MEALEY'S®
Emerging Insurance Disputes

AI Risk: New Tech, Same Coverage

By
Michael S. Levine,
Washington, DC

Alex D. Pappas
Washington, DC

and

Torrye N. Zullo
New York, NY

Hunton Andrews Kurth LLP

A commentary reprinted from the March 6, 2025 issue of Mealey's Emerging Insurance Disputes

Commentary

AI Risk: New Tech, Same Coverage

By
Michael S. Levine,
Alex D. Pappas
and
Torrye N. Zullo

[Editor's Note: Michael S. Levine is a partner with Hunton Andrews Kurth LLP in the firm's Washington, DC, office. Alex D. Pappas and Torrye N. Zullo are associates with Hunton Andrews Kurth LLP. Any commentary or opinions do not reflect the opinions of Hunton Andrews Kurth LLP or LexisNexis® Mealey Publications™.

As AI continues to permeate the business landscape, the likelihood of loss and damage tied to the use of AI will continue to increase. As with other business risks and causes of loss, businesses will look to insurance to mitigate the financial consequences. The question becomes, therefore, *which* line or lines of insurance should respond? In this article, we explore the new risks posed by the use of AI and how those risks align with traditional or so-called "legacy" lines of coverage.

Not surprisingly, traditional coverages were not designed with AI-specific risks in mind. However, commonality of risks, regardless of the specific cause, allows clear application of legacy coverage lines to what might appear as new AI-related risks. We use several case studies to illustrate this commonality, including cases involving bodily injury and property damage, securities law violations, employment law risks and cyber breaches. We also highlight potential coverage gaps that can arise from the introduction of AI-specific coverages. While these insurance products are in their infancy, the potential coverage gaps underscore the importance of developing comprehensive AI risk management strategies premised on a sound knowledge of how the insured company is using AI and relying on the use of AI by others.

I. AI and Legacy Insurance Products: A Brief Tale of Four Insurance Products

1. Commercial General Liability (CGL) Insurance

CGL policies, designed to cover damages because of bodily injury or property damage, should apply equally to claims arising from the use of AI technologies where the tech causes bodily injury or property damage. This assumes, of course, that the insurer has not added an AI-specific exclusion that would exclude AI as a *cause* of loss. Point being, AI is just another cause of loss, damage, or injury. Where the loss, damage, or injury is of the type insured, and the cause of that loss is not specifically excluded, the resulting claim should be covered.

For example, in *A.F. et al. v. Character Technologies, Inc. et al.,* No. 2:24-cv-01014 (E.D. Tex.) (Dec. 9, 2024), the plaintiffs allege that Character Technologies' AI product poses various risks to American youth, including enhancing the risk of suicide, self-mutilation, sexual solicitation, isolation, depression, anxiety and harm toward others. The complaint further alleges that the AI's design and data promote violent and sensational responses by youth.

From the perspective of a lawsuit against a product manufacturer whose product allegedly injured someone, *Character Technologies* is unremarkable. What makes it remarkable, though, is that the product is AI. But as we look beyond the shiny new tech and focus on the basis for the claim against the insured, it becomes clear that this is really no different than any other allegedly defective product case. The lawsuit thus shows how traditional liability insurance can serve as an important first line of defense when AI-related risks materialize into legal actions. For instance, primary and excess CGL policies typically cover the cost of defending and settling lawsuits premised on bodily injury, as in *Character Technologies*.

2. Directors & Officers (D&O) Liability Insurance

Traditional D&O insurance likewise should extend coverage to claims premised on AI, just the same as they would for claims involving alleged wrongful acts based on other causes of loss. In fact, from what has already been seen in claims predicated on corporate disclosures and other similar corporate wrongful acts involving AI, traditional D&O policies are particularly well-suited to respond to AI-related claims.

For example, in *Sarria v. Telus International (Cda) Inc. et al.*, No. 1:25-cv-00889 (S.D.N.Y.) (Jan. 30, 2025), a class action was brought against Telus International (CDA) Inc., a Canadian company, along with its former and current corporate leaders. The lawsuit claims that Telus failed to inform stakeholders that its AI offerings required the cannibalization of higher-margin products, that profitability declines could result from its AI development and that the shift toward AI could exert greater pressure on company margins than had been disclosed. When these risks became reality, Telus' stock plummeted and the lawsuit followed. According to the complaint, the omissions allegedly constitute violations of Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 and Rule 10b-5.

Telus illustrates how D&O insurance can serve as an important line of defense when AI-related risks materialize into legal actions. For instance, depending on policy language, D&O insurance policies might cover securities lawsuits just like *Telus*.

3. Employment Practices Liability (EPL) Insurance

EPL insurance protects businesses from claims related to employment practices. This type of insurance may be used to cover AI-related risks, particularly when AI systems may inadvertently result in discrimination, harassment or other violations of employee rights.

For example, in *Mobley v. Workday*, No. 3:23-cv-00770 (N.D. Cal.) (Feb. 21, 2023), the plaintiff sued Workday Inc., alleging that Workday's AI-powered hiring software engaged in discriminatory practices. Plaintiff alleges that Workday uses machine-learning algorithms and artificial-intelligence tools to screen out applicants who are African-American, disabled or over the age of 40. The lawsuit further alleges that Workday should have known about and prevented the discrimination.

Mobley highlights the potential importance of EPL coverage in protecting companies from legal and financial risks associated with AI-driven employment practices. In a world where AI systems can perpetuate bias, EPL coverage can provide essential coverage for businesses facing lawsuits that challenge their employment practices.

4. Cyber Insurance

Cyber insurance can also be a critical safeguard for businesses, offering essential protection against the potentially devastating financial impact of data breaches and cyberattacks. With the growing reliance on AI systems, this coverage becomes even more vital, as it may extend to risks associated with AI technologies. When AI systems handle sensitive data, any security lapse can make businesses vulnerable to targeted cyberattacks, leading to significant data breaches.

For example, in 2022, T-Mobile experienced a large-scale data breach. In this data breach, a cybercriminal apparently exploited AI-enhanced Application Programming Interface (API) tools to access sensitive customer information. On January 19, 2023, T-Mobile issued a press release informing its customers that an attacker had used a single API, a form of artificial intelligence, to infiltrate their accounts.

This breach underscores why having cyber liability insurance is essential and how a cyber policy can come into play with AI-related risks too. A cyber policy may offer vital coverage in the event of an AI-related data breach, helping businesses mitigate both the immediate costs and long-term consequences of cyberattacks.

5. Intellectual Property (IP) Insurance

IP insurance can help mitigate the financial impact of AI-generated IP risks. It can cover legal costs associated with defending against claims of infringement, as well as indemnity for damages awarded in such cases. This type of insurance can help organizations protect their assets and maintain financial stability while addressing potential IP disputes. Furthermore, IP insurance can offer resources for risk assessment and management, helping companies proactively identify and address vulnerabilities in their AI systems. By transferring some of the financial risks associated with IP litigation to an insurer, organizations can focus on innovation and growth.

AI-generated IP risks are increasingly becoming a concern as artificial intelligence systems create content. These systems can inadvertently infringe on existing patents, copyrights, or trademarks leading to potential legal disputes.

As AI technology progresses, organizations must navigate the increasingly complex and shifting landscape of IP, making it essential to understand and manage the associated risks. An example of this is the case *Andersen v. Stability AI Ltd.*, No. 3:23-cv-00201 (N.D. Cal.) (Oct. 30, 2023), where the plaintiffs allege that the defendants' use of copyrighted works to train AI models infringes on the artists' copyrights. The plaintiffs claim that the AI models generate new works that closely resemble the artists' original copyrighted images, without authorization or compensation.

To that end, AI-generated outputs may not clearly attribute authorship, complicating ownership rights and potentially leading to disputes over IP rights. With AI models trained on vast datasets, there is also the risk of AI inadvertently mimicking protected works, which can result in infringement claims like the claims in *Andersen.*

In the broader context of a risk management program, IP insurance can be an essential tool for protecting an organization's intangible assets. It complements other risk management strategies by offering specialized coverage for legal risks associated with IP, which can be particularly complex and costly. By integrating IP insurance into a comprehensive risk management framework, businesses can better safeguard their innovations and competitive advantage.

II. Are Legacy Insurance Products Enough? What the Future Could Bring for AI-Related Insurance Coverage

As described above, legacy insurance products should cover AI-related risks. From our teachings with the evolution of cyber-specific coverages, some may soon label coverage under traditional or "legacy" coverages as "silent coverage." But is it really so mysterious, or is it that AI is just another of the many things that can give rise to the same old risks of liability that companies face every day? Regardless, as insurers introduce new lines of AI-specific coverage, and new AI exclusions and limitations options for traditional lines of coverage, it is invariable that gaps in protection will emerge, leaving the unwary financially exposed. And as with the coverage lines discussed previously, policyholders may wish to consider relevant exclusions and gain a deep understanding of whether and how their insurance policies address AI. Some of these exclusions include the following:

Artificial Intelligence Exclusions. Some insurers, like Hamilton Select Insurance and Philadelphia Indemnity Company, have already rolled out AI-specific exclusions that potentially bar coverage for AI-related losses or stand to create or widen coverage gaps. An artificial intelligence exclusion may broadly provide that the policy will not cover any claims arising out of, or in any way involving any actual or alleged use of artificial intelligence. Some may be specific to use by only the insured, others may try to reach more broadly. In this way, the policy's definitions are just as important as the coverage and exclusionary provision, maybe more so. And in almost all instances, the definition of "artificial intelligence" itself may help determine whether the exclusion applies. For instance, given the robust breadth of AI, and the many factors that help determine whether tech is "AI," or simply really good computing, and the various types of AI (machine learning, generative AI, etc.), all become relevant when trying to define what actually is within or outside the scope of the broad term "artificial intelligence."

Expected or Intended Exclusions. An **expected or intended exclusion** is a clause in an insurance policy that can preclude coverage for damages or losses that were anticipated or intentionally caused by the insured, typically excluding situations where harm was foreseeable. This exclusion may be relevant if a company is sued for a decision made by an AI system that the company expected to occur based on prior modeling, training or testing, or where the insured reasonably should have foreseen when implementing the AI system.

Cyber Exclusions. Policies might also contain broad "cyber" exclusions. A cyber exclusion is a provision in an insurance policy that specifically limits or denies coverage for losses or damages arising from cyber-related incidents, such as data breaches, hacking or cyberattacks, often including risks associated with digital technologies that could be confused with AI. In addition, these exclusions may be interpreted expansively, potentially applying to any AI-related allegations—whether or not the connection to the wrongdoing is direct. This could include scenarios where AI tools or algorithms contributed to a data breach, discrimination claim or product malfunction, even if the AI was only indirectly involved.

In sum, by carefully considering how insurance policies treat claims involving AI technologies, businesses can better protect themselves from unexpected gaps in coverage that could leave them exposed to significant financial losses or legal battles. This proactive approach is especially crucial as AI technologies continue to evolve rapidly and become integrated into business operations, as traditional insurance policies may not fully account for the nuances of AI risks. Understanding these exclusions and limitations in advance helps ensure that businesses are adequately covered, reducing the risk of financial instability in the face of emerging AI-related challenges.

III. Conclusion: Practice Pointers for Policyholders in the AI Era

As AI becomes increasingly integrated into the way companies conduct routine business operations, companies need to proactively consider how AI is being used in their specific operations and then assess their full insurance portfolio to ensure a seamless continuity of coverage. By staying informed and proactive, businesses can navigate the evolving landscape of AI risks and insurance, ensuring their continued success in an increasingly AI-driven world. AI has, and will continue to, influence the insurance market, creating both opportunities and risks for policyholders.

Below, we offer a suggested approach for assessing and mitigating AI risk:

1. **Audit Business-Specific AI Risk**: AI risks are inherently unique to each business, heavily influenced by how AI is integrated into various aspects of the company and the jurisdictions in which a company operates. Companies will want to conduct thorough audits to identify these risks, especially as they navigate an increasingly complex regulatory landscape shaped by a patchwork of state and federal policies.

2. **Involve Relevant Stakeholders**: Unlike more fundamentally obvious risks like property, equipment and even management-level liabilities, AI requires a clear and real-time understanding of how the entire company is using AI. That use will differ significantly from one business unit to the next. For example, the way a company procures materials will differ from the way it uses AI to enhance manufacturing or service efficiencies, which will differ from the way it uses AI to control sales, distribution and logistics, which will differ from how it assesses financial activity, or the way it monitors its facilities. It cannot be reasonably expected that any one person can be knowledgeable across all of these facets of operation. Effective risk assessments should therefore involve all relevant stakeholders, including various business units, third-party vendors and AI providers. This comprehensive approach ensures that all facets of a company's AI risk profile are thoroughly evaluated and addressed.

3. **Consider AI Training and Educational Initiatives**: Given the rapidly developing nature of AI and its corresponding risks, businesses may wish to consider education and training initiatives for employees, officers and board members alike. After all, developing effective strategies for mitigating AI risks can turn in the first instance on a familiarity with AI technologies themselves and the risks they pose.

4. **Evaluate Insurance Needs Holistically**: Following business-specific AI audits, companies may wish to meticulously review their insurance programs to identify potential coverage gaps that could lead to uninsured liabilities.

5. **Consider AI-Specific Policy Language**: As insurers adapt to the evolving AI landscape, companies should be vigilant about reviewing their policies

for AI exclusions and limitations. When traditional insurance products fall short, businesses might consider AI-specific policies or endorsements, such as Munich Re's aiSure™, to facilitate comprehensive coverage that aligns with their specific risk profiles.

6. **Consider Alternative Risk Transfer for AI Risk**: Insurance is only one way to transfer AI risk. Others include the use of strategic indemnification provisions in service and vendor agreements, and the insistence on being named as an additional insured under policies held by business partners, vendors and suppliers. These types of alternative risk transfer, when coupled with a comprehensive insurance portfolio, offer the most comprehensive protection against AI and other types of risk.

By adopting these practices, businesses can better navigate the complexities of AI-related risks and insurance coverage, safeguarding their operations and ensuring resilience in an AI-driven future. ■

MEALEY'S EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

LexisNexis®

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: lexisnexis.com/mealeys
ISSN 1087-139X