refusal should be treated as a material finding.



The risk of AI washing as a compliance and privacy issue can arise within any gap created between the commercial pressure to signal AI sophistication and the operational discipline required to back those signals up. That gap is where enforcement actions may be born, where



securities class actions may find their footing, and where board and executive credibility may be most exposed.

Although the enforcement landscape continues to evolve, the underlying legal exposure has concentrated around a predictable set of risks. Companies that make accurate, documented, and substantiated AI claims and that build the internal processes to keep those claims current are building the kind of institutional credibility that regulators, investors, and customers expect as a baseline.

The organizations best positioned in this environment will be those that treat AI governance not as a documentation exercise, but rather as an operational discipline that runs alongside every AI-related decision they make.

Kiley Kio is a director at [FTI Consulting](#). [Dera Nevin](#), managing director, is a data lawyer and expert with more than 20 years of experience addressing digital risk issues, including privacy, data protection, information risk management, e-discovery, advertising technology, and the application of emerging technologies to the delivery of legal services and compliance programs.



Popular Tags

Accounting

AI

AI washing

Data privacy

Governance

Industry

IT

Privacy

Risk

SEC

Technology

Third-party vendors

UK

US Content

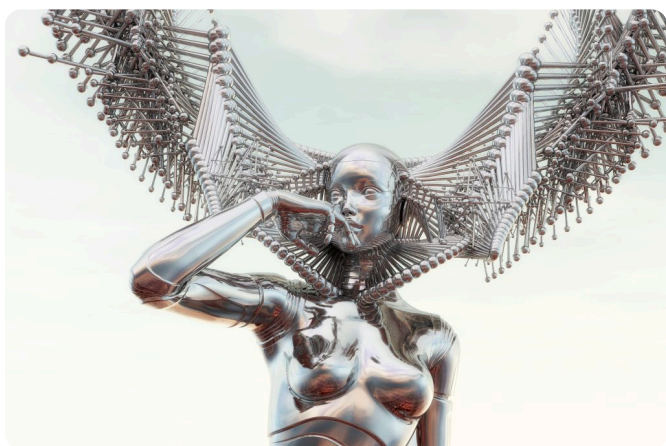




Make the most of Premium

You've got access to everything on GRIP – all articles from our 5,000+ archive, exclusive podcasts and interviews, and Rules Navigator to stay ahead. It's all yours for another 144 days.

You may also like



AI

AI enforcement accelerates as federal policy stalls and states step in

This article examines the evolving federal and state AI enforcement landscape and outlines practical considerations for companies deploying AI technologies.

Ezra D. Church, Morgan Lewis; **Elizabeth B. Herrington**, Morgan Lewis

Apr 20, 2026



ESG

Clean claims or dirty lies? The battle against corporate washing

Washing risks can lead to loss of reputation, loss of stakeholder trust and goodwill, employee brand damage, and costly legal/regulatory action.

Thera Adam van Straaten, Eversheds Sutherland; **Eve England** | Eversheds Sutherland; **Louise Howarth**, Eversheds Sutherland; **Zoe Haden**, Eversheds Sutherland

Dec 3, 2024





AI

Gensler speaks about AI and the risk of AI-washing, conflicts, deception

Publicly traded companies that misleadingly promote their use of AI risk engaging in “AI-washing” and running foul of US securities law, said SEC Chair Gary Gensler.

Julie DiMauro • Feb 14, 2024



Enforcement

SEC and SDNY signal eyes on AI-washing fraud as AI firm founder charged

G. Premium

The SEC is eyeing bold claims made by AI startups and investors about AI capabilities, and this AI-washing case is a prime example.

Julie DiMauro • Jun 13, 2024

Grip. By  **globalRELAY.**

[About Grip](#) | [Contact Us](#) | [Editorial Policy](#) | [Legal Terms & Policies](#)

Copyright © 2026 Global Relay Communications Inc. All Rights Reserved.

