Reuters Legal News

AI-focused procurement playbook refresh

By Ken D. Kumayama, Esq., and Pramode Chiruvolu, Esq., Skadden, Arps, Slate, Meagher & Flom LLP

APRIL 10, 2024

Companies need to adapt their procurement playbooks (Playbooks) to the rapid integration of generative artificial intelligence (GenAI) features and functionality into the tools their teams procure. While GenAI features and functionality are attractive to the customer, it's important to remember that they can not only increase the magnitude of risks associated with traditional software and software as a service (SaaS) tools, but they can also present entirely new risks.

As a result, while existing Playbooks and policies may already address some considerations applicable to GenAI tools, the potential increase in magnitude of the existing risks and new risks presented by GenAI require a fresh approach.

Licensing terms

GenAI tools, especially those based on SaaS models, often come with online terms of use, usage policies, publication policies, privacy policies and other terms and conditions that are incorporated by reference in vendors' form enterprise licensing agreements. These terms are often subject to frequent changes by the vendor, and vendors are often reluctant to negotiate such terms outside of high-value business engagements.

Playbooks should require counsel review to these terms together with the enterprise licensing agreement, and if possible, to negotiate so that such terms remain fixed or consent is required for material changes. In addition to avoiding clauses that allow unilateral changes by the vendor, this legal review should focus particularly on the terms discussed below.

Vendors' rights to use inputs and outputs

Vendors often want to use customer inputs (including prompts and data retrieved from customers' systems) and outputs not just to provide AI services to the customer, but also to improve (i.e., to train or fine-tune) the vendor's models. They also frequently want flexibility to share customer data with third parties, including their subcontractors, partners and other customers, and use the customer data to investigate abuse or misuse of the vendor's AI tools.

Using GenAI tools offered to consumers would typically involve such broad grants to the vendors. However, vendors are often willing to give enterprise customers better terms that restrict the vendors' rights to use inputs or outputs beyond providing the services to the customer.

Playbooks should therefore address when the company can agree to these broad vendor rights and when the company should push back. In particular, policies should restrict vendor use of inputs and outputs for tools that will be used for potentially sensitive projects, or into which proprietary, confidential or private data will be input. And in general, even for less sensitive projects and data, there is enough risk of accidental misuse that policies should instruct counsel to ensure contracts do not allow the vendor to claim ownership or unrestricted use of any inputs or outputs.

Confidentiality considerations

The use of GenAI tools often involves handling sensitive data, including third-party materials like customer data. For example, large language model tools increasingly offer retrieval-augmented generation (RAG) functionality, where the tool retrieves relevant context to respond to prompts from a database or graph consisting of a wide range of user data.

> *While existing Playbooks and policies may already address some considerations applicable to GenAI tools, the potential increase in magnitude of the existing risks and new risks presented by GenAI require a fresh approach.*

If these RAG-based systems involve broad access to unencrypted data, there is a heightened risk of confidentiality breaches, as providing the vendor access to that data itself may breach confidentiality obligations and if it does not, it may undermine access permissions, creating a risk that confidential, proprietary and third-party data may be leaked in response to unrelated queries.

As a result, information security reviews, including data access controls, should be part of any GenAI tool Playbook. Companies should also ensure the confidentiality provisions clearly outline the vendor's obligations regarding data handling and confidentiality and restrict the use of the customer's data in line with its confidentiality obligations owed to third parties.

Where any sensitive, proprietary or private data will be shared with the vendor, agreements should include the right to conduct regular audits and reviews of the vendor's compliance with data security and confidentiality obligations. Counsel should also note any rights vendors have to monitor usage of AI tools, including monitoring for abuse or misuse of the systems, as such monitoring can undermine the confidentiality and security of the company's data and in some cases, vendors will permit companies to opt out of such monitoring.

Protecting AI-generated content

The protectability of AI-generated content under IP laws varies across jurisdictions, affecting how companies can exploit this content commercially. While the issue remains largely unsettled, in many jurisdictions, AI-generated content may not be eligible for copyright protection, while in others, this content may be entitled to copyright protection as a computer-generated work.

Information security reviews, including data access controls, should be part of any GenAI tool Playbook.

Playbooks should require legal counsel to expressly consider addressing ownership of outputs between the vendor and customer to ensure customers have flexibility to seek protection if there is any, particularly given the potential for international variation and the unsettled state of the law.

Restrictions on creating competing models

Another critical consideration is the restriction that many AI vendors impose on using their models to create competing (or similar) tools. These clauses, often embedded in the licensing agreements, can be broad and all-encompassing, potentially preventing the company from using any generated content for training or developing future models.

Though a company may not have current plans to develop its own GenAI models, those plans could change, and these provisions can potentially limit this ability to use generated content in connection with other third-party GenAI tools.

In some cases, it may be possible to negotiate carve-outs or more favorable terms that allow for greater flexibility in using the AI-generated content. So Playbooks should be updated to ensure counsel proactively seek to clarify and negotiate these terms to avoid hindering the company's innovation and development capabilities.

Intellectual property infringement risks

Because training state-of-the-art GenAI tools generally requires massive amounts of data, the training data sets typically include copyrighted works compiled from crawling the internet and as a result, sometimes aspects of those copyrighted works appear in the outputs.

If an output contains aspects of copyrighted material, there is risk that using that output infringes a third party's copyrights. There is ongoing litigation regarding the extent to which this occurs and whether the GenAI tool providers are liable for copyright infringement as a result.

While end users of GenAI tools have not yet been sued for infringement based on their use of outputs containing copyrighted materials, the rapid proliferation of these tools and companies' reliance on these tools to generate content and code for published materials and production systems suggest that customers may face these claims in the future.

As a result, many vendors, in response to customer concerns about potential infringement risks, offer indemnification for IP infringement claims. However, these protections often come with important limitations. For instance, indemnification might be contingent on using specific filters or on the prompts or inputs not including copyrighted materials.

To ensure consistency and appropriate review of infringement risks arising from using GenAI tools, Playbooks should address these IP indemnification clauses. Playbooks should clarify the company's stance on limitations to such IP indemnification, including the acceptability of conditioning indemnification on the use of filters. Where AI tools may be used to generate external-facing content or code, legal counsel also should review the use case to determine the extent to which infringement risks are mitigated by the proposed indemnification clauses.

In addition, once AI tools are procured, companies should have policies and procedures in place to ensure required filters are implemented enterprise-wide and that any other conditions to IP indemnification are being met.

Companies should also consider whether to maintain records of AI tool usage to support indemnity tenders. Record-keeping could include detailed logs of version settings, system prompts, inputs and outputs, but note that keeping such records may require significant investments to build a technology pipeline and to store potentially voluminous records.

Retention of such records should be considered together with general record-retention policies and obligations, including legal holds or other restrictions on destruction of documents, as well as data minimization requirements (e.g., for personal data under applicable privacy laws).

Service levels and warranties

GenAI tools require significant computing power to operate and vendors can struggle to procure sufficient resources to provide GenAI services to customers. As a result, they are reluctant to make firm service level commitments regarding uptime or latency.

The unpredictability of the outputs also means that vendors almost always disclaim warranties regarding accuracy and reliability of the outputs. This means that typical procurement policies relating to service levels and vendor warranties may not be well-suited to procuring AI tools.

Playbooks instead should reflect the reality that there is unlikely to be a one-size-fits-all approach for GenAI tools, and counsel should work with their clients to consider how to adjust service level and warranty expectations in light of the use case and nature of the tool.

Conclusion

Procuring GenAI tools requires a considered approach — failing to update Playbooks will likely result in companies bearing outsized risks. Legal counsel should regularly update Playbooks to address key concerns and common pitfalls in typical GenAI vendor contracts. Relatedly, companies should consider revisiting their existing vendor contracts where GenAI functionality may be newly offered.

Ken D. Kumayama and Pramode Chiruvolu are regular, joint contributing columnists on legal issues in artificial intelligence for Reuters Legal News and Westlaw Today.

About the authors

Ken D. Kumayama (L) is a partner in the intellectual property and technology group at **Skadden, Arps, Slate, Meagher & Flom LLP**. He concentrates his practice on transactional matters relating to intellectual property, technology, privacy and cybersecurity, as well as artificial intelligence and machine learning. He can be reached at ken.kumayama@skadden.com. **Pramode Chiruvolu** (R) is a counsel in the intellectual property and technology group at the firm. He advises clients on complex transactional matters involving emerging technologies, including artificial intelligence, digital health and biotechnology, the internet of things and 5G networks. He can be reached at pramode.chiruvolu@skadden.com.

This article was first published on Reuters Legal News and Westlaw Today on April 10, 2024.