In-House

DEFENSE QUARTERLY

FALL 2024

dri™

For Today's Corporate Defense Practitioner

Including . . .

Contract Law Application to NIL Deals: Just Another Contract?

Also in this issue . . .

Charitable Giving Fraud and Other Online Dangers

A Comprehensive Analysis of AI Regulation, Compliance and Risk Mitigation

Integrating Artificial Intelligence (AI) into business operations presents significant advantages for companies, including increased revenue generation, efficiency, improved decision-making and enhanced data security. However, these benefits come with substantial risks that require careful attention and oversight, especially in companies without the resources of larger enterprises.

Understanding AI's potential and the associated legal challenges is crucial for company officers and in-house counsel. Corporate leaders must find a balance between an overreliance on AI use, potentially causing heightened liability exposure and underutilization of AI which may lead to being disadvantaged competitively. Additionally, businesses may struggle to establish this balance while navigating the complexities of complying with both current and future AI regulations.

This article provides an in-depth examination of AI, the hurdles businesses face during its implementation, regulatory environments in the United States and abroad, compliance strategies, risk mitigation and ethical considerations. By analyzing these facets, businesses can better navigate the complexities of AI adoption and harness its potential while addressing associated challenges.

What does your company need to know about AI?

To develop a comprehensive strategy to implement AI, businesses must understand the essence of the technology. Generative AI, or machine learning (ML), encompasses a broad range of technologies that process substantial data sets to perform tasks designed to generate new content such as text, images, videos or other data models. For example, ChatGPT is a large language model (LLM) that has gained popularity among AI programs capable of performing intellectual tasks normally assigned to humans. Businesses that implement AI systems into their operations enjoy a host of benefits, including:

- Enhanced market research data and predictive analytics;
- Increased operational efficiency for routine tasks and reduction in the likelihood of human error; and
- Heightened understanding of consumers' needs and preferences leading to better product and service development.
- Businesses that incorporate AI programs like ChatGPT into their operations may enjoy a competitive advantage, but those businesses are also exposed to regulatory hurdles and legal risks.

What basic challenges come with AI implementation?

Although the benefits of AI implementation are clear, and the potential for the technology seems uncapped, AI implementation also comes with many challenges. Businesses must be able to navigate these challenges to fully reap the benefits of AI and successfully maintain the incorporation of the technology in their long-term operations. Obstacles to AI implementation include:

Expertise is needed to understand the vast complexities of AI algorithm.

Because AI models use algorithms to perform their tasks, one of the fundamental challenges to AI implementation is understanding the complexities of its algorithms. Businesses that fail to obtain and retain qualified personnel who can understand and interpret AI algorithms will be plagued with issues such as dealing with discriminatory outputs resulting from biased algorithms and dealing with the consequences of an inability to make AI-related decisions within ethical bounds. To address this challenge, corporate officers must make tough decisions regarding the resources needed to research and develop efforts that enhance personnel knowledge of AI systems.

Significant resources are needed to safeguard data and maintain privacy.

Another challenge to AI implementation is the security of the personal data used to train and operate AI models. AI heavily relies on this information so companies must devote significant resources toward establishing comprehensive data protection programs and policies. At a minimum, an adequate data protection program should include secure data transfer and storage measures, encryption mechanisms and action items for compliance with data privacy regulations.

Richik Sarkar is a partner in the Cleveland, Ohio, office of Dinsmore & Shohl LLP – a longtime supporting of DRI. Richik is legal strategist who transforms complex business challenges into winning solutions. He is nationally recognized as a top lawyer, and he empowers companies and boards by providing clear, actionable insights on matters such as litigation, regulatory compliance, and ESG issues, including data privacy, business strategy, and governance. **Jarman Smith** is an associate in the Cleveland, Ohio, office of Dinsmore & Shohl LLP. Jarman focuses his practice on business transactions and intellectual property, including a focus on cybersecurity and data privacy law. In addition to his experience handling trademark, copyright and trade secrets law matters, his knowledge of consumer data protection regulations law allows him to deliver specialized guidance to business and organizations of all sizes.

Advanced technology comes with new technical difficulties to overcome.

Common technical challenges faced by businesses that implement AI into their operations involve security, storage and scalability. Issues in these areas arise because of the large volumes of data needed to run AI systems. Accordingly, implementing AI requires a heavy investment in infrastructure that can handle vast amounts of data. Attempting to use AI with weak computing systems may result in frequent technical issues.

There may be significant costs to implement AI.

Depending on the complexity of the AI system needed for your business, the costs to implement AI could be relatively high. For instance, developing a customized AI model will require more time and resources than simply integrating ChatGPT into your operations. Additionally, companies may face increased costs when integrating AI with legal systems. Initial investments in AI technology, including software, hardware and talent, can be a substantial barrier for many organizations. Companies may be able to cut costs by outsourcing AI development and implementation, but even outsourcing could result in hefty service and project fees. Thus, AI implementation is likely to come with a substantial monetary investment.

Businesses must understand the risks of AI use and plan accordingly.

While AI minimizes some risks, it also introduces new exposures because AI systems depend on the massive amounts of data that humans input. For example, a business training AI with sensitive personal information may face financial damage if the data is improperly used or disclosed.[1] Moreover, the effectiveness of

merger due diligence can be eviscerated if a company blindly uses AI that cannot filter out wrong information.[2] AI also introduces new public-facing service endpoints, creating more entrances for cyberattacks. Failing to take appropriate precautions against these attacks can lead to a breach of fiduciary duties and civil liability. Furthermore, faster data processing means a quicker rate of errors, more complex vulnerabilities and more potential legal violations. AI creates questions about legal exposure, risk management, adequate

> By analyzing these facets, businesses can better navigate the complexities of AI adoption and harness its potential while addressing associated challenges.

insurance coverage and the discharge of fiduciary duties.

AI systems can experience malfunctions and failures resulting from improper maintenance, design defects or human error. These defects can lead to financial loss, property damage or bodily injury.[3] For example, generative AI has a "well-documented tendency to provide plausible-sounding answers that are factually incorrect or so incomplete as to be misleading[.] AI might generate a description of a product with non-existent features or provide product instructions that are dangerous when implemented."[4] Such lies by omission may make companies liable for deceptive marketing or injuries caused by defects in the AI components of their products. Lastly, AI developers keep their algorithms under lock and key. This lack of transparency makes it hard to deter-

mine the cause of errors. Insureds, in turn, may not fully understand risks when purchasing AI products. Meanwhile, insurers cannot differentiate between covered unintended errors and intentional acts that would be excluded from coverage. Furthermore, this confusion hinders risk assessment and accurate pricing.

Navigating regulatory compliance is difficult as AI laws continue to develop.

The legal landscape concerning the development, use and governance of AI is constantly evolving as new regulations continue to be created and amended. This rapidly changing regulatory environment places immense pressure on businesses to understand the obligations and requirements that are associated with AI use. Any organization that utilizes AI without a proper understanding of existing and forthcoming regulations may be faced with penalties resulting from the misuse of AI.

How is AI use regulated?

The regulatory landscape of AI is rapidly changing, which can affect how businesses in all industries develop, implement and use this technology. Current trends in AI regulation focus on governance of AI use, notifying consumers that they are interacting with AI and protecting consumers from discriminatory AI outputs.

AI regulation has become a global trend.

As the technology continues to advance, jurisdictions all across the globe are scrambling to enact legislation and guidance to govern the use of AI. The European Union (EU) set the pace for regulatory AI governance by enacting the first comprehensive regulation on AI by a major regulator in the world.[5] The EU's AI Act is a landmark rule that aims to regulate how companies develop and use AI.[6] First proposed

1 The Mahoney Group, Navigating the Risks and Exposures of Artificial Intelligence: Essential Insurance Coverage for AI-Related Claims (May 8, 2023) (**https://www.mahoney-group.com/artificial-intelligence-insurance-claims/**).
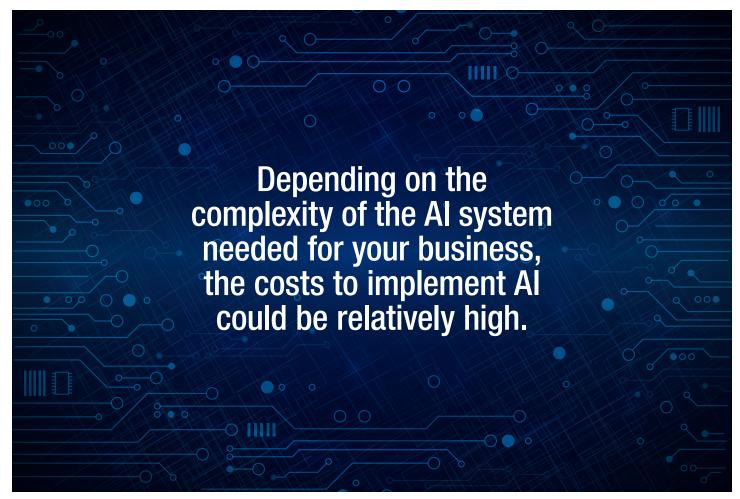
2 Thomas Belcastro, Getting on Board with Robots: How the Business Judgment Rule Should Apply to Artificial Intelligence Devices Serving as Members of a Corporate Board, 4 Geo. L. Tech. Rev. 263, 275-76 (2019).

3 The Mahoney Group, Navigating the Risks and Exposures of Artificial Intelligence: Essential Insurance Coverage for AI-Related Claims.

4 John Buchanan, Stuart Irvin & Megan Mumford Myers, Generative AI Loss Adds New Risk Area to Insurance Policies, Bloomberg Law (May 9, 2023).

5 **https://artificialintelligenceceact.eu/the-act/**

6 **https://www.cnbc.com/2024/08/01/eu-ai-act-goes-into-effect-heres-what-it-means-for-us-tech-firms.html**

Depending on the complexity of the AI system needed for your business, the costs to implement AI could be relatively high.

by the European Commission in 2020, the law became effective on August 1, 2024.[7] EU's AI Act addresses risks to consumers' health, safety and fundamental rights by providing AI developers and deployers with concrete requirements and obligations concerning specific uses of AI. Thus, the regulation establishes a comprehensive regulatory framework for AI across Europe. However, the scope of the EU's AI Act reaches beyond European borders and will impact many businesses across the globe, especially those with any operation or impact in the EU.[8] This means any business that uses AI to provide goods or services to EU residents will need to comply with the EU's AI Act and its regulatory requirements. Other countries, including the United States, have begun to follow the EU's lead by considering the adoption of comprehensive AI legislation and establishing regulatory frameworks.

The US has begun regulating AI use.
Although the US federal government has acknowledged the necessity to establish some form of regulatory framework to govern AI use by businesses,[9] the most likely outcome for the US is a bottom-up patchwork of state laws regulating AI use rather than a uniform federal standard. This approach is likely to disappoint proponents of a robust national standard, but some form of AI regulation in the US currently exists and more regulations will continue to be established. In the absence of a unified AI regulation, the US federal government has established guidelines and frameworks to govern the AI sector on a federal level. For instance, in October of 2023, the Biden administration issued an executive order (EO) on AI with aims to promote the safe, secure and trustworthy development and use of AI.[10] This EO has affected organizations across all sec-

7 https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en#:~:text=On%201%20August%202024%2C%20the,AI%20Act)%20enters%20into%20force

8 https://www.cnbc.com/2024/08/01/eu-ai-act-goes-into-effect-heres-what-it-means-for-us-tech-firms.html

9 https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trust-worthy-artificial-intelligence/#:~:text=Ensuring%20Responsible%20and%20Effective%20Government,the%20security%20of%20government%20systems.

10 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

tors of the economy as it directs executive departments and agencies to adhere to guiding principles and priorities when using and developing AI. Moreover, the National Institute of Standards and Technology (NIST) was mandated by the EO to establish guidelines and best practices for safe and secure AI use.[11]

The NIST has established guidelines for AI risk management.

Through the NIST AI Risk Management Framework, NIST has been a foundation in the development of guidelines to govern AI use in the US NIST's AI framework has substantial legal significance because it is one of the most frequently cited risk management frameworks in the US[12] The NIST AI Risk Management Framework (AI RMF) helps organizations identify and propose actions for AI risks by providing more than 200 actions across twelve different risk categories for managing AI risks.[13] Notable elements of the NIST AI RMF include:

- Trustworthiness: NIST's AI RMF draws on standards from the International Standard of Organization (ISO), including validity, reliability, resilience, security and fairness, to provide a means to assess whether an AI system is trustworthy.
- Monitoring: The AI RMF calls for continuous monitoring and testing of AI systems to ensure they function as designed and meet performance expectations. Organizations are also encouraged to regularly improve systems based on findings from monitoring.
- Controls, training and evidence: The AI RMF also contains its own set of controls, employee training information and suggested evidence to be collected.

- Ethical Uses: Lastly, the framework helps organizations ethically use AI while promoting accountability and transparency among developers and deployers.

Instead of waiting for the federal government to adopt a national standard for AI regulation in the US, states have been relying on guidance like the NIST AI RMF to develop and enact AI regulations on the state level across the country.

States have begun establishing a patchwork framework for AI regulation in the US

Utah was the first state to adopt an AI-centric law surrounding consumer protection in the US through the enactment of the Utah Artificial Intelligence Policy Act (UAIP) in March of 2024.[14] The UAIP imposes certain disclosure requirements on organizations that use AI to engage with consumers and limits their ability to avoid accountability for statements or acts made by AI that constitute consumer protection violations.[15] However, one of the most significant AI laws enacted in the US is the Colorado Artificial Intelligence Act, which is the first comprehensive law relating to the development and deployment of AI systems in the US[16] The Colorado AI Act focuses primarily on consumer protection and requires companies to use reasonable care to protect consumers from risks of AI discrimination.[17] Colorado's AI Act is similar to the EU's AI Act in that it has adopted a risk-based approach to AI regulation by imposing specific requirements on developers and deployers of AI systems concerning notice, documentation, disclosure and impact assessments. Both the Colorado AI Act and the EU AI Act emphasize regulating certain high-risk industries, including education, employment, finance or lend-

ing services, healthcare, housing, insurance and legal services.[18]

The Colorado AI Act (CAIA) was enacted in May of 2024 and aims to prevent algorithmic discrimination that results in differential treatment or impact that disfavors individuals based on age, color, disability, ethnicity, genetic information, language proficiency, national origin, race, religion, reproductive health, gender, veteran status or any other classification protected under state or federal law.[19] To fulfill its purpose, the CAIA sets forth several requirements and obligations, including:

AI developers make available documentation disclosing foreseeable inappropriate uses of the system, the type of data used to train the system and information concerning how the system will be governed to mitigate the effects of algorithmic discrimination;

- AI developers and deployers provide public disclosures of any high-risk AI systems they have developed and how they manage associated risks;
- AI developers disclose to the Colorado Attorney General and AI deployers any information learned from a credible source that their AI system has caused or is likely to cause discrimination;
- AI deployers notify consumers when AI will be used to make a consequential decision about the consumer;
- AI deployers disclose to consumers that they are interacting with an AI system; and
- AI deployers exercise a reasonable degree of care in implementing AI systems by having an updated risk management policy and program, and perform annual impact assessments.

Colorado's AI Act has fueled other states to propose similar legislation and will likely

---

11 **https://www.ey.com/en_us/insights/public-policy/key-takeaways-from-the-biden-administration-executive-order-on-ai**

12 **https://natlawreview.com/article/nist-updates-ai-rmf-mandated-white-house-executive-order-ai**

13 **https://www.techpolicy.press/unpacking-new-nist-guidance-on-artificial-intelligence/**

14 **https://le.utah.gov/~2024/bills/static/SB0149.html**

15 *Id.*

16 **https://leg.colorado.gov/bills/sb24-205**

17 **https://leg.colorado.gov/bills/sb24-205; https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf**

18 *Id.*

19 **https://kpmg.com/us/en/articles/2024/ai-regulation-colorado-artificial-intelligence-act-caia-reg-alert.html**

influence many states to contribute their own set of comprehensive AI regulations to the patchwork of state AI laws with which companies must comply absent any federal standard. Furthermore, this expected surge in AI regulation will expand beyond the US, as countries across the globe continue to propose and enact similar legislation. For instance, Canada has established the groundwork to develop a comprehensive regulatory framework for AI use through the introduction of its Artificial Intelligence and Data Act (AIDA) in June of 2022.[20] AIDA's stated purposes are to regulate cross-border trade in AI systems and to prohibit discriminatory conduct concerning AI systems.[21] Although this piece of legislation is still developing, and it is unclear

Colorado's AI Act has fueled other states to propose similar legislation and will likely influence many states to contribute their own set of comprehensive AI regulations to the patchwork of state AI laws with which companies must comply absent any federal standard.

when the AIDA will come into effect, it signals that AI legislation is a global priority that will be at the forefront of regulatory advancements for years to come.

How can your business become compliant, or prepare for compliance, with existing and forthcoming AI regulations?

AI is a tool that will revolutionize practices across multiple industries including healthcare, financial services, education and transportation. However, organizations that implement AI into their operations must take on the responsibility of adhering to existing and forthcoming AI regulations. AI regulatory compliance will mitigate potential risks and foster best practices in the implementation and deployment of AI systems. Thus, AI regulatory compliance should be a major priority for every organization that deploys the technology. To become compliant with AI regulations, your business should follow these guidelines:

Partner with qualified legal advisers with knowledge of AI and various regulations impacting the technology.

Obtaining legal counsel experienced in AI law will better position company leaders to understand the technology and make the decisions necessary to comply with applicable regulations. Legal AI advisers can assist with regularly monitoring AI regulations and keeping businesses informed on their obligations. With proper counsel, organizations that implement AI will be ahead of regulatory changes and able to maintain ongoing compliance. Moreover, legal counsel can review and provide guidance on the development of AI risk management programs and policies.

Understand how AI is used in your business.

Businesses need to understand how AI is used in their operations. This will allow such businesses to articulate their AI systems to third-party representatives assisting with regulatory compliance and obtaining AI-focused insurance coverage. Company employees should be trained in areas of AI development, deployment and management. By fostering a culture of awareness and responsibility, businesses will better position themselves to remain within the legal and ethical bounds of AI use.

Develop your AI systems around principles of transparency and fairness.

To better align with trends seen in AI regulation, corporate leaders should ensure that AI outputs are explainable to consumers and company stakeholders. Moreover, businesses should implement measures to identify and mitigate biases in AI algorithms by regularly assessing the fairness and security of AI systems.

Establish a written AI risk management program.

From existing AI use guidelines and regulations, such as NIST's AI RMF and the CAIA, it is clear that a common regulatory requirement will be for organizations to establish written policies regarding their use of AI systems. Every business that implements AI should create and enforce written policies that govern its AI use and outline how its practices adhere to AI regulations. A comprehensive AI governance policy or risk management program should at least incorporate the following principles: (i) a requirement for regular risk assessments for AI systems to identify potential vulnerabilities; (ii) development of mitigation strategies and implementation of controls to safeguard against identified risks; (iii) monitoring of AI systems continuously for emerging risks; and (iv) establishing incident response plans to handle AI-related failures and breaches effectively. Additionally, these programs and policies should clearly define roles and responsibilities for human oversight of AI use.

By following the guidelines presented above, your business will be able to become compliant with existing AI regulations and be better positioned for compliance with regulations to come. Being proactive with AI regulatory compliance will allow businesses to avoid the penalties and consequences that may ultimately follow the misuse of AI systems.

Why is compliance with AI regulations necessary?

As discussed, some major challenges to implementing AI involve dealing with potentially biased training data, avoiding AI outputs that result in discriminatory treatment or impact and mitigating the effects of such biases or algorithmic discrimination. Gearing toward compliance

---

20 **https://www.parl.ca/LegisInfo/en/bill/44-1/C-27**

21 *Id.*

with AI regulations will help businesses avoid using biased training data, prevent the use of discriminatory algorithms and establish clear procedures for addressing issues in the event biases or discriminatory effects are discovered. Additionally, demonstrating compliance with AI guidelines and regulations shows that your organization takes consumer protection seriously, which may positively impact the public's perception of your business operations. There is a push to further the movement of safe and responsible uses of AI and organizations that are proactive in complying with applicable guidelines and regulations will be ahead of the curve and seen as leaders in the realm of proper AI use.

In addition to promoting practices of sound consumer protection, companies that comply with AI guidelines and regulations are better placed to avoid penalties and consequences that follow noncompliance and unethical uses of AI. For instance, noncompliance with certain AI regulations provided for in the EU's AI Act could result in fines of up to 35 million euros or 7 percent of a company's annual turnover.[22] Under the CAIA, penalties for violations include the imposition of civil fines up to $20,000 per violation as assessed on a per-consumer or per-transaction basis.[23] Considering that violations of the CAIA are counted separately for each consumer or transaction, it would only take roughly fifty affected consumers or transactions to reach the maximum civil penalty of $1 million.[24] When considering a business' operations across the US, and the current trend for independent state-level regulations across the country, there is immense potential for penalties for noncompliance to add up quickly and cripple even some of the largest companies using AI.

Lastly, ensuring compliance with AI regulations could help companies avoid lawsuits that may result from AI systems

> **In addition to promoting practices of sound consumer protection, companies that comply with AI guidelines and regulations are better placed to avoid penalties and consequences that follow noncompliance and unethical uses of AI.**

that violate the fundamental rights of consumers. For example, the EU's AI Act provides consumers with private rights of action to submit complaints when harmed by AI.[25] Although the CAIA does not currently provide for private rights of action, this risk is not completely immaterial in the US because Colorado is free to amend the CAIA to allow for such. Other states may follow the EU's lead in allowing such lawsuits, and consumers may rely on other federal and state laws to develop lawsuits against companies that misuse AI.

In addition to regulatory compliance, how else can your business mitigate AI-related risks?

Many of the steps to mitigating AI-related risks overlap with the steps taken to comply with AI regulations and guidelines. However, there are some additional measures companies can take to ensure risks are mitigated across the board. Every organization that implements AI should consult with legal advisers with knowledge of AI who can provide recommendations regarding adequate AI insurance coverage and ethical uses of the technology.

Traditional insurance policies may not cover the risks introduced by AI, which

may result in substantial gaps in current coverage. For example, insurers may seek to exclude claims from coverage that arise from the use of unlawfully collected training data.[26] To improve their coverage posture, businesses need to obtain insurance policies that integrate principles of AI use to more accurately reflect business operations and account for unknown claims that may arise. Businesses should also consider specialized AI insurance policies that have been tailored to the unique risks posed by AI. These products have the potential to provide more comprehensive coverage than traditional insurance policies and could help cover claims relating to AI hallucinations, algorithmic bias, regulatory investigations, IP infringement and other consumer-driven lawsuits. When obtaining coverage for AI use, companies should:

- Evaluate and obtain AI-specific insurance coverage to address unique risks posed by AI;
- Consider specialized AI insurance products for comprehensive coverage;
- Regularly review and update insurance policies to reflect the evolving AI landscape; and
- Prepare for renewal discussions by articulating AI strategies, current uses and compliance statuses.

Obtaining adequate AI-related coverage comes with a host of complexities and potential roadblocks. Therefore, businesses need to discuss coverage issues with their team of trusted advisers before an AI risks develops into a potential insurance claims.

What are the best practices to ensure that your business implements AI systems that are ethical?

Any company that devotes significant time and resources toward considering ethical AI use practices will be more successful in establishing regulatory-compliant AI risk management programs and mitigating

---

22 https://artificialintelligenceact.eu/article/99/#:~:text=Non%2Dcompliance%20with%20certain%20AI,of%20a%20company's%20annual%20turnover

23 https://iapp.org/news/a/the-colorado-ai-act-what-you-need-to-know

24 *Id.*

25 https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/#:~:text=Most%20importantly%2C%20the%20AI%20Act,the%20appropriate%20market%20surveillance%20authority.

26 *See* Rachel Curry, *Companies want to spend more on AI to defeat hackers, but there's a catch* ("Policy around things like the use of generative AI can mitigate [the threat of uncovered intentional internal data misuses], but cyber blockades are also key").

AI risks. Perhaps one of the most important ethical considerations for businesses implementing AI revolves around preventing AI discrimination and data bias. Companies should avoid cutting corners when it comes to preventing these issues, which requires a consistent push to utilize resources to test and monitor their AI systems. In any event, ethical AI use will be based heavily on the principle of transparency. Companies that implement AI should be transparent about how their AI systems are trained, how these systems perform and complete tasks and any apparent issues with AI outputs that impact consumers. Another important ethical consideration is accountability. From an ethical standpoint, it is improper to completely disclaim all liability for AI outputs that negatively impact consumers. When implementing AI, businesses must be able to take responsibility for their technology and the results of using that technology. Additionally, businesses should consider how AI implementation will affect their employees. Workforce and job displacement may likely result from AI use. As new AI technologies lead to job losses in old industries, companies should find balance in retaining a human workforce by creating new jobs for employees to oversee AI operations.

Conclusion

AI technology is growing at an exponential rate as new tools, devices and algorithms are continually developed. While it is advantageous for businesses to acknowledge the benefits of this technological development and implement AI systems into their operations, they must also understand the complexities that come with AI implementation to mitigate associated risks and avoid negatively impacting consumers. Businesses in the process of implementing AI should consult with trusted legal advisers to address potential issues concerning AI risks, regulatory compliance, adequate insurance coverage and ethical considerations. A proactive, informed approach will enable organizations to leverage the transformative potential of AI responsibly and strategically in an evolving technological landscape.