John C. Coffee, Jr. – Boeing and the Future of Deferred Prosecution Agreements

By John C. Coffee, Jr.

Leveraging Information Forcing in Good Faith

By Hillary Sale

The Dark Side of Safe Harbors

By Susan C. Morse

THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Where Is Litigation Over AI Headed?

By Evan Bundschuh and Brad Nash November 6, 2023

Edit |

In emerging AI-related litigation, one of the most common claims so far concerns alleged over-stating or misrepresenting a company's AI capabilities to its investors. According to Stanford's Class Action Clearinghouse, there have been more than 50 class-action lawsuits involving so-called "AI-Washing." In response, the SEC has issued specific and repeated disclosure guidance, and recent statements also appear to confirm the Commission's emphasis on AI disclosures.

The current regulatory environment, however, is a dizzying patchwork of statutes and regulations. They include amendments to existing cyber or privacy laws, consumer protection laws, and discrimination laws, as well as specific and very different AI laws enacted by states. Some statutes are aimed at "frontier" developers, others address "deployers" of AI systems, and still others are designed to protect consumers, particularly in high-risk industries such as healthcare. California, Utah, Colorado, New York, and the EU are among the jurisdictions that have already passed broad regulations. Among the goals of these regulations are:

- Ensuring the safety of artificial systems
- Avoiding algorithmic bias or discrimination, including in employment decisions
- Requiring disclosures when clients or customers are engaging with AI (such as chatbots) and providing opt-out choices
- Labeling of AI-generated content, especially for political ads; and
- Requiring consent to share information that may be used to train AI models

Some of the statutes, such as California's recently passed "Transparency in Frontier Artificial Intelligence Act," implement certain whistleblower protections. Another California bill, SB468, would require businesses to implement ongoing training and designate individuals responsible for a company's "high risk" AI systems." According to the bill:

> A covered deployer whose high-risk artificial intelligence systems process personal information shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards……The program shall include the designation of one or more employees of the covered deployer to maintain the program…..Requiring ongoing employee and contractor education and training, including education and training for temporary employees and contractors of the covered deployer, on the proper use of security procedures and protocols and the importance of personal information security.

As one of the first regulations requiring the designation of responsible individuals, the proposed California legislation would increase individual accountability, whether those responsibilities are ultimately those of the organization's CISO or another designated officer, as may be determined by the company. These designated individuals may eventually encounter challenges similar to those already being faced by CISOs following cyber/privacy events, especially as legislation proliferates and develops.

According to the National Conference of State Legislatures, as of July 10, 2025, "38 states have adopted or enacted around 100 measures this year" addressing Artificial Intelligence. We can expect even more states to adopt regulations, which will eventually extend to a greater range of industries and operations while companies grapple with compliance requirements.

Given their recent emergence, these requirements may be unfamiliar to many companies, creating considerable risk of missteps. Some of them may also pose their own challenges. For example, regulations requiring notification to customers if their data are being used to train AI models may not be so straight forward given the broad use of third-party vendors that may, without an organization's knowledge, collect shared data to build or improve their own AI models. California's CPPA's recently finalized AI regulations specify that outsourcing of AI to third parties for specific uses does not insulate an organization from liability. This underscores the importance of AI-specific contractual language and strong third-party governance.

In addition to these risks, lawsuits have been filed against companies that fail to disclose their use of AI. Some suits involve allegedly inadequate disclosures of risks related to companies' use of artificial intelligence. For example, Sarria v, Telus, a class action lawsuit against a Canadian telecommunications and technology company, alleges that Telus failed to disclose to shareholders that its AI offerings could decrease revenues by cannibalizing sales from other product offerings.

More litigation could emerge over alleged "human-washing," the practice of overstating and charging for human performance actually done by AI systems. While AI can be helpful in a wide range of tasks, it still cannot replace human expertise, especially in jobs requiring specialized skills. Many clients may prefer to hire firms where humans perform the work, wanting to avoid reported AI hallucinations and other concerns with AI. In response, companies may soon advertise their human approach and refusal to use AI. Some companies have already come out publicly against the use of AI. Those companies, however, might expose themselves to allegations of human washing if they have, in fact, made use of artificial intelligence to reduce costs or expand their operations to include services in which they may lack expertise.

Compounding these challenges are unclear or inadequate insurance policies. Claims involving the capture of data by AI chatbots may be precluded by an organization's cyber policy. Failures of AI-provided professional services may be excluded from coverage by professional liability policies because services were not wholly provided by "natural persons." Insurers may also argue that investor claims following AI failures are precluded by a D&O policy's professional services exclusion. Furthermore, some insurers are beginning to draft explicit AI exclusions that are near absolute, precluding coverage for wrongful acts "in any way involving" the use of any AI (including wrongful acts committed by third- party vendors.

In response to these emerging risks, both "frontier" developers and deployers of AI systems will need to regularly and carefully monitor emerging legislation (including cross border regulations) to ensure compliance, while ensuring any statements made regarding the implementation of AI and capabilities of its systems, are as accurate as possible. As demonstrated above, even companies refraining from using AI could be subject to litigation and will need to be careful in any public statements, particularly about disclaimers of the use of AI or the firm's human capabilities or deliverables. Corporate officers and their counsel will also need to carefully monitor insurance policy terms, performing updated coverage assessments, particularly as to directors and officers insurance.

This post comes to us from Evan Bundschuh, vice president and head of professional and financial lines insurance at the insurance firm of GB&A in New York, and Brad Nash, an insurance-recovery partner at the law firm of Hoguet Newman Regal & Kenney, LLP in New York.

Edit