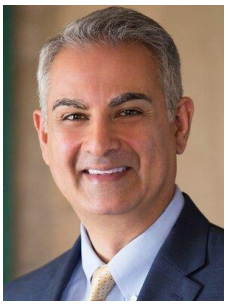
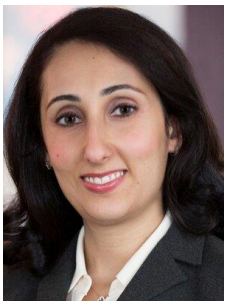
LAW360

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

Key Considerations For Evaluating An AI Vendor

By **Rahul Kapoor and Shokoh Yaghoubi** (February 12, 2024, 4:38 PM EST)


Rahul Kapoor


Shokoh Yaghoubi

Artificial intelligence technology is advancing rapidly and will soon permeate many industries.

AI technology can be used to streamline business operations and enhance client experience, and many businesses will likely turn to AI for these benefits and to gain a competitive edge.

However, selecting the right AI vendor is crucial for the successful implementation and utilization of AI technologies. This article delves into the key considerations that businesses should assess when choosing an AI vendor.

Some of the considerations discussed herein — especially as they relate to an AI model's output — may not be relevant for nongenerative AI systems, which analyze, process and make decisions based on existing data, rather than generating new content or data.

Type of Technology

What is the source of the vendor's AI model? AI models may be built internally from a proprietary base, built internally from an open-source base, or licensed from a third party, or a third party may be a subprocessor through which the vendor's team passes data to the model and receives back results.

Given that some AI vendors will not be developing their own AI models, it is important to understand the source of the vendor's AI model to determine whether company data will be passed through to a third party, the AI model's source and accuracy, and the standard of service one may be able to expect from the vendor. A well-developed AI model would provide the best base for any AI services.

Experience and Expertise

A key consideration when evaluating any vendor is its experience and expertise in the field. Given the relative novelty of AI technologies, companies will want to assess the vendor's record, including past projects, case studies and client satisfaction.

It is important that the vendor's team consists of skilled engineers, AI specialists and data scientists who have experience with the development and support of AI technology.

Businesses should also research the litigation history of the vendor. This search should include intellectual property infringement claims against the vendor and other disputes, which will allow the business to make more informed decisions regarding contractual terms with the vendor, such as indemnity for third-party claims and limitation of liability provisions.

Training Data

What type of training data does the AI model use? Does it use scraped datasets? The output of an AI model depends on the data that was used to train the model.

As such, it is imperative to know whether the model is trained on reliable sources and the quantity of data that is used to train the model.

Similarly, it is also important to know how often the vendor refreshes its training datasets. An effective AI model should have the capacity to adapt over time and ensure that the data that feeds the model remains current. Scraped datasets can lead to potential infringement claims, so understanding if a vendor obtains a license to use its training data will assist when assessing the potential for liability in using the vendor's data.

Will the vendor use the company's data as part of its training data? If so, consider how the company would like to allow the vendor to access the company's data and if the company's license to the vendor to such data should be limited to certain types of company data.

It is also important to analyze and appropriately limit the use of the company's data by the vendor as part of the vendor's offerings to third parties. This also segues into considerations regarding who should own the output data and what licenses should be granted to either the vendor or the company for output data depending on who owns such data.

Privacy

Does the vendor use personal data as part of its training data? If so, is personal data de-identified or anonymized before being used as training data? How does the vendor prevent re-identification of personal data used as input/training datasets? What levels of consent did the vendor obtain from data subjects for processing personal data in the training data used by the AI model?

It is also vital to evaluate the vendor's data security measures to protect any personal data the vendor may access when collaborating with its customers. Security measures include encryption protocols, access controls and compliance with applicable laws, including the European Union's General Data Protection Regulation and the Health Insurance Portability and Accountability Act.

Consider inquiring about the vendor's history with privacy compliance and whether the vendor has experienced any data breaches.

The inquiries regarding privacy are important because a company will want to know if the vendor will use any personal information provided by the company to the vendor as part of its training data. From a liability perspective, companies will not want to collaborate with a vendor that is not complying with applicable privacy laws in its use and disclosure of personal information.

Model Transparency and Bias

How does the AI system mitigate inaccurate, biased and underrepresented outputs? Transparency is crucial in AI, as companies will not want to rely on information from an AI system that is not easily understandable.

It is also important to understand how a vendor tests and validates its AI model to ensure that the output of the model is accurate.

Has the vendor established a risk management system related to the AI system with human oversight for the same? Companies can also request that the vendor provide case studies and test results that show the accuracy of its AI model's output.

Integration, Training and Support

Evaluate how seamlessly the vendor's AI solutions can integrate with existing systems and infrastructure.

Companies will also want to inquire if the AI solution can be customized to meet their business needs. A reputable and experienced vendor should be able to tailor its AI algorithms and models to align with a customer's business goals and requirements.

Initial and ongoing training is also key to the implementation of a successful AI solution for a company's business. AI solutions are often offered as software-as-a-service models and, as with other hosted solutions, the vendor should provide certain performance metrics such as a service-level agreement for availability of the solution and error resolution.

It is also important to determine the scalability of the AI solution. Can the vendor's AI infrastructure scale up to meet the business's demands and increased workloads? Consider the vendor's solution's processing power, storage capacity and performance optimization.

Compliance With Law, Regulations and Guidelines

While AI regulation in the U.S. is still in a nascent stage, there are various organizations, such as the National Institute of Standards and Technology — which released its Artificial Intelligence Risk Management Framework last year[1] — setting forth guidelines that assist AI actors, including organizations and individuals, addressing the unique risks posed by AI.

Although the AI framework is not binding on organizations, it does address some fundamental issues with AI, such as ensuring that AI systems are valid and reliable; safe, secure and resilient; and accountable and transparent. The framework also accounts for other key factors.

A vendor's adherence to the AI framework is voluntary, but organizations that implement the framework or implement policies incorporating the concepts addressed by it will be better prepared for the unique risks presented by AI technologies.

When choosing an AI vendor, businesses should assess a vendor's general compliance with applicable laws, regulations and guidelines including adherence to the AI framework or internal policies based on or similar to the AI framework.

It is also important to assess how the vendor will adapt to new and changing AI regulations and if it has the capacity to do so. As AI regulations evolve, AI vendors must be prepared to address varying requirements, especially if the vendor is a multinational organization. Businesses should inquire how the vendor will communicate regulatory changes to the business and how they will accommodate their clients' needs to adapt to regulatory changes.

Conclusion

Selecting an AI vendor requires a thorough assessment of the AI solution and the vendor's practices in conjunction with a company's business goals. The foregoing is a nonexhaustive list of some of the key considerations in selecting an AI vendor.

By evaluating the vendor's technology, expertise, support services, transparency and the other aforementioned factors, businesses can mitigate the risks posed by acquiring the vendor's AI services, while maximizing the value of the business's investment.

Rahul Kapoor is a partner and Shokoh Yaghoubi is a senior associate at Morgan Lewis & Bockius LLP.

[1] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.