



“If board directors will ultimately be accountable for how AI technologies are deployed and leveraged within their enterprises, then it’s critical that **executive leaders no longer view data as solely the purview of IT.**”

—Dominique Shelton Leipzig
Partner, Mayer Brown &
Author, *Trust: Responsible AI, Innovation, Privacy and Data Leadership*

AI ACCOUNTABILITY IS COMING FOR YOUR BOARDROOM

A tsunami of legislation could soon change how your board applies oversight to AI activities—and you could be held personally accountable if and when trouble arises.

By Bonnie Wingate

In January 3, 2024, the U.S. Securities and Exchange Commission (SEC) ruled that two of the world’s largest publicly traded companies—Apple and Disney—must allow shareholders to vote on their use of artificial intelligence (AI). The shareholder proposals were filed by a pension trust of the AFL-CIO, the largest American labor union federation, despite opposition from both companies, who sought to exclude these votes from their annual meetings.

At Apple, the AFL-CIO requested a report on the company’s use of AI in business operations and the disclosure of any ethical guidelines regarding AI technology. Similarly, at Disney, the proposal

called for a report on the board’s role in overseeing AI usage.

Although both measures ultimately failed to garner the number of proxy votes required to pass, the SEC’s ruling mirrors signals from the U.S. Justice Department, which, since 2022, has been actively charging ahead with policies that would make CEOs and board directors personally accountable for the effectiveness and safety of their AI compliance programs. In practice, SEC rules would have required Disney and Apple to publish annual reports describing the board’s oversight of cybersecurity threats, including identifying the persons responsible for how the board is informed about and responds to risks.

Both moves hint at what’s on the horizon:

scrutiny over AI in the corporate world is reaching a fever pitch, driven by institutional investors clamoring for responsible AI development and shareholders’ concerns regarding executive oversight into how these technologies are used.

From a regulatory perspective, board directors and corporate governors are best situated to ensure that their companies are on track to reap the benefits of AI while avoiding its harms and litigation risks. Thus, they will undoubtedly find themselves squarely in regulators’ cross-hairs as legislation becomes codified.

The startling truth is that board directors may face increased personal liability for AI-related mishaps if current litigation

Accountability Partner
One of the U.S.’ top privacy, artificial intelligence and data lawyers, Dominique Shelton Leipzig helps clients navigate the evolving legal compliance issues related to privacy, artificial intelligence and data security for their digital data initiatives. In her fourth book, *Trust: Responsible AI, Innovation, Privacy and Data Leadership*, Ms. Shelton Leipzig has pioneered a step-by-step approach for board members to successfully optimize digital technologies through responsible data stewardship.

PHOTO COURTESY OF DOMINIQUE SHELTON LEIPZIG

“As a first step, the board and CEO will want to ensure that the AI governance teams are identifying each and every use case, as previously mentioned, and include a ranking for each.”

—Dominique Shelton Leipzig

trends serve as an indicator. Board governors risk legal liabilities—for the company and themselves—if they fail to fulfill their fiduciary duty and mitigate preventable harms from AI systems created or deployed by the companies they oversee.

In addition to actions taken by the SEC and U.S. Justice Department, a medley of legislative and regulatory activities are underway across the US, UK, and EU.

In the U.S., the Federal Trade Commission (FTC) is advocating for boards to oversee AI as a mission-critical operation. Additionally, U.S. companies using AI in products and services directed to EU residents will be subject to a sweeping set of new governance obligations that will most likely take effect in 2026, underscoring the need for global companies to understand the new requirements now so they can tailor their expenditures to align with the forthcoming expectations.

In Europe, one of those expectations—as laid out in a recent draft of the EU AI Act—is to codify “trustworthy AI” to ensure a high level of protection of health, safety, fundamental rights, democracy, the rule of law, and the environment from the harmful effects of artificial intelligence systems.

“These developments signal a significant shift towards increased accountability and transparency in corporate AI practices, emphasizing the need for ethical guidelines and oversight at the board level,” says Dominique Shelton Leipzig, the author of *Trust: Responsible AI, Innovation, Privacy and Data Leadership*, published by Forbes Books in December 2023.

In addition to *Trust*, Ms. Shelton Leipzig is a partner at Mayer Brown, an international law firm representing global corporations, investment funds and financial institutions. There, she is a member of the firm’s cybersecurity and data privacy practice and leads the ad tech privacy and data management

team. She is also leader of the firm’s Global Data Innovation team that provides CEOs and Board Members with advice regarding effective digital governance. In *Trust*, she provides CEOs and board directors with a step-by-step approach for successfully optimizing digital technology through responsible data stewardship.

“Enhanced scrutiny and codified legislation regarding corporate AI practices is just around the corner,” says Ms. Shelton Leipzig. “If board directors and corporate governors will ultimately be accountable for how these technologies are deployed and leveraged within their enterprises, then it’s critical that executive leaders no longer view data as solely the purview of IT.”

Understanding the Board’s Role in the Coming Compliance Tsunami

To establish trustworthy AI frameworks that meet stakeholder demand and weather the looming compliance storm is crucial., Ms. Shelton Leipzig provides directors with an actionable playbook for transforming their organizations into ethical data leaders.

By utilizing trustworthy AI frameworks and aligning their data strategy with long-term growth, enterprises can build stakeholder engagement and avoid costly missteps. She advises corporate governors to prioritize the following six variables as part of their oversight strategy:

1. Human oversight is key to AI success.
2. Accuracy and cybersecurity are critical to protect the integrity of the data collected for the AI and the algorithms’ output, especially in machine learning, with machines generating their own patterns.
3. Processes should be in place for testing and monitoring algorithms to ensure unintended consequences do not emerge.

4. If you lead a large technology company that creates generative and other AI offerings as a service, you should conduct an antitrust analysis (of increased focus by regulators) to protect against monopolization charges based on AI.
5. Ensure testing and verify accuracy after routine changes have been made to systems, such as operating system changes or software changes.
6. Ensure diverse teams are involved in algorithmic development, data training, and system protection, which will help insulate companies from drawing a regulator’s ire about a lack of diverse perspectives used to train models.

“With a groundswell of regulatory legislation on the horizon, now is the time for boards to get ahead of AI-related concerns and risks in order to build a foundation of trust with stakeholders,” says Ms. Shelton Leipzig. “It’s important to comprehend the sheer volume of draft legislation that exists, which currently amounts to over 3,000 pages of relevant proposed legislation.”

Furthermore, says Ms. Shelton Leipzig, the regulatory tsunami is not just a factor in the US and EU, but also on six different continents and in seventy-six countries, which sits on top of the existing (less comprehensive) AI laws in 127 countries that are already in place, having been enacted since 2016.

“Among the nations drafting regulations to govern AI, the US has been active, largely inspired by the commercialization of generative AI,” she says. “Right now, there are 146 state and federal bills pending in state capitols and the US Congress.”

While it’s completely understandable that most C-suite executives, board members, and their legal counsel would not yet have had the opportunity to wade through all of these various provisions, it’s important to know that substantial similarities exist among the vast majority of these legislative measures. “There are certainly numerous explanations for these commonalities,” says Ms. Shelton Leipzig.

PHOTO COURTESY OF DOMINIQUE SHELTON LEIPZIG

“To begin with, although this technology might be bleeding edge, these aren’t new ideas or concepts. These trusted AI legal frameworks have been contemplated and in development by governments around the globe, in conjunction with research scientists, for a relatively long time, since at least 2017.”

Additionally, she advises that when you have a mountain of draft legislation that addresses the same core criteria, corporate directors would be well-served to future-proof their digital activities by mapping legislative trends into a reasonably predictable future.

“It’s very important for our C-suite, board, and in-house communities to understand that one of the most obvious similarities among these regulatory efforts is that the vast majority do not attempt to legislate by dealing with the AI technology in the abstract,” counsels Ms. Shelton Leipzig. “These legislative provisions almost uniformly hone in on the particular use case and trigger governance with very specific focus and intention. Of particular importance, the vast majority of these efforts call for a ranking of risk according to prohibited uses, high and medium, and low risk.”

To address these concerns, Ms. Shelton Leipzig introduced a “traffic light” framework to aid companies in managing AI governance and decision-making based on proposed legislation:

1. **Red-Light Use Cases (Prohibited):** Legal frameworks have identified 15 scenarios where AI should not be used. For instance, AI should be excluded from surveillance related to democratic activities like voting or ongoing public surveillance. Remote biometric monitoring and social scoring—where social media activity influences decisions on loans or insurance—are also discouraged. “Governments don’t want private companies doing this due to the potential for significant harm,” Ms. Shelton Leipzig noted.
2. **Green-Light Use Cases (Low Risk):** These include AI chatbots and product recommendations, which are generally deemed low-risk and safe from bias or other concerns. Many of these uses have a proven track record of safety.



Dominique Shelton Leipzig
Partner, Mayer Brown & Author, *Trust: Responsible AI, Innovation, Privacy and Data Leadership*

Dominique Shelton Leipzig is one of the U.S.’ top privacy, artificial intelligence and data lawyers, and is a Chambers-ranked partner at Mayer Brown’s Los Angeles office. She is a member of the firm’s cybersecurity & data privacy practice, and she also leads the firm’s ad tech privacy & data management team. At Mayer Brown, Ms. Shelton Leipzig advises CEOs and board members on their fiduciary duty of oversight related to emerging digital and data technologies, including generative AI.

In her fourth book, *Trust: Responsible AI, Innovation, Privacy and Data Leadership*, Ms. Shelton Leipzig has pioneered a step-by-step approach for successfully optimizing digital technology through responsible data stewardship.



Act Now, Don't Delay

Ms. Shelton Leipzig advises companies not to delay adopting crucial AI governance measures despite evolving legislation. "Waiting for final laws is unnecessary," she says. "Implementing these guardrails offers visibility into AI operations and ensures compliance, preventing potential fines or brand damage."

3. Yellow-Light Use Cases (High-to-Medium Risk): Most AI applications fall into this category. These high-risk cases require rigorous governance. Nearly 140 examples—from AI in HR processes, family planning, surveillance, democracy, and manufacturing—fall into this category. High-risk financial applications include evaluating creditworthiness, managing investment portfolios, or underwriting financial instruments.

To aid boards in determining appropriate use cases—as well as applicable and relevant precautions—Ms. Shelton Leipzig created

a "cheat sheet" that directors should ask regarding the use of generative AI in their company, which are mapped to the governance best practices outlined in the hundreds of pages of legislation introduced around the world. They include:

- How are we using AI?
- Have we segregated training data to know its provenance?
- Are we using protected data that can be subject to opt-out or removal requests?
- How are we testing, monitoring, and auditing for accuracy, fairness, bias elimination, and privacy, considering cybersecurity, product safety, IP, and

antitrust? Are these efforts logged and reflected in the AI system's metadata?

- How can we review and approve AI governance policies, including human oversight?
- Are we developing AI in line with legislative and regulatory expectations and mapping our governance to the draft EU AI Act?

"Based on my experience in the privacy world, these questions are important to ask since much of the pending legislation continuously calls for the same types of protections around the world," she says. "It is rare that less governance will be contemplated

ISTOCK

by regulators."

A Seven-Step Playbook for Board Directors

In addition to formulating questions that board directors should pose to teams managing AI implementations, Ms. Shelton Leipzig also offers a prescriptive path for corporate governors to assemble a playbook for developing trustworthy AI frameworks.

"As a first step, the board and CEOs will want to ensure that the AI governance teams are identifying each and every use case, as previously mentioned, and include a ranking for each," she says.

In the event that high-risk use case profiles are identified, prevailing trends strongly indicate that regulators and legislators intend to audit licensors of AI models, as well as licensees, to ensure that their enterprises are following a seven-step AI governance program, as follows:

Step One: Confirmation of High-Quality Data Use:

The first step is to determine if any projects use high-quality data, as defined by each piece of legislation. "High-quality data" generally means data that is relevant and material to the exercise. Specific additional factors may apply, but this definition suffices for immediate purposes.

Step Two: Continuous Testing, Monitoring, and Auditing:

Once identified, the second step is to ensure continuous testing, monitoring, and auditing of high-risk AI in areas like algorithmic impact, IP, accuracy, product safety, privacy, cybersecurity, and antitrust. Boards should ensure they receive cyber reports on high-risk AI—and understand high-risk AI use in relevant jurisdictions—and whether their AI systems have testing, monitoring, and auditing capabilities.

Step Three: Risk Assessment:

Next, conduct a risk assessment based on pre-deployment testing and ensure this is reflected in the AI system's logging and metadata, including mitigation efforts. It's crucial not to wait until after deployment for testing capacity. Instead, board members should maintain close communication with the AI governance team

"With a groundswell of regulatory legislation on the horizon, now is the time for boards to get ahead of AI-related concerns and risks in order to build a foundation of trust with stakeholders."

—Dominique Shelton Leipzig



to ensure that necessary measures for required testing, auditing, and monitoring are in place and up-to-date to future-proof the AI.

Step Four: Technical Documentation: It is important to factor into operational strategies that these required testing, monitoring, auditing, and mitigation measures need to be appropriately documented and reflected in the AI technical system itself. The capacity to test is crucial across various AI frameworks globally, including those in Singapore, the EU, Australia, Canada, and other jurisdictions. Enterprises must engage their AI governance teams to discuss these critical issues and ensure compliance. For those licensing large language models, enabling testing within the AI system is essential. Continuous monitoring and auditing must also be in place post-testing to reflect logging data and metadata accurately. Coding within the AI system is necessary for testing, monitoring, and auditing functions. Incorporating these features during the building phase is relatively inexpensive compared to retrofitting afterward.

Step Five: Transparency: Licensors and licensees of high-risk AI must inform end-users about AI capabilities and limitations, ensuring the system’s explainability to third-party auditors or regulators. Pending legal AI frameworks emphasize transparency to users about AI interactions and abilities, reflecting the evolving nature of technology and the need to inform users about AI presence, capabilities, and potential third-party auditing.

Step Six: Human Oversight: Trusted legal frameworks mandate human intervention to address deviations promptly, ensuring real-time protection of the brand and prevention

“Regulatory changes make AI accountability and transparency essential. Boards that adopt strong AI governance can fast-track their ability to meet stakeholder and regulatory demands, while also establishing AI oversight as a core component of their business.”

—J.W. Dobbe,
Consultant, Insigniam

of safety issues. For example, if real-time monitoring detects a departure from safety parameters, a designated human AI expert should adjust the model. Boards and executives need assurance of notification systems to alert governance teams of deviations, allowing immediate corrective action to maintain safety standards and brand integrity.

Step Seven: Fail-Safe: In the event that the AI cannot be restored to the approved parameters set in the testing phase, fail-safes must be in place to terminate its use.

Although further exploration and discussion will most likely be needed to fully understand these factors, Ms. Shelton Leipzig advocates for actionable insights to empower board members and CEOs to make informed decisions about risk, opportunity, and avoidance.

The Time for Action is Now

Looking ahead, Ms. Shelton Leipzig advises companies not to delay adopting crucial AI governance measures despite evolving legislation. Emphasizing that AI governance requires collaboration among stakeholders, she highlights the importance of involving the board of directors, general counsel, and CEO throughout the process.

“Waiting for final laws is unnecessary,” she says. “Implementing these guardrails offers visibility into AI operations and ensures compliance, preventing potential fines or brand damage.” **IQ**



Great
Minds
Don't
Always
Think
Alike

Even the best executive can benefit from **new thinking and different action**. Find the fresh perspectives you need right now at insigniam.com/thought-leadership. Stay tuned in to the latest insights at insigniam.com/quarterly-magazine.