



AMERICAN COLLEGE  
OF COVERAGE COUNSEL

## **What Could Possibly Wrong Go?: Generative AI, Liability, and Insurance**

### **American College of Coverage Counsel 2024 Annual Meeting**

Intercontinental Chicago  
May 8-10, 2024

**Jeff Bowen**

Lindemann Miller Bowen LLP  
Chicago, IL  
Jeff@lm-law.com

**Jean M. Lawler, CIPP/US**

Lawler ADR Services, LLC  
El Segundo, CA  
jlawler@lawleradr.com

**Carolyn H. Rosenberg**

Reed Smith LLP  
Chicago, IL  
CRosenberg@ReedSmith.com

**Seth A. Tucker**

Covington & Burling LLP  
Washington, DC  
stucker@cov.com

## Key Terms

### Artificial Intelligence, or AI

“[Artificial intelligence] is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.” (Source: John McCarthy, “What Is Artificial Intelligence”)

“Artificial intelligence (AI) is the intelligence of machines or software, as opposed to the intelligence of other living beings, primarily humans. It is a field of study in computer science that develops and studies intelligent machines. Such machines may be called AIs.” (Source: Wikipedia)

### Generative Artificial Intelligence, or Generative AI

“Generative AI refers to a class of artificial intelligence systems that have the capability to generate new content or data that is similar to, but not identical to, the input data they have been trained on. These systems use techniques such as neural networks, deep learning, and probabilistic models to generate outputs that mimic the patterns, characteristics, and structures present in the training data.

“Generative AI can be used in various applications, including:

1. **Image Generation:** Generating realistic images of objects, scenes, or people, even ones that don't exist in reality.
2. **Text Generation:** Creating human-like text, including articles, stories, poetry, and dialogue.
3. **Music Composition:** Generating new pieces of music or modifying existing ones to create variations.
4. **Video Synthesis:** Creating synthetic videos, altering existing videos, or generating video sequences based on input data.
5. **Content Creation:** Producing artwork, designs, and other creative content autonomously.

“Generative AI models are trained on large datasets and learn to capture the underlying patterns and relationships present in the data. They then use this learned knowledge to generate new samples that are similar to the training data but not exact replicas. Generative AI has seen significant advancements in recent years, leading to the creation of remarkably realistic and creative outputs across various domains.” (Source: ChatGPT)

“Generative AI refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.” (Source: IBM)

## Ask An Expert (I)

Q: [H]ow will generative AI change the field of insurance[?]

A: Generative AI is poised to bring transformative changes to the field of insurance across various dimensions. One of the key impacts is likely to be seen in underwriting processes. Generative AI can analyze vast datasets with incredible speed and precision, enabling insurers to assess risks more accurately. This technology can enhance predictive modeling, allowing insurers to refine risk assessments, set premiums more precisely, and improve overall underwriting efficiency.

Additionally, generative AI can revolutionize the claims processing system. By automating the claims assessment through image recognition, natural language processing, and pattern recognition, insurers can expedite the evaluation of claims, reduce fraud, and enhance the overall claims experience for customers. The technology's ability to process and analyze large volumes of data in real-time can lead to more dynamic and responsive pricing models.

Furthermore, generative AI can play a significant role in enhancing customer interactions. Chatbots powered by natural language processing can provide instant and personalized assistance to policyholders, addressing queries, and facilitating policy management. This can lead to improved customer satisfaction and streamlined communication processes.

However, the adoption of generative AI in the insurance industry also brings challenges, such as the need for robust cybersecurity measures to protect sensitive customer data and ensuring ethical use of AI algorithms. Overall, the integration of generative AI has the potential to make the insurance industry more efficient, customer-centric, and responsive to evolving risks.

(Source: ChatGPT, February 5, 2024)

## Ask An Expert (II)

Q: [H]ow will generative AI change the field of insurance[?]

A: Generative AI has the potential to revolutionize the field of insurance in several ways:

1. **Risk Assessment:** Generative AI can help insurance companies better assess risk by generating synthetic data that simulates a wide range of scenarios. This allows insurers to model potential outcomes more accurately and adjust their premiums accordingly.
2. **Fraud Detection:** By analyzing patterns in large datasets, generative AI can detect fraudulent claims more effectively. It can create synthetic data to simulate normal and abnormal claim patterns, making it easier to identify suspicious behavior.
3. **Customer Experience:** Generative AI can personalize the insurance experience by generating tailored policies and recommendations based on individual customer data. This can lead to more satisfied customers and increased customer retention.
4. **Underwriting:** Generative AI can automate the underwriting process by analyzing vast amounts of data to determine risk profiles and pricing. This can streamline the underwriting process, making it faster and more accurate.
5. **Predictive Modeling:** Generative AI can be used to create predictive models that anticipate future insurance claims based on historical data. This can help insurance companies better allocate resources and prepare for future risks.
6. **Product Development:** Generative AI can assist in the development of new insurance products by analyzing market trends and customer preferences. It can generate simulated data to test the viability of new products before they are launched.

Overall, generative AI has the potential to significantly improve efficiency, accuracy, and customer satisfaction in the insurance industry by leveraging advanced data analysis and predictive modeling techniques. However, it also raises concerns about privacy, security, and ethical use of data, which will need to be addressed as these technologies are implemented.

(Source: ChatGPT, February 7, 2024)

**THE STATE BAR OF CALIFORNIA  
STANDING COMMITTEE ON  
PROFESSIONAL RESPONSIBILITY AND CONDUCT**

**PRACTICAL GUIDANCE FOR THE USE OF  
GENERATIVE ARTIFICIAL INTELLIGENCE IN THE PRACTICE OF LAW**

**EXECUTIVE SUMMARY**

Generative AI is a tool that has wide-ranging application for the practice of law and administrative functions of the legal practice for all licensees, regardless of firm size, and all practice areas. Like any technology, generative AI must be used in a manner that conforms to a lawyer’s professional responsibility obligations, including those set forth in the Rules of Professional Conduct and the State Bar Act. A lawyer should understand the risks and benefits of the technology used in connection with providing legal services. How these obligations apply will depend on a host of factors, including the client, the matter, the practice area, the firm size, and the tools themselves, ranging from free and readily available to custom-built, proprietary formats.

Generative AI use presents unique challenges; it uses large volumes of data, there are many competing AI models and products, and, even for those who create generative AI products, there is a lack of clarity as to how it works. In addition, generative AI poses the risk of encouraging greater reliance and trust on its outputs because of its purpose to generate responses and its ability to do so in a manner that projects confidence and effectively emulates human responses. A lawyer should consider these and other risks before using generative AI in providing legal services.

The following Practical Guidance is based on current professional responsibility obligations for lawyers and demonstrates how to behave consistently with such obligations. While this guidance is intended to address issues and concerns with the use of generative AI and products that use generative AI as a component of a larger product, it may apply to other technologies, including more established applications of AI. This Practical Guidance should be read as guiding principles rather than as “best practices.”

## PRACTICAL GUIDANCE

Applicable Authorities	Practical Guidance
<p><b>Duty of Confidentiality</b></p> <p><a href="#">Bus. &amp; Prof. Code, § 6068, subd. (e)</a></p> <p><a href="#">Rule 1.6</a></p> <p><a href="#">Rule 1.8.2</a></p>	<p>Generative AI products are able to utilize the information that is input, including prompts and uploaded documents or resources, to train the AI, and might also share the query with third parties or use it for other purposes. Even if the product does not utilize or share inputted information, it may lack reasonable or adequate security.</p> <p>A lawyer must not input any confidential information of the client into any generative AI solution that lacks adequate confidentiality and security protections. A lawyer must anonymize client information and avoid entering details that can be used to identify the client.</p> <p>A lawyer or law firm should consult with IT professionals or cybersecurity experts to ensure that any AI system in which a lawyer would input confidential client information adheres to stringent security, confidentiality, and data retention protocols.</p> <p>A lawyer should review the Terms of Use or other information to determine how the product utilizes inputs. A lawyer who intends to use confidential information in a generative AI product should ensure that the provider does not share inputted information with third parties or utilize the information for its own use in any manner, including to train or improve its product.</p>
<p><b>Duties of Competence and Diligence</b></p> <p><a href="#">Rule 1.1</a></p> <p><a href="#">Rule 1.3</a></p>	<p>It is possible that generative AI outputs could include information that is false, inaccurate, or biased.</p> <p>A lawyer must ensure competent use of the technology, including the associated benefits and risks, and apply diligence and prudence with respect to facts and law.</p> <p>Before using generative AI, a lawyer should understand to a reasonable degree how the technology works, its limitations, and the applicable terms of use and other policies governing the use and exploitation of client data by the product.</p> <p>Overreliance on AI tools is inconsistent with the active practice of law and application of trained judgment by the lawyer.</p> <p>AI-generated outputs can be used as a starting point but must be carefully scrutinized. They should be critically analyzed for</p>

Applicable Authorities	Practical Guidance
	<p>accuracy and bias, supplemented, and improved, if necessary. A lawyer must critically review, validate, and correct both the input and the output of generative AI to ensure the content accurately reflects and supports the interests and priorities of the client in the matter at hand, including as part of advocacy for the client. The duty of competence requires more than the mere detection and elimination of false AI-generated results.</p> <p>A lawyer’s professional judgment cannot be delegated to generative AI and remains the lawyer’s responsibility at all times. A lawyer should take steps to avoid over-reliance on generative AI to such a degree that it hinders critical attorney analysis fostered by traditional research and writing. For example, a lawyer may supplement any AI-generated research with human-performed research and supplement any AI-generated argument with critical, human-performed analysis and review of authorities.</p>
<p><b>Duty to Comply with the Law</b></p> <p><a href="#">Bus. &amp; Prof. Code, § 6068(a)</a></p> <p><a href="#">Rule 8.4</a></p> <p><a href="#">Rule 1.2.1</a></p>	<p>A lawyer must comply with the law and cannot counsel a client to engage, or assist a client in conduct that the lawyer knows is a violation of any law, rule, or ruling of a tribunal when using generative AI tools.</p> <p>There are many relevant and applicable legal issues surrounding generative AI, including but not limited to compliance with AI-specific laws, privacy laws, cross-border data transfer laws, intellectual property laws, and cybersecurity concerns. A lawyer should analyze the relevant laws and regulations applicable to the attorney or the client.</p>
<p><b>Duty to Supervise Lawyers and Nonlawyers, Responsibilities of Subordinate Lawyers</b></p> <p><a href="#">Rule 5.1</a></p> <p><a href="#">Rule 5.2</a></p> <p><a href="#">Rule 5.3</a></p>	<p>Managerial and supervisory lawyers should establish clear policies regarding the permissible uses of generative AI and make reasonable efforts to ensure that the firm adopts measures that give reasonable assurance that the firm’s lawyers and non lawyers’ conduct complies with their professional obligations when using generative AI. This includes providing training on the ethical and practical aspects, and pitfalls, of any generative AI use.</p> <p>A subordinate lawyer must not use generative AI at the direction of a supervisory lawyer in a manner that violates the subordinate lawyer’s professional responsibility and obligations.</p>

Applicable Authorities	Practical Guidance
<p><b>Communication Regarding Generative AI Use</b></p> <p><a href="#">Rule 1.4</a></p> <p><a href="#">Rule 1.2</a></p>	<p>A lawyer should evaluate their communication obligations throughout the representation based on the facts and circumstances, including the novelty of the technology, risks associated with generative AI use, scope of the representation, and sophistication of the client.</p> <p>The lawyer should consider disclosure to their client that they intend to use generative AI in the representation, including how the technology will be used, and the benefits and risks of such use.</p> <p>A lawyer should review any applicable client instructions or guidelines that may restrict or limit the use of generative AI.</p>
<p><b>Charging for Work Produced by Generative AI and Generative AI Costs</b></p> <p><a href="#">Rule 1.5</a></p> <p>Bus. &amp; Prof. Code, §§ <a href="#">6147</a>–<a href="#">6148</a></p>	<p>A lawyer may use generative AI to more efficiently create work product and may charge for actual time spent (e.g., crafting or refining generative AI inputs and prompts, or reviewing and editing generative AI outputs). A lawyer must not charge hourly fees for the time saved by using generative AI.</p> <p>Costs associated with generative AI may be charged to the clients in compliance with applicable law.</p> <p>A fee agreement should explain the basis for all fees and costs, including those associated with the use of generative AI.</p>
<p><b>Candor to the Tribunal; and Meritorious Claims and Contentions</b></p> <p><a href="#">Rule 3.1</a></p> <p><a href="#">Rule 3.3</a></p>	<p>A lawyer must review all generative AI outputs, including, but not limited to, analysis and citations to authority for accuracy before submission to the court, and correct any errors or misleading statements made to the court.</p> <p>A lawyer should also check for any rules, orders, or other requirements in the relevant jurisdiction that may necessitate the disclosure of the use of generative AI.</p>
<p><b>Prohibition on Discrimination, Harassment, and Retaliation</b></p> <p><a href="#">Rule 8.4.1</a></p>	<p>Some generative AI is trained on biased information, and a lawyer should be aware of possible biases and the risks they may create when using generative AI (e.g., to screen potential clients or employees).</p> <p>Lawyers should engage in continuous learning about AI biases and their implications in legal practice, and firms should establish policies and mechanisms to identify, report, and address potential AI biases.</p>



Applicable Authorities	Practical Guidance
<b>Professional Responsibilities Owed to Other Jurisdictions</b> <a href="#">Rule 8.5</a>	A lawyer should analyze the relevant laws and regulations of each jurisdiction in which a lawyer is licensed to ensure compliance with such rules.

## AI Comes to the Board Room in a Black Box: Are the Personal Assets of Directors at Risk in AI-Related Claims?

By Stuart Irvin, Seth Tucker, David Engvall & David Dapaah-Afriyie – Edited by Edwin Farley

Cite as: Stuart Irvin, Seth Tucker, David Engvall & David Dapaah-Afriyie, *AI Comes to the Board Room in a Black Box: Are the Personal Assets of Directors at Risk in AI-Related Claims?*, JOLT DIG. (Sept. 15, 2023), <https://jolt.law.harvard.edu/digest/ai-comes-to-the-board-room-in-a-black-box>.

---

### Introduction

Artificial intelligence and machine learning (“AIML”) technologies are transforming data-intensive industries, like healthcare and finance, at an astonishing speed. AIML tools can enhance decision-making processes at the enterprise level by analyzing financial data, operational data, customer data, and data collected in research and development activities.

The AIML tools and technologies that are beginning to come to market for enterprise customers can help management and boards to make more informed decisions based on real-time (or near real-time) insights. Business risks can be identified and mitigated, and business opportunities can be spotted and seized.

All new technologies, particularly when implemented at the enterprise level, carry a risk of loss for the business that implements them. Depending on the technology, the risks may include physical harm to the business’s customers or even third parties, or they may be limited to financial losses incurred by the company. What happens when, for example, a pharmaceutical product that is developed using AIML tools results in poor health outcomes or patient deaths? What is the civil liability of the directors of a company if their AI-developed drug turns out to be the next thalidomide, or the outputs of AIML tools prompt the directors to pursue a business strategy that fails spectacularly? If history is any guide, the directors who rely on AIML tools could well face derivative actions brought by shareholders on behalf of the corporation alleging a breach of their duties to the corporation.

A focus of discovery in any future derivative action in this vein will likely encounter elements of the so-called “black box” problem. AIML technology, particularly in the context of deep learning models like neural networks, can develop so rapidly, and at such a level of complexity, that the internal workings of the AI model can no longer be understood by a corporation’s management or even by the engineers who developed the model.<sup>1</sup> If the developers don’t understand how an

---

<sup>1</sup> Yavar Bathaee, [The Artificial Intelligence Black Box and the Failure of Intent and Causation](#), 31 HARV. J.L. & TECH. 889 (2018); Cynthia Rudin & Joanna Radin, [Why Are We Using Black Box](#) (continued...)

AI tool is making decisions, it can be extremely difficult to correct errors or modify the tool to ensure its safe and ethical performance. At some level, the functioning of AIML technologies could, quite literally, be beyond human understanding.

To return to the “new thalidomide” hypothetical, would the directors of a pharmaceutical company have *personal* liability if the plaintiff in a derivative action can show that management and the board of the corporation knew, or should have known, that the drug development process was effectively a black box? In the business strategy hypothetical, would the directors face liability if their pursuit of a business strategy devised by a black box AI tool resulted in a plunge in the value of the shares of the company or even its bankruptcy? There certainly could be meritorious defenses to such claims, but the defense costs could be substantial and a judgment could be ruinous for a director who is named as a defendant in a personal capacity in the case.

### **Protecting Personal Assets**

The personal assets of the directors who serve a corporation are typically protected by (1) indemnification commitments by the company and (2) Directors & Officers (“D&O”) liability insurance. These protections will remain critical for individuals who serve as directors of corporations, including corporations that rely increasingly on AIML tools.

In this Commentary, we suggest updates to the standard indemnification terms used in contracts with directors and in corporate bylaw provisions. We also discuss best practices for ensuring that D&O policies continue to protect individual board members against the emerging risks that may follow from the widening use of AIML.

### **Information Systems and Red Flags**

The use of AIML technology by a corporation to make decisions could expose the corporation’s directors to two types of breach-of-fiduciary-duty claims. Directors serving on the boards of Delaware corporations owe fiduciary duties of care and loyalty, which include a duty of oversight. In the seminal *Caremark* decision,<sup>2</sup> the Delaware Supreme Court explained that the fiduciary duties of a director include a duty to make a good-faith effort to ensure that “information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation’s compliance with law and its business performance.”<sup>3</sup>

The Court also addressed when directors could be held liable for failing to implement a reporting system to facilitate board oversight. The Court noted that:<sup>4</sup>

only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability.

---

[Models in AI When We Don’t Need To? A Lesson From an Explainable AI Competition](#), HARV. DATA SCI. REV. (2019).

<sup>2</sup> [In re Caremark Int’l Inc. Derivative Litig.](#), 698 A.2d 959 (Del. Ch. 1996).

<sup>3</sup> *Id.* at 970.

<sup>4</sup> *Id.* at 971.

Such a test of liability—lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight—is quite high.

In *Stone v. Ritter*,<sup>5</sup> the Delaware Supreme Court ruled that to survive a motion to dismiss a failure-of-oversight claim, a plaintiff must allege particularized facts supporting a reasonable inference that either “(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.”<sup>6</sup> A recent decision of the Delaware Court of Chancery has classified these two types of claims as, respectively, “Information-Systems Claims” and “Red-Flags Claims.”<sup>7</sup>

The use of an AIML tool that functions as a black box for mission-critical decision-making tests the boundaries of both an Information Systems Claim and, as the risks associated with AI become better known to the public, a Red-Flags Claim. It is entirely possible that AIML tools could evolve to the point where the workings of a model, and its decisions that a corporation implements, can no longer be understood by a corporation’s management or its board. On the basis of these facts, a court could conclude that the corporation has utterly failed to implement information and reporting systems that provide the board with timely, accurate information sufficient to allow the board to reach informed judgments concerning the corporation’s compliance with law and its business performance. If whistleblowers, governance experts, or others publicize the risks to a corporation associated with these AIML tools, a Red-Flags Claim becomes more likely.<sup>8</sup>

---

<sup>5</sup> [Stone v. Ritter](#), 911 A.2d 362 (Del. 2006).

<sup>6</sup> *Id.* at 370.

<sup>7</sup> [In re McDonald’s Corp. Stockholder Derivative Litig.](#), No.2021-0324, 2023 WL 387292, at \*21–22 (Del. Ch. Jan. 26, 2023).

<sup>8</sup> As public understanding of a particular risk to companies increases, the potential for related red-flags claims increases—especially when the harm at issue falls directly within the ambit of a director or officer’s responsibilities. *In re McDonald’s Corp.* is illustrative of this dynamic. The case concerned a corporate officer responsible for ensuring workplace safety whom stockholder-plaintiffs alleged had consciously ignored red flags about sexual harassment and misconduct affecting company employees throughout his tenure with the corporation, which ended with the officer’s termination for sexual harassment in 2019. *Id.* at \*2-5. In denying a motion to dismiss the stockholder-plaintiffs’ red-flags claim, the Court highlighted widespread internal and external scrutiny of the corporation in connection with numerous allegations of sexual harassment, noting that this scrutiny contributed to a reasonable inference that the corporation had red flags for sexual harassment and misconduct of which the corporate officer was aware. *Id.* at \*55-57. The increased public understanding of sexual harassment and the ability of directors and officers of a corporation to address and deter workplace sexual harassment factored into both the stockholder-plaintiff’s complaint and the Court’s decision. This greater public understanding, which in part enabled the red-flags claim in *In re McDonald’s Corp.*, is a relatively recent development, however, as the term “sexual harassment” was not coined until 1975 and did not enter the public consciousness until later. Sascha Cohen, [A Brief History of Sexual Harassment in America Before Anita Hill](#), TIME (April 11, 2016). Moreover, it was only in 1986 that the Supreme Court ruled for the first time that a claim of “hostile environment” sexual harassment is a form of sex discrimination that is actionable under Title VII of the Civil Rights Act of 1964 (in [Meritor Savings Bank, FSB v. Vinson](#), 477 U.S. 57, 63-69 (1986)). The history of red-flags claims related to sexual harassment suggests that as public understanding of the risk that uninformed reliance upon AIML (continued...)

Delaware law presumes that directors act in good faith, and to be viable a complaint must plead facts sufficient to support an inference of bad faith.<sup>9</sup> Establishing a breach of a duty of oversight “requires pleading and later proving disloyal conduct that takes the form of bad faith.”<sup>10</sup> This is a high burden, but not an insurmountable one on the right facts.<sup>11</sup> And for directors, the prospect of personal liability means that even a small risk of a potentially catastrophic loss is highly problematic. It is for this reason that Delaware corporations typically indemnify their board members for the risks associated with derivative actions alleging a breach of fiduciary duties owed by directors to the corporation and purchase D&O insurance.

## Indemnification for AI-Related Losses

Indemnification undertakings can be in the form of individual indemnification agreements or indemnification provisions contained in the bylaws or other charter documents of the corporation. Indemnification obligations also can be created by a vote of the board of a corporation or its shareholders.

These indemnification obligations are substantively quite similar, regardless of the form used to implement them, at least for companies chartered in Delaware. The corporation typically agrees to indemnify the director (called an “Indemnitee” in most provisions) if “the Indemnitee acted in good faith and in a manner that the Indemnitee reasonably believed to be in or not opposed to the best interests of the Company.”<sup>12</sup> Some, but not all, indemnification provisions go further and define the concept of “good faith” in detail. A typical provision states:<sup>13</sup>

Indemnitee shall be deemed to have acted in good faith if [Indemnitee’s] action is based on the records or books of account of the [Company], including financial statements, or on information supplied to Indemnitee by the officers of the [Company] in the course of their duties, or on the advice of legal counsel for the [Company] or on information or records given or reports made to the [Company] by an independent certified public accountant or by an appraiser or other expert selected with reasonable care by the [Company]...In addition, the knowledge and/or actions, or failure to act, of any director, officer, agent or employee of the

---

tools by directors poses to companies increases, the potential for related red-flags claims will increase.

<sup>9</sup> *Id.* at 3.

<sup>10</sup> *Id.* at 2–3.

<sup>11</sup> For example, in *Marchand v. Barnhill*, reversing the Delaware Court of Chancery’s dismissal, the Delaware Supreme Court permitted a failure-of-oversight claim to proceed against Blue Bell Creameries USA, Inc. and its directors. [Marchand v. Barnhill](#), 212 A.3d 805 (Del. 2019). In permitting the claim, the Court held that the stockholder-plaintiff alleged sufficient facts to support a fair inference that the defendants failed to make a good-faith effort to establish a reasonable board-level monitoring-and-reporting system to ensure the exercise of due care with respect to an “essential and mission critical” compliance risk of the company: food safety. *Id.* at 824. In the absence of such a good-faith effort, the defendants would have breached of their duty of oversight. The Delaware courts never made a decision on the merits of the alleged breach, however, as the parties [reached a \\$60 million settlement](#) in July 2020 before trial.

<sup>12</sup> For a good example of an Indemnification Agreement, see the agreement filed by Gain Therapeutics, Inc. at the SEC, <https://perma.cc/NZ5C-GU5C>.

<sup>13</sup> *Id.* § 6(e).

[Company] shall not be imputed to Indemnitee for purposes of determining the right to indemnification under this Agreement.

The question for directors is whether this indemnification language, which is intended to be very broad and to approach the limits of what is permissible for public policy reasons, is nevertheless sufficiently broad to cover decisions made by the corporation using AIML technologies, especially in circumstances where a black box problem is known or suspected.

An answer to this question would typically involve research under Delaware law and the careful crafting of arguments based on precedent that has absolutely nothing to do with AIML. While the common law can and does adapt to new and unanticipated circumstances, it also rarely provides clear “yes” or “no” answers, especially on issues of first impression. In addition, litigating a case to conclusion is expensive, and whatever is ultimately decided by a trial court will, for a time, be vulnerable to revision, correction, or reversal by subsequent courts looking at similar facts—a process that can extend for years.

Given the uncertainty inherent in the common-law process and the delay in getting guidance from the courts on issues involving a fast-moving technology, corporations may seek to avoid the problem entirely and expressly provide for good-faith reliance on AI-related decision-making. The exact standard to be used in indemnification provisions could be debated at length by corporate governance wonks and care has to be taken to stay within the bounds of what is permissible under state law<sup>14</sup> and public policy. But the process has to start somewhere, and to get that process started the authors offer the following addition to standard indemnification language and trust to the wisdom of the crowd to refine and improve upon it:

Indemnitee shall be deemed to have acted in good faith if [Indemnitee's] action is based on the records or books of account of the [Company], including financial statements, or on information supplied to Indemnitee by the officers of the [Company] in the course of their duties **(including information that was created, in whole or in part, using deep learning, machine learning, or other artificial intelligence technologies)**....

The added text above is not intended to absolve a director from the duty of oversight. It merely seeks to confirm that a director can, in appropriate circumstances, rely in good faith on information created using AIML tools. The inclusion of language of this kind would help to counter the argument that reliance on information that was created using AIML technology is, in itself and without a further showing of dereliction, a breach of a director's duty to the corporation.

## **Ensuring D&O Insurance**

Indemnification will usually be the first resort when a director is sued for an alleged breach of duty to the corporation. Indeed, D&O insurance often requires the corporation to indemnify directors against derivative claims to the extent permissible by law.

But if the corporation is unwilling or unable to indemnify its directors — as it might be if it were in financial distress — the individuals will look to the company's D&O insurance to cover their defense costs and any settlement or judgment.

---

<sup>14</sup> [8 Del. C. § 145](#).

At present, there is no standard, widely used exclusion that would bar coverage for a director accused in a derivative action of breach of a duty owed to the corporation arising from the corporation's reliance on AIML tools or the board's reliance on AIML outputs. The fact that the insurance industry has not developed AI exclusions is probably due to one or both of two reasons. First, the insurers that sell D&O policies understand that providing broad protection and keeping exclusions to a small number makes their product attractive, and that they will be at a disadvantage in the market if they lard their policies with exclusions. Second, AI and commercially available AI tools have burst into the public consciousness fairly recently, and the risks of AI implementation by corporations are only beginning to be understood. Insurers may not have yet had time to fully consider whether they wish to protect themselves by either excluding AI risk altogether or putting in place a lower limit (a "sublimit") for claims that arise out of an insured's use of AI.<sup>15</sup>

Finally, D&O policies typically have an exclusion for acts (and sometimes omissions) by a director that were deliberately fraudulent or deliberately criminal.<sup>16</sup> The safest way for directors to distance themselves from such an exclusion may well be to disclose to the public that a corporation is using AIML tools to automate certain business processes and that the members of the board are using AIML outputs to assist with decision-making. Such a disclosure could reduce the risk of a claim that a board member had acted "fraudulently" by accepting remuneration for board service but had outsourced all the work of being a board member to an AI tool. A disclosure of this sort might not prevent a breach-of-fiduciary-duty claim from being asserted, but it should mitigate the risk of the D&O insurer being able to avoid responsibility for the claim by invoking the exclusion for deliberately fraudulent conduct.

---

<sup>15</sup> Some insurance companies are moving faster to address AI-related risk of loss than others. Munich Re has advertised a policy called "[aiSure™](#)" that promises an "insurance-backed performance guarantee" for AI providers that "can increase your clients' trust in your AI solution." This is not a D&O policy, but as described it could provide insurance at a key link in the AI value chain, and the fact that Munich Re has brought it to market suggests that the industry could move quickly to implement new forms of coverage if there is a demand in the market for that coverage.

<sup>16</sup> Often, such exclusions apply only if a tribunal has determined in a non-appealable adjudication that the director engaged in deliberate fraud or criminal activity, or if the director has admitted such misconduct.



# Let's "chat" about A.I. and insurance

By Carolyn H. Rosenberg, Esq., and David M. Cummings, Esq., Reed Smith LLP

OCTOBER 24, 2023

The widespread consideration of artificial intelligence technologies ("A.I.") across platforms and industries is not surprising. Among other operational advantages, A.I. is touted as creating efficiencies and reducing costs, and on a global scale, accelerating progress on key issues such as health, security and sustainability. See K. Basu, "Immigration Lawyers Look to AI to Make Rote Work Faster, Cheaper," Bloomberg Law (Sep. 28, 2023); J. Peltz, "Top UN tech policy official feels 'optimistic about AI,'" Chicago Tribune (Sep. 27, 2023).

Although A.I. may hold great promise, businesses are exploring how to work with such technologies in a manner that avoids or limits exposure, including measures to create appropriate guardrails for employee use, adequately protect content and data, manage vendors, and navigate privacy issues and existing and anticipated regulations.

It is critical that companies evaluate and consider their insurance coverage programs when planning for, and responding to, these and other A.I. risks, including employment practices liability, cyber, directors and officer liability, media liability, professional liability/errors and omissions, property and business interruption, and general liability insurance, to name only a few.

## A.I. and a changing risk landscape

Despite that incorporation of A.I. into business operations is still in its relative infancy, some risks are beginning to materialize. For example, at least one Equal Employment Opportunity Commission (EEOC) claim has been filed, *EEOC v. iTutor Group, Inc., et al.*, No. 1:22-cv-02565 (E.D.N.Y. 2022).

In that case, the EEOC alleged that the defendant company, which provides English-language tutoring services, used an A.I. tool to automatically reject older applicants because of their age. Although this matter settled out of court — Press Release, "iTutorGroup to Pay \$365,000 to Settle EEOC Discriminatory Hiring Suit," EEOC (Sep. 11, 2023) — similar employment-related disputes are anticipated.

Emerging risks are not limited to the employment arena. As A.I. is increasingly leveraged across business units, companies must navigate new or increased exposures related to these spheres.

Companies may face exposures, for example, related to data privacy and cybersecurity claims where A.I. is used to enhance these threats. See C. Stupp, "AI Spurs New Cybersecurity Threats," Wall St. J. (Oct. 6, 2023). Businesses may conceivably face A.I.

exposure for "climate impact" claims. See N. Dolby, "Artificial Intelligence Can Make Companies Greener, but It Also Guzzles Energy," Wall St. J. (Sep. 12, 2023).

In addition, many companies are already dealing with exposure related to violations of intellectual property laws. For example, there have been numerous copyright infringement lawsuits filed against A.I. companies that use internet "scraping" functions to aggregate data and generate "unique" content and training, alleging that copyrighted materials are used without appropriate author permissions. See B. Brittain, "More writers sue OpenAI for copyright infringement over AI training," Reuters (Sep. 11, 2023).

---

*As A.I. is increasingly leveraged across business units, companies must navigate new or increased exposures related to these spheres.*

---

Moreover, company boards and leadership might face claims for breaches of their fiduciary obligations related to, for example, inadequate financial reporting where A.I. assists with such function, or more broadly the implementation of A.I. policies and safeguards. Companies also run the risk of professional liability exposure to the extent A.I. technologies are alleged to adversely impact professional services, including in the medical and financial management industries.

## Insurance considerations for A.I. risks

The rise in A.I. technologies across industries and functions should lead companies to question what protections might exist for related exposures. Beyond the implementation of A.I. usage and compliance policies and robust training, and the drafting of strong indemnification provisions in contracts with these technologies in mind, insurance is a key risk management tool.

For risk assessment purposes, insurers should not treat claims that involve A.I. any differently than claims that do not include such a component. If the claim at issue is a third-party lawsuit, for example, with allegations that otherwise trigger one or more coverages within the company's insurance program, that claim should still be covered absent an applicable exclusion.



As indicated, A.I.-related claims can take many forms, including, for example, alleged violations of employment law, breaches of data privacy statutes, breaches of fiduciary duties or professional obligations, violations of securities laws, intellectual property infringement, or any other number of events, acts or omissions. As such, companies should continue to first look to their insurance policies that would otherwise respond to such claims — employment practices liability, cyber, directors and officers liability, media liability, professional liability/errors and omissions, property and business interruption, and general liability insurance, to name but a few.

In addition to the foregoing “traditional” insurance products, the insurance industry is expected to respond in a more dedicated way to some of the specialized risks faced by companies innovating in the A.I. space. In fact, certain insurers are already beginning to market bespoke insurance advertised to cover the heightened financial risks associated with the development and sale of new A.I. models. See B. Lin, “Is your AI model going off the rails? There may be an insurance policy for that,” Zywave (Oct. 2, 2023).

To date, exclusions specific to A.I. have not yet been identified in the insurance market. Nonetheless, in the event such exclusions or other coverage limitations begin to appear during placements and renewals — for example, exclusions for claims, losses, or damages that “arise out of” or are “related to” A.I. — such changes should be vigorously resisted by insureds. Moreover, where policy definitions can be augmented to clearly cover A.I., care should be taken to negotiate for those enhancements.

In addition, policyholders should be vigilant in completing insurance applications. Cyber insurance applications, for example, are notoriously complex and lengthy, and often presuppose a robust understanding of how a company’s technology systems operate. Although insurers have not begun routinely asking non-A.I.

companies about A.I. usage during the underwriting process, as the A.I. landscape continues to grow, this might change.

Relatedly, just as insureds must manage their own risks with respect to A.I., they should be watchful where insurers may be employing A.I. to assist with their underwriting and claims handling functions. If insurers lean too heavily on A.I. to aggregate data and/or make underwriting or claims handling determinations without critical and thoughtful human involvement, insureds may bear the brunt of poor A.I. policy. This may run afoul of insureds’ entitlement to good faith, thoughtful consideration of their submissions whether in obtaining insurance or processing claims.

More broadly, A.I. represents a new era of risk that insurers are learning to manage and underwrite appropriately. Similar to the sudden onset of cyber-attacks that shifted the cyber insurance industry, a learning curve is inevitable and might lead to variable and uncertain underwriting, pricing, and offerings over the coming years. See Cyber Insurance Academy, “Surge in AI Ushers A ‘New Silent Cyber’” *Risk* (Oct. 3, 2023). Insureds should stay closely involved in placements and negotiations to flag material changes, and engage with insurers and brokers accordingly.

## Conclusion

The current risk landscape with respect to A.I. is fluid and uncertain, holding not only immense promise but also hidden pitfalls. Insurance is designed to protect against such risks and provide assurances for businesses and their c-suites.

It is important that insureds remain involved and engaged as A.I. continues to grow so that these protections remain available and affordable. Knowledgeable coverage counsel can assist. With adequate protections in place, innovation can continue to flourish.

*The information and statements in this article are provided for informational purposes only, and should not be construed as legal advice on any subject matter.*

## About the authors



**Carolyn H. Rosenberg** (L) is a partner in **Reed Smith’s** insurance recovery group and a member of the firm’s A.I. and ESG task forces. She advises corporations, directors and officers, risk managers and other professionals when obtaining or renewing insurance policies, addressing corporate indemnification and enterprise risk management, and resolving coverage disputes. She can be reached at [croseberg@reedsmith.com](mailto:croseberg@reedsmith.com). **David M. Cummings** (R) is a partner in the firm’s insurance recovery group. His practice focuses on advocating for corporate policyholders seeking counsel with respect to insurance placements and renewals, as well as during disputed claims, litigation, mediation and arbitration. He writes and speaks regularly on emerging risks and insurance issues, including with respect to A.I., ESG, and cyber. He can be reached at [dcummings@reedsmith.com](mailto:dcummings@reedsmith.com).

This article was first published on Reuters Legal News and Westlaw Today on October 24, 2023.