Bloomberg Law

Generative AI Loss Adds New Risk Area to Insurance Policies

May 9, 2023

Covington attorneys analyze emerging risks that generative AI tools pose to business insurance policies, and new policies on the market that might provide specific coverage for AI claims.

Business use of generative AI tools is in its early stages. Accenture advises that "companies will need to radically rethink how work gets done" following enterprise adoption of generative AI technology. Part of that rethinking will inevitably involve risk management.

All software products and services, when implemented at the enterprise level, carry risks of loss associated with their use. What unique attributes of AI tools might give rise to loss for their business users? Here are a few hypothetical examples.

AI "hallucination." Generative AI tools have a well-documented tendency to provide plausible-sounding answers that are factually incorrect or so incomplete as to be misleading. For example, AI might generate a description of a product with non-existent features or provide product instructions that are dangerous when implemented.

Infringing AI training data. AI models can be trained using data from the internet and other unlicensed sources, including social media platforms. For example, copyright litigation over the use of training data has already begun, with Getty Images suing Stability AI for allegedly using over 12 million of its images to train its AI model to create images from text.

Sabotage by AI-displaced employees. Economists at Goldman Sachs recently warned that AI technology could replace 300 million jobs. Highly skilled employees faced with job loss from AI may try to sabotage the AI technology or the business that has adopted it, potentially causing a wide range of losses to the employer and to third parties.

Pick Your Policy

A variety of existing commercial insurance policies may respond to losses arising from business use of generative AI. Different lines of insurance may overlap in their coverage, but policyholders should also consider potential gaps, as well as policy language formulated for older risks that could be ambiguous

when applied to AI. Careful scrutiny of policy language, with the company's specific AI risk profile in mind, is increasingly necessary to prevent coverage disputes after a loss.

Cyber policies. A natural first place for a business to look for AI-related coverage will be its cyber policies. Cyber policies vary greatly, but they typically cover risks ranging from first-party digital asset loss to third-party liability for data breaches. This coverage could become particularly important if a generative AI-powered system is hacked and data systems are compromised.

A business may also reasonably expect its cyber policy to cover the AI-specific risks outlined above, but insurers may deploy exclusions or other gaps in their policy wording to dispute such claims. For example, liability for use of infringing training data would not fit neatly into the Insurance Services Office's basic cyber form's coverages for security breaches, extortion threats, or restoration of electronic data. In contrast, many specialized cyber policies extend coverage to "media acts," including unauthorized use of copyright, trade dress, or trademarks.

Property policies. Many property policies, because they cover "all risks" of physical damage to property except those expressly excluded, may "silently" cover damage from AI-related causes. Insurance brokers have noted that AI uniquely blends tangible and intangible asset values and perils. Intangible AI can cause indisputably tangible harm to owned property—for example, in the dangerous instructions hypothetical above, incorrect AI-generated instructions could damage company machinery.

Property policies may also be a particularly valuable source of business interruption coverage, if a qualifying event such as a hacked AI model or a damaged server hosting the AI service disrupts the company's operations.

Technology errors and omissions policies. These policies may respond to claims for copyright violations, as well as AI-generated erroneous advice. For example, Philadelphia Insurance offers a media liability endorsement to its Tech E&O form that covers a "media wrongful incident," defined to include a range of conduct, including trademark/copyright infringement and plagiarism.

But again, traps may lurk for the unwary. The same tech coverage form excludes copyright infringement claims "arising from software or computer hardware," likely contemplating infringement in "traditional" software's fixed code rather than a dynamic algorithm. It also excludes any "intentionally false, misleading or fraudulent statement you make about your products or services."

Insurers may point to allegations that the coding or lack of disclaimers for incomplete responses establishes intent to mislead, and that such "intentional" AI acts are excluded. Policyholders would counter that claims arising from AI losses are traditional products claims—based on strict liability—and therefore intent is not relevant.

Crime policies. A disgruntled employee whose job is made redundant by AI might seek revenge on an employer by sabotaging computer systems or diverting automated payments. Among other lines of coverage, crime policies and so-called fidelity bonds or employee dishonesty policies might respond to such conduct.

Although these novel risks have parallels to more traditional risks, it could be harder, and costlier, to prove criminal or dishonest human conduct involving AI. Commercial policyholders should consider

supplemental coverage for specialized claims expenses, similar to coverage for security breach forensics commonly found in cyber policies.

New Risks, Policies, or Exclusions

Some insurers view the risks associated with an emerging technology as an opportunity to devise new policy wording and earn additional premiums. At least one insurer has already begun to offer an AI specialty policy: Munich Re's advertisements for its "aiSure" policy promise that if an AI "solution does not perform as promised, we will step in and help you to compensate your clients."

The flip side of this phenomenon is exemplified by "silent cyber" initiatives: concerned that unanticipated, and unpriced, risks may fall within the broad coverage grants of traditional policies, insurers may introduce new exclusions. Some of these exclusions may be poorly drafted, creating costly coverage disputes if traditionally insured losses—such as traditional bodily injury or property damage—happen to have an arguable nexus to an AI algorithm's operation.

As a business deploys more generative AI tools, coverage renewals in all lines of insurance will require more careful attention to wording details, so that its insurance programs all mesh to cover its unique AI risks.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

John Buchanan is senior counsel with Covington and focuses on insurance coverage litigation, including major cyber and tech-related losses.

Stuart Irvin is of counsel with Covington, advising clients on technology transactions, including AI licensing and joint venture matters.

Megan Mumford Myers is an associate with Covington and represents corporate policyholders in complex, high-stakes insurance coverage disputes and litigation.