Professional Perspective

A Harmonized AI Governance Framework Starting at the Board & C-Suite Level

Arsen Kourinian and Dominique Shelton Leipzig, Mayer Brown LLP

Bloomberg Law

A Harmonized AI Governance Framework Starting at the Board & C-Suite Level

Contributed by Arsen Kourinian and Dominique Shelton Leipzig, Mayer Brown LLP

The rapid advancement of artificial intelligence (AI) and its wide availability to the general public has sparked a debate regarding the safeguards necessary to ensure that AI is used ethically and for the benefit of humankind. A recent open letter published by some AI researchers even calls for an immediate "pause for at least 6 months the training of AI systems . . . to jointly develop and implement a set of shared safety protocols for advanced AI design and development that are rigorously audited and overseen by independent outside experts."

However, as history has shown, human innovation and advancement cannot be paused and it is impracticable to expect new laws, regulations, or expert consensus to be reached in a six-month period regarding AI. Until lawmakers, scientists, and the general public ultimately reach an understanding on how AI should be governed, it will be up to companies to self-regulate the use of AI. To do so, organizations need to implement top-to-bottom AI governance that starts at the board and C-suite level.

State of AI Laws

There is currently no single definition of AI. However, at its core, AI refers to computer systems and machines that can perform tasks that would typically require human intelligence, such as language translation, fraud detection, targeted advertising, virtual assistants, facial recognition, identifying diseases, and growing food more efficiently.

Globally, AI is generally regulated under data protection laws and various frameworks, guidelines, and white papers published regarding the ethical use of AI. Under data privacy laws, AI is referred to as profiling or automated decision-making.

In the US, there is no federal law expressly governing the use of AI. The White House Office of Science and Technology Policy, however, recently released a "Blueprint for an AI Bill of Rights" to provide five guiding principles for the use of AI, which includes ensuring that AI:

- Is safe and effective;
- Does not discriminate;
- Avoids abusive data practices through built-in protections;
- Is transparent and explainable; and
- Is subject to a human alternative

Moreover, while there is no federal AI or privacy law, the US Federal Trade Commission (FTC) and other regulatory agencies may enforce the improper use of AI through existing laws, such as Section 5 of the Federal Trade Commission Act (FTC Act). In fact, at the 2023 IAPP Global Privacy Summit, FTC Commissioner Alvaro Bedoya stated that Section 5 of the FTC Act applies to AI:

The reality is AI is regulated (in the U.S.). Unfair and deceptive trade practices laws apply to AI,' Bedoya said. 'At the FTC, our core Section 5 authority extends to companies making, selling or using AI. If a company makes a deceptive claim using or about AI, that company can be held accountable.

On the state level, recently-passed comprehensive consumer privacy laws, such as the Colorado Privacy Act, Virginia Consumer Data Protection Act, and the Connecticut Data Privacy Act, regulate the use of AI by offering consumers the right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects on them. These privacy laws also require preparing data protection assessments to identify the risks affiliated with the use of AI and how those risks are mitigated.

In addition, the California Privacy Protection Agency is currently in the process of developing regulations under the California Privacy Rights Act regarding AI. US state laws also regulate certain types of AI, such as facial recognition and other technology that process biometric data. This includes the Illinois Biometric Information Privacy Act (BIPA), Texas Capture or Use of Biometric Identifier law, and Washington Biometric Privacy Law.

In the United Kingdom (UK) and European Union (EU), the UK GDPR—implemented through The Data Protection Act 2018—and the General Data Protection Regulation (GDPR) provide data subjects the right not to be subject to decisions based solely on automated decision-making that produce legal or similarly significant effects on them, unless certain exceptions apply, such as data subject consent or contract performance. The controller must also complete a data protection impact assessment when using automated decision-making tools. The UK and EU have also published a number of guidelines regarding the lawful use of AI and AI principles for the ethical use of AI, such as the UK Information Commissioner's Office's Guidance on AI and Data Protection and the European Commission's High-Level Expert Group on AI Ethics Guidelines.

To date, the UK and EU appear to take different approaches for regulating AI. The EU is working on a draft AI Act that will heavily control the use of AI and constitute the most comprehensive global AI regulation, while the UK recently published a white paper directing a pro-innovation stance for AI regulation, which is based on five principles: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

Lastly, other international privacy laws regulate AI, such as China's Personal Information Protection Law (PIPL) and Brazil's Lei Geral de Proteção de Dados (LGPD). For example, China's PIPL requires transparency, fairness, non-discrimination, and the right to refuse decisions based solely on automated decision-making. Brazil's LGPD provides data subjects the right to request review of decisions based solely on automated decision-making and receive clear and adequate information regarding the criteria and procedures used for the automated decision. Like the other privacy laws discussed above, PIPL and LGPD also require a privacy impact assessment when AI is used for automated decision-making. Globally there are also guidelines and frameworks regarding AI, such as the OECD AI Principles, and AI principles in Australia, Dubai, Singapore, and Hong Kong, to name a few.

A Harmonized Approach to AI

Based on a review of global AI laws, guidelines, and frameworks, an appropriate governance of AI requires implementing a six-phase solution.

- **Phase 1.** Companies providing AI need to implement leadership within the organization regarding the ethical and lawful use of AI. On the board level, directors need to know whether AI is developed and used in a trustworthy manner.

  Applying the mantra "nose in fingers out," the board needs to ask the right questions regarding AI and emerging technology, but it will be up to the C-suite to provide direction for an AI proposal, ensure that AI has human values, and direct AI to be used in a manner that is beneficial for human beings, society and the environment, while at the same time profitable for stockholders. C-suite needs to also direct the hiring of diverse and properly trained experts within the organization to develop the AI, such as researchers, data scientists and engineering teams.

- **Phase 2.** AI governance requires proper data collection and preparation, application and training of AI algorithms and models, and choosing an AI model that is repeatable, reproducible, reliable, and undergoes regular tuning. The organization needs to maintain a data provenance record that identifies the lineage of the data, such as where the data came from, how it was collected, curated and moved within the organization, and the steps taken to ensure the data is accurate over time.

- **Phase 3.** Organizations need to assess that their use of AI complies with existing laws, including data privacy and security laws and sector-specific regulations—e.g., finance, healthcare, employment, intellectual property, etc. The organization must then address any compliance gaps identified in the assessment.

- **Phase 4.** Organizations need to assess the risks affiliated with the use of AI and implement measures to mitigate the risks.

- **Phase 5.** Organizations can mitigate AI risks through several guiding principles, as developed through global guidelines and frameworks:

    - Avoid deceptive, manipulative, or malicious use of AI;

    - Minimize the processing of data in identifiable form through measures, such as pseudonymization and use of synthetic data;

    - Train employees regarding proper use of AI;

    - Test AI to ensure that it is fair, inclusive and does not discriminate against certain groups or harm the vulnerable—e.g., disabled, children, etc.;

    - Confirm that the AI is robust and secure;

    - Test the AI for accuracy;

    - Implement appropriate oversight of vendors that support the organization's use of AI through adequate contract terms and due diligence;

    - Develop mechanisms for honoring data subject rights under privacy laws;

    - Be transparent regarding your use of AI and explain how the AI works with sufficient detail;

    - Utilize privacy-by-design in your AI;

    - Evaluate the level of human involvement required for a given AI processing activity—human in the loop, out of loop or over loop—depending on the level of risk; and

    - Develop a mechanism for external stakeholders—e.g., consumers, regulators and the general public—to provide feedback and contest AI decisions;

- **Phase 6.** Organizations should document the above compliance steps through an auditable record to demonstrate accountability.

Board & C-Suite Perspective

While the above compliance steps may be delegated from top-to-bottom within an organization, the board and C-suite are ultimately accountable for the company's use of AI and its consequences. The board and C-suite perspective on AI governance was on full display during the inaugural Digital Trust Summit on March 31, 2023, where approximately 60 officers, directors, and other business leaders from across the country met to discuss proper AI governance within an organization.

The Digital Trust Summit was an invitation-only event hosted at the Watson Institute at Brown University and cosponsored by The Conference Board, NASDAQ, Bank of America, and Mayer Brown. During the summit, participants explored ways to enhance trust with emerging technologies, such as AI. The participants ultimately agreed that the topic of AI should be discussed in the boardroom, with directors asking the C-suite the right questions to ensure proper oversight.

Below are 10 insights from panelists at the conference regarding officer and director oversight of AI, as recently published by The Conference Board:

1. **Appreciate that trust with data is at the core of your business success.** As Bank of America CEO Brian Moynihan stated: "Financial services institutions are based on trust. We hold it. We help people engage with the economy. With that trust, we are able to provide great capability to our customers in the digital space."

2. **Prioritize technological understanding.** It is critical that the board has access to people, inside or outside the company, with the bandwidth and sophistication to advise on technological opportunities and risks. Understanding those threats that can introduce material business, operational and financial harm is a cornerstone towards informing risk mitigation strategies.

3. **Embrace technology responsibly and iteratively.** Listen to your customers, learn from experts, learn from the adaptation of technology advances over the past several decades, adapt for your needs, and reinvent as circumstances change. Test technological systems for security, accuracy and fairness before, during, and after deployment.

4. **Promote fairness within technological systems.** Have transparent discussions and relentlessly testing so that AI reflects our ideals, not our current imperfections.

5. **Diversify the talent that is building and adapting technological systems.** Ensuring these teams are not monolithic will have a huge, positive impact on fairness and equity.

6. **Establish trust principles and embed them throughout the organization.** These should touch on the four components of trust—empathy, transparency, capability, and reliability—and will ensure cohesion and consistency in a trust strategy.

7. **Scale the speed of trust.** Identify 'mavens' within the company, but not necessarily leadership, who can act as nexus points to scale trust both inside and outside the company. This will help trust move faster and permeate better.

8. **Leverage public-private partnerships.** Collaborate with government to combine private sector information and public sector authority to advance the interests of both, with regards to advanced technology adaptation and cyber security risk and resilience.

9. **Incorporate national security principles into enterprise risk assessment.** US companies are not seen as neutral parties by US adversaries, and will be targeted accordingly.

10. **Prepare for Grey Swans.** "Conduct scenario planning and crisis tabletop exercises to prepare for and anticipate responses to events that are unlikely, but that can range from moderately impactful to significant negative consequences," as NASDAQ's Global Head of Board Advisory Byron Loflin noted.

Conclusion

AI technology is developing at a faster pace than global AI laws, regulations, guidance, and frameworks. Until—and if—a consensus is reached regarding how AI should be regulated to safeguard data subjects and reduce risks, it will be incumbent for organizations to self-regulate themselves through appropriate internal governance, which begins at the board and C-suite level.

Through responsible internal governance, organizations can ensure the healthy development of AI in society for the betterment of humankind, advancement of society, and maximizing profits.