The Computer & Internet Lawyer

Volume 42 ▲ Number 5 ▲ May 2025

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Trends in Negotiating With Software-as-a-Service Providers

By Gregory L. Cohen, Scott M. Tobin, Bryce H. Bailey and Adam A. Garcia

Over the last two decades software-as-a-service (SaaS) has become the dominant form of software transaction. However, SaaS contracting forms and negotiating norms appear to be going through some potential changes, which we expect to accelerate in 2025 and beyond.

Before discussing the trends in SaaS transactions, however, it is important to understand the history and purpose of SaaS because that informs our understanding of future trends and the way that the law, business and technology around SaaS are evolving.

HISTORY OF SAAS

SaaS contracting replaced and consolidated historically separate agreements for various elements of software typically installed and operated on the customer's premise and its computer systems and networks. These agreements often separately covered:

(i) Software licensing terms, requirements, restrictions and pricing;

(ii) Software implementation and deployment terms and pricing;

(iii) Ongoing software maintenance and technical support terms and pricing; and

(iv) Other provisions for hosting, governance and other matters.

SaaS models generally consolidated the items above and replaced a perpetual license with a more limited periodic license and recurring periodic fees.

The widespread adoption of the SaaS model emerged alongside a broader market trend of subscription-based services. Several of the driving factors of SaaS adoption include the desire:

(i) By SaaS vendors to have recurring revenue;

(ii) By SaaS customers for a single vendor to assume end-to-end responsibility for a software application and related infrastructure;

The authors, attorneys with Polsinelli, may be contacted at gcohen@polsinelli.com, scott.tobin@polsinelli.com, bryce.bailey@polsinelli.com and agarcia@polsinelli.com, respectively.

(iii) By SaaS customers to reduce capital and other expenses related to computer hardware and infrastructure needed to operate software applications; and

(iv) By both parties for greater financial certainty.

A SaaS arrangement typically provides a more stable recurring and certain revenue stream for the SaaS vendor, while often providing the SaaS customer a bundled periodic subscription fee that may be easier for the customer to anticipate and budget.

TRENDS

SaaS vendors have long argued that multi-customer SaaS offerings necessitate using the vendor's form of contract, and in the earlier years of SaaS, few software customers had their own SaaS-specific forms. SaaS agreements continue to evolve, and the industry continues to gain experience in both the negotiation and outcomes of SaaS Agreements. Emerging regulatory concerns also increase the materiality of SaaS terms to businesses at large. As such, the following issues are increasingly subject to negotiation between the SaaS vendor and SaaS customer:

- *Form of Agreement*: There is often a significant disagreement between the SaaS vendor and SaaS customer as to which party's form of agreement to use. SaaS vendors will always want to use their own form of agreement while sophisticated SaaS customers often desire to use their own form of agreement.

- *Integration of Other Forms*: In an effort to streamline both their SaaS agreement and negotiations, SaaS vendors often attempt to link to or refer to the SaaS vendor's standardized terms, policies, or procedures relating to various matters, including data privacy, security, subprocessors and other matters. From the SaaS vendor's perspective, this may discourage legal review and expedite or avoid negotiation cycles. From the SaaS customer's perspective, this introduces terms that may not have been fully reviewed or negotiated and which the SaaS vendor may be permitted to unilaterally modify in the future.

- *Privacy and Data Details*: The SaaS vendor and SaaS customer often enter negotiations having very different intentions and desires around the use of the customer's data that is processed and stored using the SaaS software. Customers often insist on more detailed and rigorous provisions around privacy compliance, data security and data use, including:

  (i) Approvals of or visibility into subprocessors/subcontractors;

  (ii) Where and how data is processed;

  (iii) Mitigation and remedies for data incidents;

  (iv) Maintaining certain industry specific qualifications, certifications, or standards (e.g., ISO, SOC II or III, NIST, etc.);

  (v) Rights and/or limitations on de-identifying or aggregating data; and

  (vi) Rights and/or limitations on artificial intelligence (AI) training or tuning using customer data.

  Conversely, SaaS vendors often want increased rights to customer data for the vendor's own purposes along with greater flexibility in how and where it processes and maintains customer data.

- *Data Privacy Agreements*: SaaS vendors are becoming increasingly concerned that various foreign and domestic data privacy and security regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), now require the inclusion of data privacy agreements (DPAs) with their standard SaaS agreements. DPAs are standard alone agreements or schedules to the broader SaaS agreement that address the specific requirements of the GDPR, the CCPA, or other regulatory schemes. SaaS customers, especially those with purely domestic operations, often remain uncertain as to whether a DPA is truly required or is applicable to the customer's operations. The inclusion of DPAs with SaaS agreement, and whether it becomes prevalent across the software industry, is an emerging trend that we expect will come into greater focus in the upcoming year.

- *Data Liability Exposure*: As in many commercial agreements, vendors and customers often take contrary views regarding the vendor's maximum liability to the customer. In SaaS agreements, liability for issues and problems related to the handling,

processing, access and use of the customer's data is a central consideration.

SaaS customers generally push vendors to assume risk and liability in excess of the annualized fees for privacy and data breaches (e.g., based on estimated potential exposure for the nature and volume of data involved, their cyber insurance deductibles, or other factors), either through an exclusion to the limitation of liability or an enhanced separate liability cap. SaaS vendors, however, typically try to limit their liability to annualized fees under the agreement or the vendor's insurance coverage (e.g., as may be required by the agreement with that customer or a percentage of its insurance considering the total exposure to all customers). SaaS negotiations often focus on the allocation of risk and liability, along with potential liability caps and exceptions to the liability caps, related to liability exposure for the misuse or unauthorized access to the customer's data.

- *Renewals and Price Increase*: The SaaS vendor and SaaS customer negotiations frequently focus on the renewal methods, potential price increases and growth in use of the software. While a SaaS vendor may seek the opportunity to grow the revenue associated with the SaaS agreement over time, a SaaS customer often seeks future cost predictability by attempting to restrain increases for additional use, during and after the initial subscription period, and for potential renewals after the initial subscription period. These discussions can be particularly challenging given the elevated macroeconomic inflationary pressures during the past several years.

- *Migration and Wind-Down Rights and Restrictions*: SaaS vendor and SaaS customer negotiations often include end of term data migration, wind-down and other rights, including the SaaS customer's rights to retrieve data and restrict post-expiration use of customer data for future AI or other purposes by the SaaS vendor.

- *Regulatory Issues*: Both SaaS vendors and SaaS customers are often concerned about future changes in privacy and data protection as they relate to the access, use and ownership of the customer's data including any future laws and regulations. As a result, both parties often seek to both future-proof the SaaS agreement and provide reasonable processes and guardrails to revise, re-price or terminate the agreement should changes in laws or regulations make that necessary.

- *AI*: SaaS vendors and SaaS customers are focused now more than ever on the potential use of customer data to broadly train and tune AI models. Vendors are seeking broad rights to use customer data to improve and develop future software products, including products that include AI components. Customers, however, are wary of allowing the broad use of their data for purposes unrelated to their business. The full scope of how a customer's data may be used in the future is unclear and likely to vary based on the software application, the customer's data and the industry.

  While many customers may wish to limit use of their data solely for the customer's own benefit, most SaaS vendors seek the ability to use the customer's data, often on a deidentified or anonymized basis, for a wider array of purposes.

- *Managed Customer Hosting*: Finally, and most interestingly, we are also occasionally seeing some vendors permit their customer to host and process (directly or with a third party cloud provider such as AWS, Microsoft Azure, or Google Cloud), all or some data within the customer's designated IT or cloud environment (as opposed to the vendor's owned or controlled environment), which is more like a pre-SaaS delivery on-premises license model. We expect this may become more prevalent in 2025 and beyond to address AI and data privacy and security concerns that both parties typically express. In some respects, this is also facilitated by the fact that vendors typically use one of these same third party cloud providers identified above as subcontractors and subprocessors in most SaaS models, so allowing the customer to engage and install directly in its own environment of a similar nature:

  (i) Does not necessarily create material inefficiencies from a support perspective;

  (ii) May decrease integration, throughput and latency issues associated with separate environments; and

  (iii) Gives the customer a sense of more control while letting the vendor distance itself from some risks and compliance issues.

CONCLUSION

In conclusion, understanding and carefully negotiating SaaS contracting terms is crucial for both SaaS vendors and customers. Clear definitions of service scope, data security requirements and allocation of risk and liability can prevent future disputes and foster a successful business relationship between the parties. As SaaS continues to be the dominant software delivery model, conforming to best practices and identifying emerging trends will help organizations mitigate the risks and maximize the benefits of their SaaS arrangements.