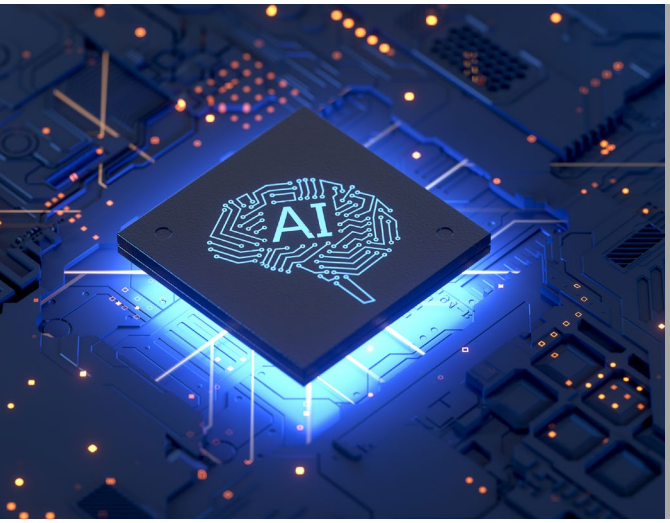
CRC Group
Wholesale & Specialty

Risks & Insurance Implications for Companies Leveraging AI

Artificial Intelligence (AI) is one of the hottest topics in today's world. It has captured the spotlight due to a recent surge in generative AI capabilities, the public availability of such tools, and the rapid expansion of IoT (Internet of Things) that connects everything from appliances and wearable devices, to homes, security systems, and vehicles.

AI capabilities are transforming how organizations manage customer engagement, operations, and almost every other facet of business. Organizations across all industries are leveraging advanced technology to enhance efficiency and innovate in an effort to gain a competitive edge. Historically, new technologies have led to significant changes, and AI's integration with modern digital operations is expected to cause significant economic disruption over time. However, it is crucial for organizations to address the risks and necessary insurance sooner, rather than later.

While AI has been developing for decades, the rise of generative AI has presented new opportunities and risks across industries. In March 2023, OpenAI released ChatGPT-4, its most sophisticated conversational AI model to date. Since then, the tech sector's market capitalization has surged by 50%, adding $6 trillion in shareholder value. The AI boom has also elevated share prices for heavy hitters like Microsoft, Alphabet (Google's parent company), and Amazon, who are laying out big money to develop the technology.[2]



In February 2024, Nvidia, a company known for designing chips essential for training AI models, reported record Q4 results, pushing its market value toward $2 trillion.[2]

Businesses around the globe, including film studios, banks, and consulting firms have rapidly adopted AI. Many large corporations are actively experimenting to determine what works. For example, JPMorgan Chase has implemented over 300 AI use cases, while consulting firm Capgemini has utilized Google Cloud's generative AI to produce a library of over 500 industry-specific use cases. Similarly, the German chemicals giant Bayer has reported more than 700 use cases for generative AI.[2]

Law firms are using generative AI to streamline tasks, such as due diligence and contract analysis. Investment banks are using AI to automate research processes, and other companies are using AI to build software, improve users' search results, or enhance advertising. Despite these advancements, an IBM poll suggests that many companies are hesitant to disclose their use of AI because their organizations still lack internal expertise on the subject. About 25% of American companies have banned the use of generative AI in the workplace entirely – possibly due to data privacy and security concerns. In their annual reports, Blackstone and Eli Lilly, leaders in private equity and pharmaceuticals respectively, cautioned investors about AI-related risks, including the potential for leakage of intellectual property.[2] Consequently, many companies have wisely started asking more questions about how AI is incorporated into tech stacks.

According to IBM, approximately 34% of businesses use AI and another 42% are exploring AI integration.[1]

AI TECHNOLOGY RISKS

From a cybersecurity perspective, AI presents both benefits and expanded risk. Nonetheless, companies around the world are integrating AI into their products and operations, despite the emerging and varied regulations on AI safety and liability. The European Union is working to create a comprehensive AI Act, while Great Britain is taking more of a wait-and-see stance. In October 2023, President Biden issued an executive order on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," to formulate, among other things, reporting requirements for AI developers in the U.S.[11] As AI applications continue to expand, so does the potential risk. Key risks that are becoming more prevalent include:

Enhanced Social Engineering. Cyberattacks are only growing more sophisticated; however, many still start with social engineering and email. Phishing emails were previously easier to spot due to incorrect grammar, low sophistication, and other errors. When attackers use generative AI to create these emails, it removes those easy-to-spot flags, enabling more seamless social engineering.

DDOS Attacks. AI algorithms can be used to automate the control and coordination of distributed denial-of-service (DDOS) attacks. In a DDOS attack, compromised devices are used to flood a target with an overwhelming amount of traffic, effectively turning these devices into "zombies."

Exploiting Vulnerabilities. Bad actors can use AI to automate the process of finding and exploiting vulnerabilities before they are patched. While the risks associated with such AI misuse are not yet completely understood, one can envision terrifying scenarios. Consider that modern cars are internet-enabled, allowing drivers access to roadside assistance, navigation, and other features.[3] New vulnerabilities could arise if bad actors gained access to these connected vehicles' systems or data. Connected vehicles gather massive amounts of sensitive data on drivers and passengers; interact with critical U.S. infrastructure; and can be piloted or disabled remotely. At the end of February 2024, President Biden took action to protect Americans from the security risks posed by connected vehicles from concerning countries such as China. The Department of Commerce is now investigating the national security risks presented by connected vehicles that incorporate technology from countries of concern and considering regulations to address those risks.[4]

Privacy Concerns. The ability of AI to process and analyze large volumes of data can undermine efforts at anonymization. This means that AI can potentially identify individuals even if personal information is not directly included by correlating and synthesizing information from multiple data points across a dataset.

POTENTIAL INSURANCE IMPLICATIONS

As AI use cases increase, so do the potential implications for insurance. Both private and public sector stakeholders, particularly shareholders, are paying close attention. Governing bodies, tasked with outsourcing investment and raising capital, often look to emerging technologies to raise funds. This trend was previously seen with non-fungible tokens (NFTs) and digital assets, and the focus has now shifted to AI.

AI Washing Allegations. The expansion of AI use cases sometimes serves merely as marketing or "window-dressing." This phenomenon, known as "AI washing," involves companies exaggerating the use of AI in their products and services to boost their market appeal.[2] This practice not only misleads investors, but also raises significant legal and insurance issues as these claims are scrutinized as deceptive and the true capacities of the products and services are evaluated.[5]

In March, the SEC settled charges against two investment advisors for making false and misleading statements about their use of AI. The firms paid $400,000 in total civil penalties.[6]

Regulatory & Plaintiff Lawsuits. Gary Gensler, head of the U.S. Securities & Exchange Commission (SEC), is also focused on the risk to markets and investors when AI is utilized to make recommendations and trades. AI models can generate incorrect outputs known as "hallucinations." If that occurred on a large scale, it could wreak havoc on financial markets. The SEC is now developing regulations for how brokers and investment advisors leverage AI and other predictive data analytics when interacting with customers. Generally, evolving regulatory oversight contributes to an uptick in claims and lawsuits.[7]

Privacy Violations. The trend toward personalized insurance has substantial privacy implications that are likely to come under greater scrutiny. Take car insurance as an example. Many drivers may not be aware that activating AI-supported features in their vehicles allows the collection and use of data about their driving behaviors, which is often shared with third-parties, including insurance companies and data brokers. Auto manufacturers and others claim to have permission to collect and use such personal information, asserting that consent is given through fine print in click-through agreements and privacy policies, but such practices are almost invisible to drivers, and certainly invisible to passengers.[3] This situation highlights the need for more transparent data handling practices to ensure that consumers are truly informed and consenting.

Copyright Infringement Claims. AI models rely on large amounts of data sourced from third parties. However, there is often a lack of transparency regarding the source of that data or how it is stored within the AI itself, presenting substantial copyright issues that will only grow over time.[11] Many of the key intellectual property issues brought to light by AI, ranging from the use of copyrighted material as training data for AI models to whether or not AI-generated works can be copyrighted, will likely only find resolution in the court room or through new legislation.10 The courts are already seeing cases emerge. In December 2023, The New York Times sued OpenAI and Microsoft for copyright infringement, starting an intense legal battle over the unauthorized use of published information to train AI models.[8] And in a similar case, four unidentified plaintiffs sued GitHub, OpenAI, and Microsoft over the reproduction of licensed open-source code.[9]

Defamation & Discrimination Lawsuits. AI can generate inaccurate information or biased outputs, giving rise to defamation and discrimination claims. In December 2023, Rite Aid faced regulatory action when the Federal Trade Commission (FTC) imposed a 5-year prohibition on the company's use of AI-based facial recognition technology. The FTC had alleged that the company used such technology without implementing reasonable safeguards, resulting in harm to consumers as the technology exhibited bias when tagging consumers, particularly women and people of color, as shoplifters. The FTC's settlement with the company confirmed that preventing the misuse of biometric information is a high priority for the FTC, which issued a warning earlier in 2023 that the agency would be scrutinizing biometrics use.11 In another case, OpenAI is being sued for defamation due to a "hallucination" that claimed Mark Walters, a conservative radio host, had embezzled money from the Second Amendment Foundation, a totally made-up fact.[12]

Blurred Liability Lines. Use of AI can make it difficult to determine where liability begins or ends. Yet, when AI goes awry, there is potential for a broad range of losses including reputational and financial harm, in addition to third-party liability. For example, if an AI algorithm causes loss, where does that liability land? – with the business utilizing it, the AI developer, or the licensor? Much depends on the contract. However, it is clear that those companies using AI will be held responsible by regulators for that use. Companies cannot blame their vendors or their employees, even when potential employee negligence increases uncertainty for insurers. The lines between professional and product liability may continue to shift as regulations take hold. But even now, the relationship between users and developers is blurring as companies co-create AI systems and leverage proprietary information to train or refine AI models.[13]

The global market for generative AI was $11.3 billion in 2023 and is expected to reach $51.8 billion by 2028.[14]

HOW CAN INSUREDS PROTECT THEMSELVES?

From a liability perspective, the wisest advice applies to both individuals and organizations – Make sure to think critically about the technologies brought into your home, life, or company. Take the time to review all insurance coverages with a trusted retail agent and wholesale broker to ensure that the exposures noted above are covered. Policyholders must also have the right governance in place as well as checks and balances around AI to ensure it is not causing harm.[13]

Read the fine print. Thoroughly read the privacy notice and terms to ensure you are comfortable with the parameters. When necessary, slow the procurement process down to confirm that vendors have appropriate security and protections in place around your data. It is also vital to employ a more rigorous procurement process that satisfactorily answers key questions, including:

- **Is my organization's data encrypted?** Encryption is foundational to data security – protecting data from being compromised, stolen, or altered.
- **What data is retained, how is it stored, and how is the data used?** Many companies may not understand that on the back end many vendors utilize the Cloud and AI together, which can mean data is stored or utilized in ways not clearly outlined. Data access and use restrictions should be clearly spelled out in contracts.
- **Are the limitations on use truly honored?** The word "insights" should be treated as a yellow flag. If a vendor indicates that it can derive insights from a user's data, that signals that something is being done with an insured's data that warrants further questioning.
- **What does the actual contract say vs. marketing materials?** It is important that insureds require clarity around data use via the actual contract rather than through marketing materials. Vendors are moving quickly in this area because many existing contracts allow them to add new features, but that can mean AI is integrated and rolled out without much proactive insight for users.

Focus on education across the organization. A company is only as strong as its awareness of evolving threats and what they can mean for their systems. Businesses should build out guidelines for the responsible use of AI across the organization and follow that with training that helps people truly understand what can and should not be shared to help reduce the potential likelihood of harm. Insureds should be taking reasonable steps to ensure cyber security and privacy through basic safeguards. Such policies should amend or extend acceptable use policies, data use policies, and others as applied to AI systems.

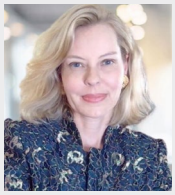
If concerns about compromising data persist after answering these questions, organizations should consider partitioning to keep certain data on a separate network so that their most valuable information is not compromised.

BOTTOM LINE

In our digital age, AI is here to stay. However, the emerging risks and insurance implications are complex, diverse, and constantly evolving. Many companies and vendors are scrambling to incorporate AI because it sells. However, new opportunities also offer new risks that must be confronted. The risk is even broader than liability. Losing control of data, which is a critical asset of any company, means losing value and it is likely that insurers will begin carving out AI exclusions as claims hit. Make it a point to review all current policies to determine if there are any gaps in coverage that should be addressed at renewal.

There is already a global focus from both legislators and regulators considering how best to regulate AI, including generative AI. It largely remains to be seen how various jurisdictions will respond (though Utah has passed a law that brings generative AI under its consumer protection statute). At this point, the court systems are beginning to review complex liability cases involving technology - and coming to different conclusions. When combined with third-party litigation funding, new products liability, and AI regulation, this could result in substantial liability shifts in the years ahead.11 Partnering with knowledgeable wholesale brokers well-versed in AI-related risks can help ensure your clients navigate this new world with the right safety nets in place. Reach out to your CRC Group producer today.

GUEST CONTRIBUTORS



KATHRYNE (KATE) M. MORRIS

Kathryne (Kate) M. Morris is a co-founder and member of Hosch & Morris, PLLC. Kate is a versatile, tech-savvy attorney with expertise in data privacy and cybersecurity and more than 15 years of experience in commercial transactions and litigation. She specializes in U.S. and E.U. data privacy and cybersecurity issues, focusing on transactional and governance matters related to data and technology. Learn more here.

RUSSELL (RUSS) B. PEARLMAN

Russell (Russ) B. Pearlman serves as Of Counsel to Hosch & Morris, PLLC, and acts as the firm's Chief Technology Officer. Russ has a unique background that includes over 25 years of progressively senior positions in business and technology roles. His hands-on approach has made him responsible for developing technology strategy and operating it, including support for thousands of employees and multiple data centers. In addition, Russ obtained his law degree with a focus on the issues that face companies that utilize technology for competitive advantage including intellectual property, trade secrets, cyber security, data privacy, e-discovery, and technology-based contracts. Learn more here.

CONTRIBUTORS

- **Drew Taylor** is a Vice President & Broker with CRC Group's San Francisco office where he focuses on helping clients find solutions in new and emerging sectors like digital assets, cannabis, and fintech.
- **Alex Slawson** is a Senior Broker with CRC Group's San Francisco office where he leads the Cyber & Professional Liability Practice for CRC Group's San Francisco Financial Services Team.

ABOUT HOSCH & MORRIS

Hosch & Morris, PLLC is a boutique law firm dedicated to data privacy, information security, the Internet, and technology. The firm offers extensive transactional and litigation experience, privacy and technology depth, as well as a wide breadth of perspective across many different industries in distribution, marketing, finance, employment, competition, intellectual property, and professional services. Hosch & Morris takes the time to learn clients' businesses and focus on what they need with the aim of growing, improving, and maximizing the value of the data and technologies on which clients' businesses are built. Learn more here.

END NOTES

1. Top Artificial Intelligence Statistics and Facts for 2024, CompTIA, February 29, 2024. https://connect.comptia.org/blog/artificial-intelligence-statistics-facts#:~:text=Machine%20Learning%20and%20AI%20Stats&text=34%25%20of%20companies%20currently%20use,new%20AI%20and%20automation%20tools

2. How Businesses Are Actually Using Generative AI, The Economist, February 29, 2024. https://www.economist.com/business/2024/02/29/how-businesses-are-actually-using-generative-ai

3. Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies, New York Times, March 13, 2024. https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html

4. FACT SHEET: Biden-Harris Administration Takes Action to Address Risks of Autos from China and Other Countries of Concern, The White House, February 29, 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/fact-sheet-biden-harris-administration-takes-action-to-address-risks-of-autos-from-china-and-other-countries-of-concern/#:~:text=At%20the%20President's%20direction%2C%20the,regulations%20to%20address%20those%20risks

5. AI Washing Explained: Everything You Need to Know, TechTarget, February 29, 2024. https://www.techtarget.com/whatis/feature/AI-washing-explained-Everything-you-need-to-know#:~:text=The%20goal%20of%20AI%20washing,they%20have%20on%20the%20environment

6. SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence, Securities and Exchange Commission, March 18, 2024. https://www.sec.gov/news/press-release/2024-36

7. Gensler's Warning: Unchecked AI Could Spark Future Financial Meltdown, Politico, March 19, 2024. https://www.politico.com/news/2024/03/19/sec-gensler-artificial-intelligence-00147665

8. The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work, The New York Times, December 27, 2023. https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

9. GitHub Copilot copyright case narrowed but not neutered. https://www.theregister.com/2024/01/12/github_copilot_copyright_case_narrowed/

10. Ruling on Motion to Dismiss Sheds Light on Intellectual Property Issues in Artificial Intelligence, JD Supra, May 24, 2023. https://www.jdsupra.com/legalnews/ruling-on-motion-to-dismiss-sheds-light-6984451/

11. Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, Federal Trade Commission, December 19, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

12. OpenAI Fails to Escape First Defamation Suit From Radio Host. https://news.bloomberglaw.com/ip-law/openai-fails-to-escape-first-defamation-suit-from-radio-host

13. 13 AI Will Shift Liability Rather Than Create New Risks, Commercial Risk, March 19, 2024. https://www.commercialriskonline.com/ai-will-shift-liability-rather-than-create-new-risks/

14. 25 Top Generative AI Statistics For 2024, BloggingWizard, February 12, 2024. https://bloggingwizard.com/generative-ai-statistics/#:~:text=According%20to%20research%20conducted%20by,of%2035.6%25%20year%20over%20year