AMERICAN COLLEGE OF COVERAGE COUNSEL

UNIVERSITY OF MINNESOTA
Driven to Discover®

AI Risk Management:
Gee, What Could Possibly Go Wrong?
. . . Uh, Is That Covered?

American College of Coverage Counsel
2024 Insurance Law Symposium
University of Minnesota Law School
Minneapolis, MN
November 15, 2024

Session Panelists

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

Evans Mburu
Medtronic
Minneapolis, MN
Evans.Mburu@medtronic.com

Jascha Prosiegel
Munich Reinsurance Company
San Francisco, CA
jprosiegel@munichre.com

John Buchanan (Moderator)
Covington & Burling LLP
Washington, DC
jbuchanan@cov.com

US Law Week
May 9, 2023, 4:00 AM

Generative AI Loss Adds New Risk Area to Insurance Policies

By John Buchanan, Stuart Irvin, and Megan Mumford Myers

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.

Write for Us: Author Guidelines

LAW360®

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Insurance Policies Can Cover Generative AI Risks

By **Josianne El Antoury** (October 4, 2023, 12:14 PM BST)

Josianne El Antoury

The pace of artificial intelligence technology integration into U.K. businesses is rapidly increasing and providing unquestionable efficiency benefits to businesses.

In 2022, more than 3,000 AI companies were working in the U.K., which generated more than £10 billion ($12 billion) in AI-related revenue.[1]

On June 7, 2023, Prime Minister Rishi Sunak announced that the U.K. will host the first major global summit on AI safety — a step toward making the U.K. a "world leader for AI innovation" — and one of its focuses is mitigating AI risks.[2]

At the same time as embracing AI, U.K. authorities have warned of its potential risks, such as AI-facilitated hacking and intellectual property infringement.

This article summarizes some of the U.K.'s concerns as they relate to generative AI, a new category of AI tools, and some potential insurance coverage solutions for those risks.

The takeaways are that policyholders' existing insurance policies, such as cyber, property, professional liability — particularly technology errors and omissions, and directors and officers insurance — and crime are likely to provide coverage for these new risks.

AI risks might not fit neatly into the language of these policies, and insurers may argue that exclusions or gaps in policy wordings apply.

However, after careful analysis of their existing coverages and unique AI-related risks, policyholders should consider any gray areas, including exploring new AI-focused specialty insurance products.

Generative AI Risks

On June 14, Lindy Cameron, CEO of the U.K. National Cyber Security Centre, highlighted the NCSC's commitment to "realize the benefits provided by AI." However, the NCSC warned of risks around the security of AI, such as the increasing risk of novel forms of AI-facilitated hacking.

For example, generative AI, such as large language models, or LLMs, might be used to write more "convincing spear-phishing emails" to help penetrate a company's cybersecurity defenses and promulgate mass hacking campaigns.[3] This can also lead to business data being compromised.

Other risks identified by the NCSC include businesses' IP being at risk if their staff submit confidential information into LLM prompts. IP risks around ambiguity over who owns the content created by generative AI may result in claims of IP infringement.

The U.K. government has highlighted that increasingly sophisticated AI could displace workers, which in turn can lead to disgruntled employees sabotaging AI technology — a 21st-century version of the Luddite attacks on job-displacing textile machinery at the start of the industrial revolution.

A U.K. government report in May suggests that AI could replace around 7% of jobs, particularly low-paid jobs, during the five-year period of 2021-2026, rising to around 18% after 10 years, and to just under 30% after 20 years.[4]

The malfunction of innovative generative AI tools used by professionals, such as law firms, may also result in professional negligence claims, physical loss or damage to property, or personal injury to consumers.

Traditional Business Insurance Coverage for Generative AI Risks

What existing insurance coverage is available for the new risks that may arise from generative AI?

Some examples of likely responsive insurance policies are considered below.

Cyber Policies

Cyber risk or technology errors and omissions policies may be the best fit for AI risks if an AI system is hacked or its data is compromised.

There is no "one size fits all" cyber policy, but generally, it can cover certain first-party losses to the insured business. This includes business interruption due to digital asset loss following a cyber incident and the costs for breach response experts such as IT forensics and external legal counsel.

Such policies can also cover third-party liability for data breaches.

As previously reported, cyberinsurance premiums have risen exponentially, due predominantly to the increase in ransomware attacks. As a result, some companies have been priced out of purchasing cover.[5] This trend continues, even though it may be starting to level out at current high premium rates.

For example, in the legal sector, the Law Society of England and Wales confirmed in July that only seven in 10 law firms had cyberinsurance.[6]

In 2021, the Solicitors Regulatory Authority, the regulatory body of law firms in England and Wales, excluded cyber-related first-party loss from the minimum standard terms for professional indemnity cover, which may result in a potential gap in coverage for AI risks.

For businesses that have cyberinsurance coverage, AI risks may not fit neatly into the language of those policies, and insurers may argue that exclusions or gaps in policy wordings apply.

Insurers may dispute coverage under some cyber policy wordings for brand damage caused by an AI-based antivirus tool that has been tricked by threat actors into thinking a specific type of ransomware is benign.

Property Policies

Physical loss or damage caused by AI risks would likely be covered by traditional property policies.

Property policies are generally underwritten on an "all risks" basis, covering all loss or damage except what is expressly excluded. Such policies also provide a "time element" or business interruption and extra expense cover in response to physical damage that may be caused by AI.

However, property insurers, among others, have taken steps to introduce exclusions aimed at so-called silent cyber exposures and may assert that those exclusions apply to AI-related risks.[7]

Policyholders should check their cover for such exclusions and evaluate them carefully in light of the particular AI-related functions and applications they deploy.

Professional Liability Policies

Claims for breach of IP rights and AI-generated advice might be covered by liability policies, including professional indemnity, such as those covering lawyers, media liability, and technology error and omission.[8]

Directors and officers policies also might be triggered where a claim has been made against a director or officer — in some cases an entity — for AI-related loss.

Some English law-governed policies with a liability trigger may require the insured to prove that it would have been legally liable to the third party in order to recover for settlement of a claim.

This may create difficulties for policyholders where it is unclear whether they would have been legally liable, particularly in light of the uncertainty around the application of existing regulations over AI and the difficulty of proving evidentiary issues, such as causation for the underlying claimant.

Crime Policies

The sabotage of AI technology, including by disgruntled employees, and related financial losses could be covered under crime policies, also known as fidelity coverage.

Generally, a key requirement of these policies is to prove a criminal or dishonest act, which could be challenging where, for example, an AI system itself has been subtly manipulated to become the direct perpetrator of the sabotage, or where the complexity of the AI system otherwise impedes identifying a human perpetrator.

New Insurance Products for Generative AI Risks

The insurance industry is aware of the potential for inadequate protection under existing insurance products for the full range of novel risks posed by AI,[9] and some insurers have already started promoting new AI-specific insurance products.

While it is still unclear how broadly such products have actually been implemented in the marketplace, some AI-specific products currently promoted include American International Group Inc.'s robotics shield,[10] and Munich Re's aiSure, which is aimed at vendors of AI solutions,[11] and aiSelf, which is aimed at companies developing their own AI.[12]

Other insurers have promoted enhancements via endorsements for existing policies that might otherwise exclude silent cyber. This includes Marsh McLennan's cyber catalyst forms, including its "Silent Cyber Bridge" extension[13], and Lockton's "Silent Cyber Property Solution for Businesses."[14]

Before considering purchasing AI-specific insurance policies such as these, policyholders should evaluate their current policies to understand the amount and scope of coverage currently available, including any applicable exclusions, as applied to the generative AI risks presented by their operations.

After careful analysis of their existing coverages and their unique AI-related risks, policyholders should consider any gray areas. This should be done well before renewal, leaving adequate time to develop a thoughtful strategy to negotiate clarified wording for their existing lines of coverage, explore new AI-focused specialty insurance products or both.

Josianne El Antoury is special counsel at Covington & Burling LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] "Artificial intelligence sector study 2022" published by the Office for Artificial Intelligence and the Department for Science, Innovation and Technology, dated March 29, 2023, https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2022/artificial-intelligence-sector-study-2022-ministerial-foreword-and-executive-summary.

[2] UK to host first global summit on Artificial Intelligence - GOV.UK (www.gov.uk). Press Release by the UK Government, dated June 7, 2023, https://www.gov.uk/government/news/uk-to-host-first-global-summit-on-artificial-intelligence.

[3] Lindy Cameron at Cyber 2023, Chatham House - NCSC.GOV.UK, dated June 14, 2023, https://www.ncsc.gov.uk/speech/lindy-cameron-cyber-2023-chatham-house.

[4] Report commissioned by the UK Government from consultancy firm PWC in 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1023590/impact-of-ai-on-jobs.pdf. See also the World Economic Forum's Report: "These are the jobs most likely to be lost – and created – because of AI", dated May 4, 2023, which also expects that many clerical or secretarial roles are likely to decline quickly because of AI. https://www.weforum.org/agenda/2023/05/jobs-lost-created-ai-gpt/.

[5] Law360 "How The Rise In Ransomware Is Affecting Business Insurance" April 25, 2022, https://www.law360.co.uk/articles/1485332/how-the-rise-in-ransomware-is-affecting-business-insurance.

[6] Solicitors Journal, "Law Society: 7 in 10 firms lack cyber insurance" July 21, 2023, https://www.solicitorsjournal.com/sjarticle/law-society-7-in-10-firms-lack-cyber-insurance.

[7] Covington Alert: "The Noise About "Silent Cyber" Insurance Coverage," https://www.cov.com/-/media/files/corporate/publications/2020/01/the-noise-about-silent-cyber-insurance-coverage.pdf.

[8] For example, Lloyd's launched a Technology E&O Policy for the tech sector in 2014, which provides cover for technology companies for losses caused by the failure of the policyholder's technology products or services sold to third parties. (Lloyd's launches new E&O facility for the tech sector, June 10, 2014, https://www.lloyds.com/news-and-insights/news/lloyds-launches-new-eo-facility-for-tech-sector).

[9] R. S. S. Kumar & F. Nagle, "The Case for AI Insurance," Harvard Business Review (April 29, 2020), https://hbr.org/2020/04/the-case-for-ai-insurance.

[10] AIG Robotics Shield, "End-to-End Management for the Booming Robotics Industry," https://www.aig.com/content/dam/aig/america-canada/us/documents/business/professional-liability/aig-robotics-shield-hs.pdf.

[11] Munich Re, aiSure, "Insure the performance of your Artificial Intelligence Solutions," https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/MRE_aiSure_Infographic.pdf/_jcr_content/renditions/original./MRE_aiSure_Infographic.pdf.

[12] Munich Re, aiSelf, "Insure the performance of your Artificial Intelligence Solutions," https://www.munichre.com/en/solutions/for-industry-clients/insure-ai/ai-self.html.

[13] Marsh Cyber Catalyst, https://www.marsh.com/us/services/cyber-risk/products/cyber-catalyst.html.

[14] "Lockton Launches Silent Cyber Property Solution for Businesses", Insurance Journal (October 20, 2021), https://www.insurancejournal.com/news/international/2021/10/20/638002.htm.

JOLT DIGEST

HARVARD JOURNAL OF LAW & TECHNOLOGY

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.[1] If the developers don't understand how an

[1] 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,[2] 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."[3]

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:[4]

> 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).

[2] *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

[3] *Id*. at 970.

[4] *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*,[5] 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."[6] 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."[7]

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.[8]

[5] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).

[6] *Id*. at 370.

[7] *In re McDonald's Corp. Stockholder Derivative Litig.*, No.2021-0324, 2023 WL 387292, at *21–22 (Del. Ch. Jan. 26, 2023).

[8] 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.[9] Establishing a breach of a duty of oversight "requires pleading and later proving disloyal conduct that takes the form of bad faith."[10] This is a high burden, but not an insurmountable one on the right facts.[11] 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."[12] Some, but not all, indemnification provisions go further and define the concept of "good faith" in detail. A typical provision states:[13]

> 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.

[9] *Id*. at 3.

[10] *Id*. at 2–3.

[11] 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.

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

[13] *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[14] 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.

[14] 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 owned 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.[15]

Finally, D&O policies typically have an exclusion for acts (and sometimes omissions) by a director that were deliberately fraudulent or deliberately criminal.[16] 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.

[15] 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.

[16] 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.