BCLP. Client Intelligent

Insights

REVIEWING SAAS AGREEMENTS IN THE AGE OF AI

Feb 02, 2024

SUMMARY

The development and implementation of AI-powered tools, including in SaaS platforms, have experienced a meteoric rise over the course of the last year. Businesses are understandably looking to realize competitive advantages from leveraging these new AI technologies, but adding AI to a tech stack can present serious risks related to bias, data ownership, privacy, accuracy and cybersecurity. As with many new tools, an organization's procurement team is its first line of defense in de-risking AI, and AI literacy is essential in this process. Fortunately, while AI presents unique issues and considerations, the incorporation of AI into SaaS does not require a wholly novel SaaS agreement. Nevertheless, there are key provisions that must be considered carefully to meaningfully address the new risks and issues triggered by the incorporation of AI and the nascent state of the law and contract norms in this space. With this in mind, we have addressed below a number of key provisions that should be front and center in this analysis.

OWNERSHIP; USE

As with more traditional SaaS products, a key question to ask is who owns and/or has the right to use what? To properly address this issue, it is important to identify the components involved in receiving services from the SaaS platform and to understand where and how AI factors in. For AI, these components include: algorithm(s), training data, production data, output, and iterations of the algorithm(s) that evolve during training and usage. A key first step is to identify who owns each component, so an organization can then determine what rights the parties have with respect to each component.

In particular, the customer should consider whether to insist on ownership of, and whether to limit the vendor's use rights with respect to, customer input data, customer prompts and output generated by the SaaS platform. With respect to output, under current caselaw, AI cannot be an "author" for copyright purposes. But the parties can agree contractually whether the SaaS vendor or customer owns the output. The market is still evolving, but it is our current experience that Customers generally seek to own SaaS output from a SaaS platform—whether or not it includes AI.

Another important aspect of use is whether any of the customer input data, customer prompts or output can be used to train the AI (similar to the concept of the vendor using customer data to improve products or services). On the one hand, training can improve the underlying algorithms and thus the relevance and accuracy of the output data for the customer and other users in the future. On the other hand, customers need to guard against the risk their confidential information used as an input could potentially end up as outputs or otherwise be visible to other users of the SaaS platform. Furthermore, a customer would not want to bear any liability for the SaaS platform arising out of the fact that the customer helped train the AI component of the SaaS platform. To address this issue, organizations should consider pushing for a prohibition on use of their data for model training or for any purposes other than providing the SaaS services. Market practice is also rapidly evolving to allow for private instances of certain AI technologies so that customers can reap the benefits of allowing their data to be used for training without triggering the risks discussed above. Organizations may also consider adding a disclaimer from the customer regarding training data or indemnity from the vendor regarding its SaaS platform.

REPRESENTATIONS

The inclusion of representations related to AI is still evolving but becoming increasingly common and may be an important protection for customers. Some customers may request an assurance that the SaaS platform is devoid of any AI, while others seek comprehensive representations and warranties pertaining to the AI's development and performance. Specifically, customers may inquire about assurances aligning with legal and anti-bias principles during development and performance, as well as accuracy-related commitments.

RECORDS; AUDIT

AI legislation is on the rise around the world (see our US state law tracker) and most of these laws include some sort of auditing and recordkeeping requirements. For example, New York City's law on the use of automated employment decision tools requires businesses to conduct bias audits of AI employment tools in certain circumstances. Therefore, customers should evaluate the use cases of AI carefully but should generally consider including AI-bias-related record-keeping and customer audit rights in the agreement.

SERVICE LEVEL AGREEMENTS (SLAS)

Most SaaS agreements include obligations for the vendor to maintain the SaaS platform uptime at a certain amount and/or obligations for the vendor to respond to errors in the SaaS platform within a certain period of time. Depending on the parties' respective leverage, failure to meet these SLA obligations may lead to certain remedies for the customer, such as financial credits or a termination right. The introduction of AI to SaaS will likely not wholly revise the contractual approach to SLAs, but special consideration should be applied to understanding how the AI technology could impact

the functionality of the platform as a whole. Moreover, companies should consider requiring specific SLAs for AI accuracy, efficiency, and relevance.

DATA PRIVACY

Among the domains of risk presented by the adoption of AI technologies, data privacy and cybersecurity rank at the top of the list. As such, companies will need to pay careful attention to data ownership, use, and protection issues. A well drafted data processing addendum will hit on most relevant points for engaging an AI vendor or a vendor that will utilize AI, but businesses need to consider whether to include a specific prohibition on using customer data (which should be broader than just personal data) for training of the AI or take advantage of a private offering of the tool where available.

Also, data privacy regimes mandate transparency in connection with the collection, use, and disclosure of personal data, and where a business engages in automated decision-making (automated data processing is not the same as AI but is generally broad enough to encompass AI), there are heightened notice and consent obligations. In order for businesses to satisfy their privacy law obligations in the context of AI (which notoriously has a black box problem), they will need to lean on their vendors to provide meaningful information regarding the logic being used by the AI system and cooperation to operationalize any necessary consents or opt-out rights. Vendors will also need to make assurances that they can assist their customers in meeting related obligations, such as data subject rights of access and deletion, even with regard to the AI technologies.

INDEMNITY

In SaaS agreements generally, it is customary and appropriate for the vendor to provide certain indemnities to its customers. The importance of such protection to customers is heightened in the context of AI. The vendor should indemnify for any claims that the SaaS platform infringes any intellectual property right; and any exclusions to such intellectual property indemnity related to modifications or combinations of the SaaS platform should be scrutinized. Furthermore, as noted above, if a customer allows any of its inputs, prompts or outputs to train the vendor's AI, the customer should require a vendor indemnity for third party claims arising out of errors in output or other third-party use of the AI.

CONCLUSION

Reviewing SaaS agreements where AI is part of the SaaS platform involves a familiar process, but demands heightened awareness. Customers should think carefully about ownership and use rights, representations, indemnification, audits, SLAs, risk-shifting, and data privacy. Customers should also consider updating their template SaaS agreements and their vendor contract review playbooks.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Nathan M. Boyce

St. Louis

nathan.boyce@bclplaw.com
+1 314 259 2257

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448