
News

Client Insight: Assessing AI-Related Risks – for Public Disclosures, Investors or the Board

January 3, 2024 – Insights

RELATED FOCUS

[Private & Public Companies](#)

[Data Privacy](#)

[Employment & Labor](#)

[Strategic Transactions & Licensing](#)

The recent emergence of sophisticated artificial intelligence (AI) technologies with far-reaching use cases has opened up new opportunities for companies across industries. But as has been the case with many rapidly developing technologies, AI also creates new risks or heightens existing risks for many companies. Because companies are integrating AI into their businesses in many ways, there will not be a single risk management, governance or disclosure approach for all of them. Drawing on our clients' experience, we present a few discrete categories of risks to help boards, management teams and investors assess some of the AI-related risks that their companies may face.

Investors, technology companies, regulators and the general public have increased their focus on the field of technologies based on artificial intelligence, machine learning and other advanced computational methods, which we collectively refer to as AI. In board rooms, investors' letters and earnings calls, companies are expressing excitement for what AI, including generative AI technologies, can make possible for their operations and products. The list of use cases is expansive. While some companies are developing and integrating AI-powered features into their products, others are seeing potential growth from integrating third-party AI-powered offerings into their operations.

New risks accompany these new opportunities. Boards and management teams have to identify the material risks faced by their companies, whether to exercise risk oversight and risk management governance or to update disclosure in public filings or Rule 701 prospectus risk factors. Assessing these risks can be challenging given the breadth of AI's potential uses as well as its evolving capabilities.

Drawing on our clients' experience, we have broken this risk assessment into a two-part analysis as follows:

1. a framework for understanding how a company is using AI technologies, and
2. the categories of risks companies should consider depending on how, if at all, the company is using AI technologies.

The hype around AI, and frequent overuse or misuse of AI-related terminology, can obscure how AI is being integrated into a business. The following table categorizes certain ways companies may be using AI-powered technologies, to help identify what specific types of risks may be implicated.

How is the company deploying AI-powered technologies?

Integrating AI-powered features into its externally-facing products

Purchasing AI-powered offerings to support its internal operations

Training AI models on public or unlicensed third-party data

Training AI models on the company's or customer's proprietary data

Using AI-tools to generate new and original content (e.g., text, images, audio)

Using AI-powered technology for product development

Using AI-powered technology for high-stakes or regulated decision-making

A solid grounding in the company's use cases for AI can then inform an assessment of the related company-specific risks. The following table presents some key potential AI-related risks that a company may identify when performing this risk assessment. This list is not exhaustive, and we expect the risks and opportunities to change as AI technologies continue to evolve.

Certain Risk Categories Depending on the Use of AI

<p>Risks faced by all companies, whether or not they are using AI technologies</p>	<p>Increased Cybersecurity Risks. Commentators expect AI to be used in more numerous and more sophisticated cyberattacks. AI's use to automate, target and coordinate cybersecurity attacks will affect startups and incumbent companies alike.</p> <p>Increased Market Competition. AI is not simply a new industry, but rather it is a catalyst to innovation in many legacy industries. AI-powered offerings are appearing in a variety of different sectors, including healthcare, financial services, automotive, e-commerce, manufacturing, retail and communications. Technology entrepreneurs may be entering marketplaces where they compete with each other and with incumbents that have the resources to build or deploy similar, AI-powered offerings. In addition, companies that aren't using AI today may find that the adoption of AI by competitors or new market entrants disrupts their industry and changes their competitive landscape.</p>
<p>Risks faced by companies</p>	<p>Defects in AI-Powered Offerings. Defects in AI-powered offerings can arise from a variety of factors, including the underlying models, the nature</p>

Certain Risk Categories Depending on the Use of AI

using AI technologies

of data used to train the AI model and the prompts used to query models, AI models can produce inaccurate results that appear to be logical and factually accurate, particularly since AI models tend to report results with a high degree of confidence. The training data may be inaccurate or biased or may come from one context that is not suited for models deployed in other contexts. Incorrect results may be generated by an AI model when its underlying data have structural defects and these issues could negatively affect companies even when they did not generate or collect the underlying data. Customers or others may rely on or use flawed content to their detriment. Addressing these issues can be time-consuming, expensive and distracting, and they can exacerbate the legal, regulatory and reputational risks described below.

Ethical Risks and Potential Reputational Harm of Using AI. AI technologies present emerging ethical and social issues. AI algorithms can create unintended biases or discriminatory outcomes, either due to the data source being used or the design of the predictive analytics. Generative AI can produce unexpected results or hallucinations, that is, results that contain false or misleading information. These hallucinations can raise ethical concerns when, for example, they are presented to users as factual. Reputable AI and generative AI tools may be used for abusive, illegal or manipulative ends. The actual or perceived lack of transparency in the algorithms or data being used can heighten concerns around equity, accountability, bias, breach of privacy, consumer protection and quality control in the use of AI-powered tools. Such concerns have caused many legislators, regulators and members of the general public to criticize technology companies using or developing AI-powered offerings. The addition of AI-powered technology to an offering that was not previously based on AI may expose that offering to new scrutiny or negative attention. To the extent a company is exposed to negative attention, whether from a specific incident or general ethical concerns, its reputation could be negatively affected. Implementing compliance measures to address potential ethical concerns can be costly or ineffective.

Legal and Regulatory Risks. Critical attention on AI may lead to a stricter regulatory environment, government investigations and litigation from private parties. The last decade has seen tremendous changes in regulations relating to data privacy and to the use, storage and movement of electronic data. It is unclear how regulators and legislators will respond to AI technologies in the United States, at the federal and state level, European Union, United Kingdom, Canada, China and otherwise, and such regulation, at a minimum initially, is likely to vary between jurisdictions. Companies will face not only direct costs from litigation or investigations alleging non-compliance, but also indirect costs to establish policies, controls, training, risk management and governance procedures to comply with evolving and potentially uncertain or conflicting domestic and international regulations. Specific AI use cases may be, and in some cases already are, subject to express regulation. For example, use of AI for employment decisions has been scrutinized by the Equal Employment Opportunity Commission, use of AI for healthcare decision-making can require compliance with Food and Drug Administration regulation for medical devices, and the extent to which online service providers are immune for using AI for content moderation and publishing AI-generated outputs remains subject to the ongoing legislative debate over reforming Section 230 of the Communications Decency Act. Further, in accordance with the Biden Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI, forthcoming US regulations and agency guidance will apply to companies using AI technologies across all sectors—including stricter measures for companies acquiring, developing, or possessing large-scale computing clusters to develop dual-use foundational AI models—which could increase regulatory compliance costs for companies in the future.

Evolving Industry Standards. In addition to domestic and international regulatory changes, mounting pressure for companies to comply with self-regulatory standards is expected. For example, in the United States, various self-regulatory frameworks for responsible AI use and

Certain Risk Categories Depending on the Use of AI

governance have emerged in the absence of formal regulation. Furthermore, as of December 1, 2023, the members of the G7—Canada, France, Germany, Italy, Japan, United Kingdom, European Union and the United States—have agreed upon and endorsed a voluntary set of AI Principles and Code of Conduct for businesses. Companies may face additional costs to align with increased industry-motivated scrutiny for compliance with voluntary AI governance principles.

Uncertain Intellectual Property Rights. Companies typically rely on a wide variety of intellectual property, or IP, rights, including copyright and trade secrets, to protect their business. It is unclear whether technology companies will have copyright protection over code that their employees produce by means of AI-powered tools.

Risks from Using Non-Proprietary Training Data. When AI-powered tools are trained on third-party data sets or other non-proprietary data (like customer data), companies have to be careful not to incur liability through potential violations of privacy laws, contracts or other third-party rights. Companies will need to develop appropriate protections and safeguards for handling the use of customer data with AI technologies. In addition, developing technology using AI-powered tools trained on datasets whose provenance is unknown may expose the company to third-party claims of IP ownership rights. Concerns about data set ownership may lead to the development of new approaches and processes to provide attribution or remuneration to creators of training data, which could increase compliance or financial costs for companies in the future.

Risks from Using Third-Party AI Technologies. Companies may use third-party AI technologies to analyze their own data or customer data, to enhance their products or services, or to develop software. Using third-party or open source software, including AI-powered tools, to develop products, services or software can raise IP ownership issues. In addition, sharing data with third parties to use third-party AI tools can create a risk that proprietary data may be accidentally released, even in connection with authorized uses. Employee interest in using AI to streamline routine tasks or to automate difficult tasks has pushed many large companies to adopt explicit policies around such uses. For example, in May 2023, Samsung reportedly banned employee use of third-party generative AI tools after discovering that its engineers had accidentally leaked internal source code by uploading it to ChatGPT.

**Additional risks
faced by
companies
developing their
own AI
technologies**

Uncertain Return on Investment. Companies are seeing their expenses go up as they invest in the development of new, AI-powered offerings and more complex machine learning models. Development of a new AI-powered offering might require significant outlays of cash for new hardware or additional costs related to cloud-computing resources. In addition, the development of any new technology will be time-consuming and may require additional personnel to be hired or contracted. These additional costs may not lead to a significant breakthrough or result in a product or technology that can be offered or licensed at a price yielding a return on investment.

Increased Labor Competition. AI is a specialized field comprised of many subfields, such as natural language processing, large language models, computer vision and machine learning. In addition, specialized knowledge may be helpful or required for the application of AI to certain areas, such as healthcare or cybersecurity. The underlying domains of knowledge have been changing rapidly over the last several years, and the increased attention on AI seems likely to spur more interest in developing this base of knowledge. Companies seeking to develop innovative

Certain Risk Categories Depending on the Use of AI

AI-powered technology are therefore seeing increased competition for specialists in AI and software engineers required to support their AI initiatives.

Litigation Risk. Companies developing or deploying proprietary AI technologies, including foundational large language models, are exposed to a wide range of potential actions brought by private and governmental actors. Companies offering such proprietary AI technologies may see a significant increase in legal expenses for the defense against actions related to intellectual property infringement, consumer protection, privacy rights, employment rights, and contractual violations, as well as potential civil or criminal liability incurred from the distribution of errors, bias, or misinformation through such AI systems. These risks are heightened by the rapidly-evolving regulatory landscape for AI-related matters, and lack of established precedent or historical case law parallels. For example, in addition to a defamation case filed in state court by a private party, several class actions have been filed in federal court against OpenAI in 2023 alleging that the data OpenAI used to develop and train the AI models underlying its products violates consumer privacy laws and constitutes copyright infringement. Similar class action lawsuits have been filed against other AI technology providers—including Anthropic, Microsoft, Alphabet, Meta, and Stability AI—which remain ongoing without final settlement or adjudication. Given the lack of clarity in potential litigation risk and liability, companies developing proprietary AI technologies may experience increased costs and resource expenditure monitoring, defending, and implementing appropriate guardrails to comply with legal judgments.

As illustrated above, AI creates new risks and may heighten existing risks for many companies. Because companies are integrating AI into their business in various ways, there will not be a single risk management, governance or disclosure approach for all of them. As AI is expected to be a fixture in the business landscape, we anticipate companies will need to review their approach to AI-related risks on a regular basis. Companies would be wise to focus on developing prudent risk management, governance and disclosure approaches that account for the particular AI-related risks that they encounter and expect to encounter.

[SILICON VALLEY](#) [ANN ARBOR](#) [AUSTIN](#) [BEIJING](#) [BOSTON](#) [LOS ANGELES](#) [NEW YORK](#) [SAN DIEGO](#) [SAN FRANCISCO](#) [SÃO PAULO](#) [SINGAPORE](#)

[contact](#) | [terms of use](#) | [privacy policy](#) | [legal notices & attorney advertising](#)

Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP

© 2024 Gunderson Dettmer; all rights reserved.

[Website Credits](#)